SecMaster

API Reference

Issue 10

Date 2025-06-24

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Contents

1 Before You Start

SecMaster is a next-gen cloud-native security operations center that helps with cloud asset management, security posture management, security information and incident management, security orchestration, and automatic response. It helps prevent risks, detect threats, and automatically handle security incidents.

Before calling SecMaster APIs, ensure that you have understood the concepts related to SecMaster. For more 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 all 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 under the account 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.

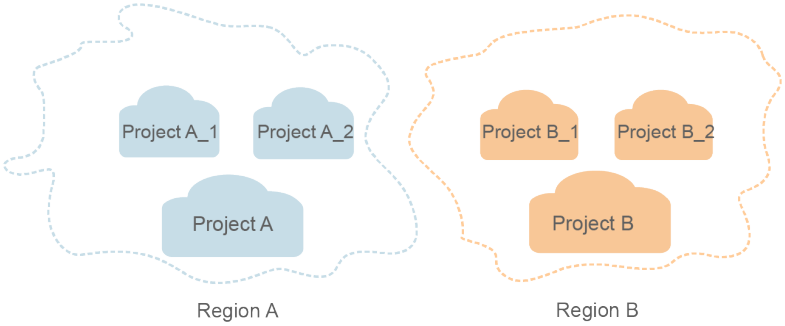
- Availability Zone (AZ)

  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 interconnected 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 create 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 in multiple regions, and resources can be directly transferred between enterprise projects.

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

2 API Overview

You can use all SecMaster functions through APIs.

Type	Description
Alert APIs	APIs for creating, deleting, and converting alerts to incidents.
Incident APIs	APIs for creating, updating, and obtaining incidents.
Indicator APIs	APIs for managing indicators, including APIs for creating, updating, and obtaining indicators.
Playbook APIs	APIs for querying, creating, and modifying playbooks.
Alert rule API	APIs for creating, deleting, viewing, and enabling alert rules.
Playbook version APIs	APIs for querying, creating, and updating playbook versions.
Playbook rule API	APIs for creating, querying, and deleting playbook rules.
Playbook instance API	APIs for querying and operating playbook instances.
Playbook review API	Playbook review APIs, including the APIs for reviewing playbooks and querying playbook review results.
Incident associations APIs	APIs for querying, creating, and cancelling incident associations.
Data class APIs	APIs for querying the data class list and field list.
Workflow APIs	Workflow APIs, including the API for querying the workflow list.
Data space APIs	Data space APIs, including the API for creating data spaces.
Pipeline APIs	Pipeline APIs, including the API for creating a pipeline.

Type	Description
Workspace APIs	Workspace APIs, including the APIs for adding and querying workspaces.
Metering and billing APIs	Metering and billing APIs
Metric APIs	APIs for querying metrics, including the API for batch queries.
Baseline inspection APIs	Baseline inspection APIs, including the API for searching check results.

3 Calling APIs

3.1 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**:

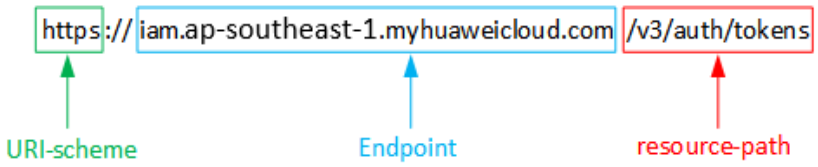
  Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of "Parameter name=Parameter value". For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

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 3-1 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 ***xxxxxxxxxxxxxxxxx*** 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": "xxxxxxxxxxxxxxxxx"
            }
        }
```



```
    }
}
```

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.

3.2 Authentication

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

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

Token-based Authentication

NOTE

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

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

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

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


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

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3.0/OS-USER/users
Content-Type: application/json
X-Auth-Token: ABCDEFG....
```

AK/SK-based Authentication

NOTE

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

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

- AK: access key ID, which is a unique identifier used in conjunction with a secret access key to sign requests cryptographically.
- SK: secret access key used 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.

3.3 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 Codes**.

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

Response Header

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

Figure 3-2 shows the response header fields for the API for **Obtaining a User Token**. The x-subject-token header field is the desired user token. Then, you can use the token to authenticate the calling of other APIs.

Figure 3-2 Header of the response to the request for obtaining a user token

(Optional) Response Body

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

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

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

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

```
{
    "error_msg": "The format of message is error",
    "error_code": "AS.0001"
}
```

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

4 API

4.1 Alert Management

4.1.1 Querying the Alert List

Function

This API is used to query the alert list.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/search

Table 4-1 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-2 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.
content-type	Yes	String	Content type.

Table 4-3 Request body parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	The number of records on each page.
offset	No	Integer	Offset.
sort_by	No	String	Sorting field: create_time | update_time
order	No	String	Sorting order. Options: **DESC** and **ASC**.
from_date	No	String	Search start time, for example, 2023-02-20T00:00:00.000Z.
to_date	No	String	Search end time, for example, 2023-02-27T23:59:59.999Z.
condition	No	**condition** object	Search condition expression.

Table 4-4 condition

Parameter	Mandatory	Type	Description
conditions	No	Array of **conditions** objects	Expression list.
logics	No	Array of strings	Expression name list.

Table 4-5 conditions

Parameter	Mandatory	Type	Description
name	No	String	Expression name.
data	No	Array of strings	Expression content list.

Response Parameters

Status code: 200

Table 4-6 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-7 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
total	Integer	Total number of alerts.
limit	Integer	The number of records on each page.
offset	Integer	Offset.
success	Boolean	Successful or not.
data	Array of **ListAlertDetail** objects	Alert list.

Table 4-8 ListAlertDetail

Parameter	Type	Description
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
data_object	**ListAlertRsp** object	Alert entity information.
dataclass_ref	**dataclass_ref** object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an alert. The value is in UUID format and can contain a maximum of 36 characters.
type	String	Data type.
project_id	String	ID of the current project.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-9 ListAlertRsp

Parameter	Type	Description
version	String	Version of the data source of an alert. The value must be one officially released by the SSA service.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	String	ID of the account (domain_id) to whom the data is delivered and hosted.

Parameter	Type	Description
region_id	String	ID of the region where the account to whom the data is delivered and hosted.
workspace_id	String	ID of the current workspace.
labels	String	Tag (display only).
environment	**environment** object	Coordinates of the environment where the alert was generated.
data_source	**data_source** object	Data source reported for the first time.
first_observed_time	String	First discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
last_observed_time	String	Latest discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
arrive_time	String	Receiving time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
title	String	Alert title.
description	String	Alert description.
source_url	String	Alert URL, which points to the page of the current incident description in the data source product.
count	Integer	Incident occurrences.

Parameter	Type	Description
confidence	Integer	Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or problem. Value range: 0 to 100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.
severity	String	Severity level. Value range: Tips | Low | Medium | High | Fatal Note: **0**: Tips. No threats are found. **1**: Low. No actions are required for the threat. **2**: Medium. The threat needs to be handled but is not urgent. **3**: High. The threat must be handled preferentially. **4**: Fatal. The threat must be handled immediately to prevent further damage.
criticality	Integer	Criticality, which specifies the importance level of the resources involved in an incident. Value range: 0 to 100. **0** indicates that the resource is not critical, and **100** indicates that the resource is critical.
alert_type	**alert_type** object	Alert classification. For details, see the *Alert Type Definition*.
network_list	Array of **network_list** objects	Network information.
resource_list	Array of **resource_list** objects	Affected resources.
remediation	**remediation** object	Remedy measure.

Parameter	Type	Description
verification_state	String	Verification status, which identifies the accuracy of the incident. The options are as follows: **Unknown**: The incident is unknown. **True_Positive**: The incident is confirmed. **False_Positive**: The incident is a false positive. The default value is **Unknown**.
handle_status	String	Incident handling status. The options are as follows: **Open**: Default status. **Block** **Closed** The default value is **Open**.
sla	String	Closure time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
close_time	String	Closure time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
ipdrr_phase	String	Period/Handling phase No. **Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.

Parameter	Type	Description
chop_phase	String	Period/Handling phase No. **Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.
ppdr_phase	String	Period/Handling phase No. **Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.
simulation	String	Debugging field.
actor	String	Alert investigator.
owner	String	Owner and service owner.
creator	String	Creator.
close_reason	String	Closure reason. False detection Resolved Repeated Other
close_comment	String	Comment for the closure.
alert_list	Array of strings	Alert ID list, which is the list of alerts associated with alerts, incidents, or indicators.
incident_list	Array of strings	Incident ID list, which is the list of incidents associated with alerts, incidents, or indicators.
indicator_list	Array of strings	Indicator list, which is the list of indicators associated with alerts or indicators.
malware	**malware** object	Malware.
system_info	Object	System information.
process	Array of **process** objects	Process information.

Parameter	Type	Description
user_info	Array of **user_info** objects	User information.
file_info	Array of **file_info** objects	File information.
origin_id	String	Original ID of the alert incident. The value can contain a maximum of 128 characters.
ttd	Integer	Detection time. Unit: minute.
ttr	Integer	Response time. Unit: minute.
is_auto_closed	String	Auto close status. The value can be: **AutoClosed**: SOAR is automatically closed. **Manual**: It is closed manually.
system_alert_table	Object	Layout fields in the alerts list.

Table 4-10 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Account ID.
region_id	String	Region ID. **global** is returned for global services.
cross_workspace_id	String	Source workspace ID before data delivery. In the source workspace, the value is null. After data delivery, the value is the ID of the delegated user.
project_id	String	Project ID. The default value is null for global services.

Table 4-11 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows: **1**: Cloud service **2**: Third-party product **3**: Private product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source product is located. For details about the value range, see "Regions and Endpoints".
company_name	String	Name of the company to which the data source product belongs.
product_name	String	Name of the data source product.
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection model list.

Table 4-12 alert_type

Parameter	Type	Description
category	String	Category.
alert_type	String	Alert type.

Table 4-13 network_list

Parameter	Type	Description
direction	String	Direction. The value can be **IN** or **OUT**.
protocol	String	Protocol, including Layer 7 and Layer 4 protocols. Reference: IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Parameter	Type	Description
src_ip	String	Source IP address.
src_port	Integer	Source port. Value range: 0 - 65535.
src_domain	String	Source domain name.
src_geo	**src_geo** object	Geographical location of the source IP address.
dest_ip	String	Destination IP address.
dest_port	String	Destination port. Value range: 0 to 65535.
dest_domain	String	Destination domain name.
dest_geo	**dest_geo** object	Geographical location of the destination IP address.

Table 4-14 src_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-15 dest_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-16 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type, which is the same as the **type** field in the RMS service.
provider	String	Cloud service name, which is the same as the **provider** field in the RMS service.
region_id	String	Region. Enter the value based on the cloud region ID.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the project to which the resource belongs, in UUID format.
ep_id	String	Enterprise project ID.
ep_name	String	Enterprise project name.
tags	String	Resource tags. 1. A maximum of 50 key-value pairs are supported. 2. The value can contain a maximum of 255 characters, including letters, digits, spaces, and special characters (+, -, =, ., _, :, /,@).

Table 4-17 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.
url	String	URL, which points to the general handling details for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-18 malware

Parameter	Type	Description
malware_family	String	Malicious family.
malware_class	String	Malware classification.

Table 4-19 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Path of the process execution file.
process_pid	Integer	Process ID.
process_uid	Integer	User ID associated with the process.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.
process_parent_path	String	Path of the parent process execution file.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	User ID associated with the parent process.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Path of the subprocess execution file.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	User ID associated with the subprocess.
process_child_cmdline	String	Subprocess command line.

Parameter	Type	Description
process_launche_time	String	Process start time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
process_terminate_time	String	Process end time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Table 4-20 user_info

Parameter	Type	Description
user_id	String	User ID (UID).
user_name	String	Username.

Table 4-21 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File content.
file_new_path	String	New file path/name.
file_hash	String	File hashes.
file_md5	String	File MD5 value.
file_sha256	String	SHA256 value of the file.
file_attr	String	File attributes.

Table 4-22 dataclass_ref

Parameter	Type	Description
id	String	Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.

Parameter	Type	Description
name	String	Data class name.

Status code: 400

Table 4-23 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-24 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Query the alert list. Time range: January 20, 2024 to January 26, 2024. Alert severity: Medium. Handling status: Open. Sorting order: By creation time in descending order. Page size: 10 records on each page. Return only the first page.

```
{
  "limit" : 10,
  "offset" : 0,
  "sort_by" : "create_time",
  "order" : "DESC",
  "condition" : {
    "conditions" : [ {
      "name" : "severity",
      "data" : [ "severity", "=", "Medium" ]
    }, {
      "name" : "handle_status",
      "data" : [ "handle_status", "=", "Open" ]
    } ],
    "logics" : [ "severity", "and", "handle_status" ]
  },
  "from_date" : "2024-01-20T00:00:00.000Z+0800",
  "to_date" : "2024-01-26T23:59:59.999Z+0800"
}
```

Example Responses

Status code: 200

Response body of the request for querying the alert list.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
```



```
"message" : "Error message",
"total" : 41,
"limit" : 2,
"offset" : 1,
"success" : true,
"data" : [ {
  "data_object" : {
    "version" : "1.0",
    "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "environment" : {
      "vendor_type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "data_source" : {
      "source_type" : 3,
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "first_observed_time" : "2021-01-30T23:00:00Z+0800",
    "last_observed_time" : "2021-01-30T23:00:00Z+0800",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "arrive_time" : "2021-01-30T23:00:00Z+0800",
    "title" : "MyXXX",
    "description" : "This my XXXX",
    "source_url" : "http://xxx",
    "count" : 4,
    "confidence" : 4,
    "severity" : "TIPS",
    "criticality" : 4,
    "alert_type" : { },
    "network_list" : [ {
      "direction" : {
        "IN" : null
      },
      "protocol" : "TCP",
      "src_ip" : "192.168.0.1",
      "src_port" : "1",
      "src_domain" : "xxx",
      "dest_ip" : "192.168.0.1",
      "dest_port" : "1",
      "dest_domain" : "xxx",
      "src_geo" : {
        "latitude" : 90,
        "longitude" : 180
      },
      "dest_geo" : {
        "latitude" : 90,
        "longitude" : 180
      }
    } ],
    "resource_list" : [ {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_name" : "MyXXX",
      "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    } ],
    "remediation" : {
      "recommendation" : "MyXXX",
      "url" : "MyXXX"
    },
```



```
    "verification_state" : "**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**.",
    "handle_status" : "**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is **Open**.",
    "sla" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.",
    "simulation" : "false",
    "actor" : "Tom",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "False positive; Resolved; Duplicate; Others",
    "close_comment" : "False positive; Resolved; Duplicate; Others",
    "alert_list" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f", "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
    "incident_list" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f", "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
    "indicator_list" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f", "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "Malicious memory occupation."
    },
    "system_info" : { },
    "process" : [ {
      "process_name" : "MyXXX",
      "process_path" : "MyXXX",
      "process_pid" : 123,
      "process_uid" : 123,
      "process_cmdline" : "MyXXX"
    } ],
    "user_info" : [ {
      "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "user_name" : "MyXXX"
    } ],
    "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
    } ],
    "labels" : "MyXXX",
    "origin_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ttd" : 1,
    "ttr" : 1,
    "is_auto_closed" : "Manual",
    "system_alert_table" : { },
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "id" : "MyXXX",
  "version" : 123,
  "format_version" : 123,
  "dataclass_ref" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX"
  }
 } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Query the alert list. Time range: January 20, 2024 to January 26, 2024. Alert severity: Medium. Handling status: Open. Sorting order: By creation time in descending order. Page size: 10 records on each page. Return only the first page.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class ListAlertsSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListAlertsRequest request = new ListAlertsRequest();
        request.withWorkspaceId("{workspace_id}");
        DataobjectSearch body = new DataobjectSearch();
        List<String> listConditionLogics = new ArrayList<>();
        listConditionLogics.add("severity");
        listConditionLogics.add("and");
        listConditionLogics.add("handle_status");
        List<String> listConditionsData = new ArrayList<>();
        listConditionsData.add("handle_status");
        listConditionsData.add("=");
        listConditionsData.add("Open");
        List<String> listConditionsData1 = new ArrayList<>();
        listConditionsData1.add("severity");
        listConditionsData1.add("=");
        listConditionsData1.add("Medium");
        List<DataobjectSearchConditionConditions> listConditionConditions = new ArrayList<>();
        listConditionConditions.add(
            new DataobjectSearchConditionConditions()
                .withName("severity")
                .withData(listConditionsData1)
        );
        listConditionConditions.add(
```



```
            new DataobjectSearchConditionConditions()
                .withName("handle_status")
                .withData(listConditionsData)
        );
        DataobjectSearchCondition conditionbody = new DataobjectSearchCondition();
        conditionbody.withConditions(listConditionConditions)
            .withLogics(listConditionLogics);
        body.withCondition(conditionbody);
        body.withToDate("2024-01-26T23:59:59.999Z+0800");
        body.withFromDate("2024-01-20T00:00:00.000Z+0800");
        body.withOrder(DataobjectSearch.OrderEnum.fromValue("DESC"));
        body.withSortBy("create_time");
        body.withOffset(0);
        body.withLimit(10);
        request.withBody(body);
        try {
            ListAlertsResponse response = client.listAlerts(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 alert list. Time range: January 20, 2024 to January 26, 2024. Alert severity: Medium. Handling status: Open. Sorting order: By creation time in descending order. Page size: 10 records on each page. Return only the first page.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAlertsRequest()
        request.workspace_id = "{workspace_id}"
        listLogicsCondition = [
            "severity",
```



```
        "and",
        "handle_status"
    ]
    listDataConditions = [
        "handle_status",
        "=",
        "Open"
    ]
    listDataConditions1 = [
        "severity",
        "=",
        "Medium"
    ]
    listConditionsCondition = [
        DataobjectSearchConditionConditions(
            name="severity",
            data=listDataConditions1
        ),
        DataobjectSearchConditionConditions(
            name="handle_status",
            data=listDataConditions
        )
    ]
    conditionbody = DataobjectSearchCondition(
        conditions=listConditionsCondition,
        logics=listLogicsCondition
    )
    request.body = DataobjectSearch(
        condition=conditionbody,
        to_date="2024-01-26T23:59:59.999Z+0800",
        from_date="2024-01-20T00:00:00.000Z+0800",
        order="DESC",
        sort_by="create_time",
        offset=0,
        limit=10
    )
    response = client.list_alerts(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 alert list. Time range: January 20, 2024 to January 26, 2024. Alert severity: Medium. Handling status: Open. Sorting order: By creation time in descending order. Page size: 10 records on each page. Return only the first page.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAlertsRequest{}
    request.WorkspaceId = "{workspace_id}"
    var listLogicsCondition = []string{
        "severity",
        "and",
        "handle_status",
    }
    var listDataConditions = []string{
        "handle_status",
        "=",
        "Open",
    }
    var listDataConditions1 = []string{
        "severity",
        "=",
        "Medium",
    }
    nameConditions:= "severity"
    nameConditions1:= "handle_status"
    var listConditionsCondition = []model.DataobjectSearchConditionConditions{
        {
            Name: &nameConditions,
            Data: &listDataConditions1,
        },
        {
            Name: &nameConditions1,
            Data: &listDataConditions,
        },
    }
    conditionbody := &model.DataobjectSearchCondition{
        Conditions: &listConditionsCondition,
        Logics: &listLogicsCondition,
    }
    toDateDataobjectSearch:= "2024-01-26T23:59:59.999Z+0800"
    fromDateDataobjectSearch:= "2024-01-20T00:00:00.000Z+0800"
    orderDataobjectSearch:= model.GetDataobjectSearchOrderEnum().DESC
    sortByDataobjectSearch:= "create_time"
    offsetDataobjectSearch:= int32(0)
    limitDataobjectSearch:= int32(10)
    request.Body = &model.DataobjectSearch{
        Condition: conditionbody,
        ToDate: &toDateDataobjectSearch,
        FromDate: &fromDateDataobjectSearch,
        Order: &orderDataobjectSearch,
        SortBy: &sortByDataobjectSearch,
        Offset: &offsetDataobjectSearch,
        Limit: &limitDataobjectSearch,
    }
    response, err := client.ListAlerts(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	Response body of the request for querying the alert list.
400	Response body for an alert list query error.

Error Codes

See **Error Codes**.

4.1.2 Creating an Alert

Function

This API is used to create an alert.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts

Table 4-25 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-26 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.
content-type	Yes	String	Content type.

Table 4-27 Request body parameters

Parameter	Mandatory	Type	Description
data_object	Yes	**Alert** object	Alert entity information.

Table 4-28 Alert

Parameter	Mandatory	Type	Description
version	No	String	Version of the data source of an alert. The value must be one officially released by the SSA service.
id	No	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	No	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	No	String	ID of the region where the account to whom the data is delivered and hosted.
workspace_id	No	String	ID of the current workspace.
labels	No	String	Tag (display only).
environment	No	**environment** object	Coordinates of the environment where the alert was generated.

Parameter	Mandatory	Type	Description
data_source	No	data_source object	Data source reported for the first time.
first_observed_time	No	String	First discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
last_observed_time	No	String	Latest discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
create_time	No	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
arrive_time	No	String	Receiving time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
title	No	String	Alert title.
description	No	String	Alert description.
source_url	No	String	Alert URL, which points to the page of the current incident description in the data source product.
count	No	Integer	Incident occurrences.

Parameter	Mandatory	Type	Description
confidence	No	Integer	Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or problem. Value range: 0 to 100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.
severity	No	String	Severity level. Value range: Tips | Low | Medium | High | Fatal Note: **0**: Tips. No threats are found. **1**: Low. No actions are required for the threat. **2**: Medium. The threat needs to be handled but is not urgent. **3**: High. The threat must be handled preferentially. **4**: Fatal. The threat must be handled immediately to prevent further damage.
criticality	No	Integer	Criticality, which specifies the importance level of the resources involved in an incident. Value range: 0 to 100. **0** indicates that the resource is not critical, and **100** indicates that the resource is critical.
alert_type	No	**alert_type** object	Alert classification. For details, see the *Alert Type Definition*.
network_list	No	Array of **network_list** objects	Network information.
resource_list	No	Array of **resource_list** objects	Affected resources.
remediation	No	**remediation** object	Remedy measure.

Parameter	Mandatory	Type	Description
verification_state	No	String	Event verification status, which identifies the accuracy of the incident. The options are as follows: **Unknown**: The incident is unknown. **True_Positive**: The incident is confirmed. **False_Positive**: The incident is a false positive. The default value is **Unknown**.
handle_status	No	String	Incident handling status. The options are as follows: **Open**: Default status. **Block** **Closed** The default value is **Open**.
sla	No	Integer	Closure time: The deadline by which the incident must be resolved. Unit: hour.
update_time	No	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
close_time	No	String	Closure time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Parameter	Mandatory	Type	Description
ipdrr_phase	No	String	Period/Handling phase No. **Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.
simulation	No	String	Debugging field.
actor	No	String	Alert investigator.
owner	No	String	Owner and service owner.
creator	No	String	Creator.
close_reason	No	String	Closure reason. False detection Resolved Repeated Other
close_comment	No	String	Comment for the closure.
malware	No	**malware** object	Malware.
system_info	No	Object	System information.
process	No	Array of **process** objects	Process information.
user_info	No	Array of **user_info** objects	User information.
file_info	No	Array of **file_info** objects	File information.
system_alert_table	No	Object	Layout fields in the alert list.

Table 4-29 environment

Parameter	Mandatory	Type	Description
vendor_type	No	String	Environment provider.
domain_id	No	String	Account ID.
region_id	No	String	Region ID. **global** is returned for global services.
cross_workspace_id	No	String	Source workspace ID before data delivery. In the source workspace, the value is null. After data delivery, the value is the ID of the delegated user.
project_id	No	String	Project ID. The default value is null for global services.

Table 4-30 data_source

Parameter	Mandatory	Type	Description
source_type	No	Integer	Data source type. The options are as follows: **1**: Cloud service **2**: Third-party product **3**: Private product
domain_id	No	String	Account ID to which the data source product belongs.
project_id	No	String	ID of the project to which the data source product belongs.
region_id	No	String	Region where the data source product is located. For details about the value range, see "Regions and Endpoints".
company_name	No	String	Name of the company to which the data source product belongs.
product_name	No	String	Name of the data source product.
product_feature	No	String	Name of the feature of the product that detects the incident.
product_module	No	String	Threat detection model list.

Table 4-31 alert_type

Parameter	Mandatory	Type	Description
category	No	String	Category.
alert_type	No	String	Alert type.

Table 4-32 network_list

Parameter	Mandatory	Type	Description
direction	No	String	Direction. The value can be **IN** or **OUT**.
protocol	No	String	Protocol, including Layer 7 and Layer 4 protocols. Reference: IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml
src_ip	No	String	Source IP address.
src_port	No	Integer	Source port. Value range: 0 - 65535.
src_domain	No	String	Source domain name.
src_geo	No	**src_geo** object	Geographical location of the source IP address.
dest_ip	No	String	Destination IP address.
dest_port	No	String	Destination port. Value range: 0 to 65535.
dest_domain	No	String	Destination domain name.
dest_geo	No	**dest_geo** object	Geographical location of the destination IP address.

Table 4-33 src_geo

Parameter	Mandatory	Type	Description
latitude	No	Number	Latitude.
longitude	No	Number	Longitude.
city_code	No	String	City Code.

Parameter	Mandatory	Type	Description
country_code	No	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-34 dest_geo

Parameter	Mandatory	Type	Description
latitude	No	Number	Latitude.
longitude	No	Number	Longitude.
city_code	No	String	City Code.
country_code	No	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-35 resource_list

Parameter	Mandatory	Type	Description
id	No	String	Cloud service resource ID.
name	No	String	Resource name.
type	No	String	Resource type, which is the same as the **type** field in the RMS service.
provider	No	String	Cloud service name, which is the same as the **provider** field in the RMS service.
region_id	No	String	Region. Enter the value based on the cloud region ID.
domain_id	No	String	ID of the account to which the resource belongs, in UUID format.
project_id	No	String	ID of the project to which the resource belongs, in UUID format.
ep_id	No	String	Enterprise project ID.
ep_name	No	String	Enterprise project name.

Parameter	Mandatory	Type	Description
tags	No	String	Resource tags. 1. A maximum of 50 key-value pairs are supported. 2. The value can contain a maximum of 255 characters, including letters, digits, spaces, and special characters (+, -, =, ., _, :, /,@).

Table 4-36 remediation

Parameter	Mandatory	Type	Description
recommendation	No	String	Recommended solution.
url	No	String	URL, which points to the general handling details for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-37 malware

Parameter	Mandatory	Type	Description
malware_family	No	String	Malicious family.
malware_class	No	String	Malware classification.

Table 4-38 process

Parameter	Mandatory	Type	Description
process_name	No	String	Process name.
process_path	No	String	Path of the process execution file.
process_pid	No	Integer	Process ID.
process_uid	No	Integer	User ID associated with the process.

Parameter	Mandatory	Type	Description
process_cmdline	No	String	Process command line.
process_parent_name	No	String	Parent process name.
process_parent_path	No	String	Path of the parent process execution file.
process_parent_pid	No	Integer	Parent process ID.
process_parent_uid	No	Integer	User ID associated with the parent process.
process_parent_cmdline	No	String	Parent process command line.
process_child_name	No	String	Subprocess name.
process_child_path	No	String	Path of the subprocess execution file.
process_child_pid	No	Integer	Subprocess ID.
process_child_uid	No	Integer	User ID associated with the subprocess.
process_child_cmdline	No	String	Subprocess command line.
process_launche_time	No	String	Process start time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
process_terminate_time	No	String	Process end time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Table 4-39 user_info

Parameter	Mandatory	Type	Description
user_id	No	String	User ID (UID).
user_name	No	String	Username.

Table 4-40 file_info

Parameter	Mandatory	Type	Description
file_path	No	String	File path/name.
file_content	No	String	File content.
file_new_path	No	String	New file path/name.
file_hash	No	String	File hash value.
file_md5	No	String	File MD5 value.
file_sha256	No	String	SHA256 value of the file.
file_attr	No	String	File attributes.

Response Parameters

Status code: 200

Table 4-41 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-42 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**AlertDetail** object	Alert details object.

Table 4-43 AlertDetail

Parameter	Type	Description
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
data_object	**Alert** object	Alert entity information.
dataclass_ref	**dataclass_ref** object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
type	String	Data type.
project_id	String	ID of the current project.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-44 Alert

Parameter	Type	Description
version	String	Version of the data source of an alert. The value must be one officially released by the SSA service.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	String	ID of the account (domain_id) to whom the data is delivered and hosted.

Parameter	Type	Description
region_id	String	ID of the region where the account to whom the data is delivered and hosted.
workspace_id	String	ID of the current workspace.
labels	String	Tag (display only).
environment	**environment** object	Coordinates of the environment where the alert was generated.
data_source	**data_source** object	Data source reported for the first time.
first_observed_time	String	First discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
last_observed_time	String	Latest discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
arrive_time	String	Receiving time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
title	String	Alert title.
description	String	Alert description.
source_url	String	Alert URL, which points to the page of the current incident description in the data source product.
count	Integer	Incident occurrences.

Parameter	Type	Description
confidence	Integer	Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or problem. Value range: 0 to 100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.
severity	String	Severity level. Value range: Tips | Low | Medium | High | Fatal Note: **0**: Tips. No threats are found. **1**: Low. No actions are required for the threat. **2**: Medium. The threat needs to be handled but is not urgent. **3**: High. The threat must be handled preferentially. **4**: Fatal. The threat must be handled immediately to prevent further damage.
criticality	Integer	Criticality, which specifies the importance level of the resources involved in an incident. Value range: 0 to 100. **0** indicates that the resource is not critical, and **100** indicates that the resource is critical.
alert_type	**alert_type** object	Alert classification. For details, see the *Alert Type Definition*.
network_list	Array of **network_list** objects	Network information.
resource_list	Array of **resource_list** objects	Affected resources.
remediation	**remediation** object	Remedy measure.

Parameter	Type	Description
verification_state	String	Event verification status, which identifies the accuracy of the incident. The options are as follows: **Unknown**: The incident is unknown. **True_Positive**: The incident is confirmed. **False_Positive**: The incident is a false positive. The default value is **Unknown**.
handle_status	String	Incident handling status. The options are as follows: **Open**: Default status. **Block** **Closed** The default value is **Open**.
sla	Integer	Closure time: The deadline by which the incident must be resolved. Unit: hour.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
close_time	String	Closure time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
ipdrr_phase	String	Period/Handling phase No. **Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.
simulation	String	Debugging field.
actor	String	Alert investigator.
owner	String	Owner and service owner.

Parameter	Type	Description
creator	String	Creator.
close_reason	String	Closure reason. False detection Resolved Repeated Other
close_comment	String	Comment for the closure.
malware	**malware** object	Malware.
system_info	Object	System information.
process	Array of **process** objects	Process information.
user_info	Array of **user_info** objects	User information.
file_info	Array of **file_info** objects	File information.
system_alert_table	Object	Layout fields in the alert list.

Table 4-45 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Account ID.
region_id	String	Region ID. **global** is returned for global services.
cross_workspace_id	String	Source workspace ID before data delivery. In the source workspace, the value is null. After data delivery, the value is the ID of the delegated user.
project_id	String	Project ID. The default value is null for global services.

Table 4-46 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows: **1**: Cloud service **2**: Third-party product **3**: Private product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source product is located. For details about the value range, see "Regions and Endpoints".
company_name	String	Name of the company to which the data source product belongs.
product_name	String	Name of the data source product.
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection model list.

Table 4-47 alert_type

Parameter	Type	Description
category	String	Category.
alert_type	String	Alert type.

Table 4-48 network_list

Parameter	Type	Description
direction	String	Direction. The value can be **IN** or **OUT**.
protocol	String	Protocol, including Layer 7 and Layer 4 protocols. Reference: IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Parameter	Type	Description
src_ip	String	Source IP address.
src_port	Integer	Source port. Value range: 0 - 65535.
src_domain	String	Source domain name.
src_geo	**src_geo** object	Geographical location of the source IP address.
dest_ip	String	Destination IP address.
dest_port	String	Destination port. Value range: 0 to 65535.
dest_domain	String	Destination domain name.
dest_geo	**dest_geo** object	Geographical location of the destination IP address.

Table 4-49 src_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-50 dest_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-51 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type, which is the same as the **type** field in the RMS service.
provider	String	Cloud service name, which is the same as the **provider** field in the RMS service.
region_id	String	Region. Enter the value based on the cloud region ID.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the project to which the resource belongs, in UUID format.
ep_id	String	Enterprise project ID.
ep_name	String	Enterprise project name.
tags	String	Resource tags. 1. A maximum of 50 key-value pairs are supported. 2. The value can contain a maximum of 255 characters, including letters, digits, spaces, and special characters (+, -, =, ., _, :, /,@).

Table 4-52 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.
url	String	URL, which points to the general handling details for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-53 malware

Parameter	Type	Description
malware_family	String	Malicious family.
malware_class	String	Malware classification.

Table 4-54 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Path of the process execution file.
process_pid	Integer	Process ID.
process_uid	Integer	User ID associated with the process.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.
process_parent_path	String	Path of the parent process execution file.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	User ID associated with the parent process.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Path of the subprocess execution file.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	User ID associated with the subprocess.
process_child_cmdline	String	Subprocess command line.

Parameter	Type	Description
process_launche_time	String	Process start time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
process_terminate_time	String	Process end time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Table 4-55 user_info

Parameter	Type	Description
user_id	String	User ID (UID).
user_name	String	Username.

Table 4-56 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File content.
file_new_path	String	New file path/name.
file_hash	String	File hash value.
file_md5	String	File MD5 value.
file_sha256	String	SHA256 value of the file.
file_attr	String	File attributes.

Table 4-57 dataclass_ref

Parameter	Type	Description
id	String	Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.

Parameter	Type	Description
name	String	Data class name.

Status code: 400

Table 4-58 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-59 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Create an alert. Set the alert name to MyXXX, Tag to MyXXX, URL to http://xxx, number of occurrence times to 4, confidence to 4, and severity to tips.

```
{
  "data_object" : {
    "version" : "1.0",
    "environment" : {
      "vendor_type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "data_source" : {
      "source_type" : 3,
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "product_name" : "test",
      "product_feature" : "test"
    },
    "first_observed_time" : "2021-01-30T23:00:00Z+0800",
    "last_observed_time" : "2021-01-30T23:00:00Z+0800",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "arrive_time" : "2021-01-30T23:00:00Z+0800",
    "title" : "MyXXX",
    "labels" : "MyXXX",
    "description" : "This my XXXX",
    "source_url" : "http://xxx",
    "count" : 4,
    "confidence" : 4,
    "severity" : "TIPS",
    "criticality" : 4,
    "alert_type" : { },
```



```
  "network_list" : [ {
    "direction" : {
      "IN" : null
    },
    "protocol" : "TCP",
    "src_ip" : "192.168.0.1",
    "src_port" : "1",
    "src_domain" : "xxx",
    "dest_ip" : "192.168.0.1",
    "dest_port" : "1",
    "dest_domain" : "xxx",
    "src_geo" : {
      "latitude" : 90,
      "longitude" : 180
    },
    "dest_geo" : {
      "latitude" : 90,
      "longitude" : 180
    }
  } ],
  "resource_list" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "type" : "MyXXX",
    "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ep_name" : "MyXXX",
    "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  } ],
  "remediation" : {
    "recommendation" : "MyXXX",
    "url" : "MyXXX"
  },
  "verification_state" : "**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**.",
  "handle_status" : "**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is **Open**.",
  "sla" : 60000,
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "close_time" : "2021-01-30T23:00:00Z+0800",
  "ipdrr_phase" : "**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.",
  "simulation" : "false",
  "actor" : "Tom",
  "owner" : "MyXXX",
  "creator" : "MyXXX",
  "close_reason" : "False positive; Resolved; Duplicate; Others",
  "close_comment" : "False positive; Resolved; Duplicate; Others",
  "malware" : {
    "malware_family" : "family",
    "malware_class" : "Malicious memory occupation."
  },
  "system_info" : { },
  "process" : [ {
    "process_name" : "MyXXX",
    "process_path" : "MyXXX",
    "process_pid" : 123,
    "process_uid" : 123,
    "process_cmdline" : "MyXXX"
  } ],
  "user_info" : [ {
    "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "user_name" : "MyXXX"
  } ],
  "file_info" : [ {
    "file_path" : "MyXXX",
    "file_content" : "MyXXX",
```

```
    "file_new_path" : "MyXXX",
    "file_hash" : "MyXXX",
    "file_md5" : "MyXXX",
    "file_sha256" : "MyXXX",
    "file_attr" : "MyXXX"
   } ],
   "system_alert_table" : { },
   "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
   "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  }
}
```

Example Responses

Status code: 200

Response body of requests for creating alerts.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "data_object" : {
      "version" : "1.0",
      "environment" : {
        "vendor_type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "data_source" : {
        "source_type" : 3,
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "first_observed_time" : "2021-01-30T23:00:00Z+0800",
      "last_observed_time" : "2021-01-30T23:00:00Z+0800",
      "create_time" : "2021-01-30T23:00:00Z+0800",
      "arrive_time" : "2021-01-30T23:00:00Z+0800",
      "title" : "MyXXX",
      "description" : "This my XXXX",
      "source_url" : "http://xxx",
      "count" : 4,
      "confidence" : 4,
      "severity" : "TIPS",
      "criticality" : 4,
      "alert_type" : { },
      "network_list" : [ {
        "direction" : {
          "IN" : null
        },
        "protocol" : "TCP",
        "src_ip" : "192.168.0.1",
        "src_port" : "1",
        "src_domain" : "xxx",
        "dest_ip" : "192.168.0.1",
        "dest_port" : "1",
        "dest_domain" : "xxx",
        "src_geo" : {
          "latitude" : 90,
          "longitude" : 180
        },
        "dest_geo" : {
          "latitude" : 90,
          "longitude" : 180
        }
      } ],
      "resource_list" : [ {
```



```
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_name" : "MyXXX",
      "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    } ],
    "remediation" : {
      "recommendation" : "MyXXX",
      "url" : "MyXXX"
    },
    "verification_state" : "**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**.",
    "handle_status" : "**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is **Open**.",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.",
    "simulation" : "false",
    "actor" : "Tom",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "False positive; Resolved; Duplicate; Others",
    "close_comment" : "False positive; Resolved; Duplicate; Others",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "Malicious memory occupation."
    },
    "system_info" : { },
    "process" : [ {
      "process_name" : "MyXXX",
      "process_path" : "MyXXX",
      "process_pid" : 123,
      "process_uid" : 123,
      "process_cmdline" : "MyXXX"
    } ],
    "user_info" : [ {
      "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "user_name" : "MyXXX"
    } ],
    "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
    } ],
    "system_alert_table" : { },
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "id" : "MyXXX",
  "version" : 123,
  "format_version" : 123,
  "dataclass_ref" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX"
  }
```

```
 }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Create an alert. Set the alert name to MyXXX, Tag to MyXXX, URL to http://xxx, number of occurrence times to 4, confidence to 4, and severity to tips.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class CreateAlertSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateAlertRequest request = new CreateAlertRequest();
        request.withWorkspaceId("{workspace_id}");
        CreateAlertRequestBody body = new CreateAlertRequestBody();
        List<AlertFileInfo> listDataObjectFileInfo = new ArrayList<>();
        listDataObjectFileInfo.add(
            new AlertFileInfo()
                .withFilePath("MyXXX")
                .withFileContent("MyXXX")
                .withFileNewPath("MyXXX")
                .withFileHash("MyXXX")
                .withFileMd5("MyXXX")
                .withFileSha256("MyXXX")
                .withFileAttr("MyXXX")
        );
        List<AlertUserInfo> listDataObjectUserInfo = new ArrayList<>();
        listDataObjectUserInfo.add(
            new AlertUserInfo()
                .withUserId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withUserName("MyXXX")
        );
```



```
List<AlertProcess> listDataObjectProcess = new ArrayList<>();
listDataObjectProcess.add(
    new AlertProcess()
        .withProcessName("MyXXX")
        .withProcessPath("MyXXX")
        .withProcessPid(123)
        .withProcessUid(123)
        .withProcessCmdline("MyXXX")
);
AlertMalware malwareDataObject = new AlertMalware();
malwareDataObject.withMalwareFamily("family")
    .withMalwareClass("Malicious memory occupation.");
AlertRemediation remediationDataObject = new AlertRemediation();
remediationDataObject.withRecommendation("MyXXX")
    .withUrl("MyXXX");
List<AlertResourceList> listDataObjectResourceList = new ArrayList<>();
listDataObjectResourceList.add(
    new AlertResourceList()
        .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withName("MyXXX")
        .withType("MyXXX")
        .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withEpId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withEpName("MyXXX")
        .withTags("909494e3-558e-46b6-a9eb-07a8e18ca62f")
);
AlertDestGeo destGeoNetworkList = new AlertDestGeo();
destGeoNetworkList.withLatitude(java.math.BigDecimal.valueOf(90))
    .withLongitude(java.math.BigDecimal.valueOf(180));
AlertSrcGeo srcGeoNetworkList = new AlertSrcGeo();
srcGeoNetworkList.withLatitude(java.math.BigDecimal.valueOf(90))
    .withLongitude(java.math.BigDecimal.valueOf(180));
List<AlertNetworkList> listDataObjectNetworkList = new ArrayList<>();
listDataObjectNetworkList.add(
    new AlertNetworkList()
        .withDirection(AlertNetworkList.DirectionEnum.fromValue("{}"))
        .withProtocol("TCP")
        .withSrcIp("192.168.0.1")
        .withSrcPort(1)
        .withSrcDomain("xxx")
        .withSrcGeo(srcGeoNetworkList)
        .withDestIp("192.168.0.1")
        .withDestPort("1")
        .withDestDomain("xxx")
        .withDestGeo(destGeoNetworkList)
);
AlertDataSource dataSourceDataObject = new AlertDataSource();
dataSourceDataObject.withSourceType(3)
    .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withProductName("test")
    .withProductFeature("test");
AlertEnvironment environmentDataObject = new AlertEnvironment();
environmentDataObject.withVendorType("MyXXX")
    .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
Alert dataObjectbody = new Alert();
dataObjectbody.withVersion("1.0")
    .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withWorkspaceId("909494e3-558e-46b6-a9eb-07a8e18ca620")
    .withLabels("MyXXX")
    .withEnvironment(environmentDataObject)
    .withDataSource(dataSourceDataObject)
    .withFirstObservedTime("2021-01-30T23:00:00Z+0800")
    .withLastObservedTime("2021-01-30T23:00:00Z+0800")
```



```
            .withCreateTime("2021-01-30T23:00:00Z+0800")
            .withArriveTime("2021-01-30T23:00:00Z+0800")
            .withTitle("MyXXX")
            .withDescription("This my XXXX")
            .withSourceUrl("http://xxx")
            .withCount(4)
            .withConfidence(4)
            .withSeverity(Alert.SeverityEnum.fromValue("TIPS"))
            .withCriticality(4)
            .withNetworkList(listDataObjectNetworkList)
            .withResourceList(listDataObjectResourceList)
            .withRemediation(remediationDataObject)
            .withVerificationState(Alert.VerificationStateEnum.fromValue("**Unknown**: Unknown;
**True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**."))
            .withHandleStatus(Alert.HandleStatusEnum.fromValue("**Open**: Open; **Block**: Pending;
**Closed**: Closed. The default value is **Open**."))
            .withSla(60000)
            .withUpdateTime("2021-01-30T23:00:00Z+0800")
            .withCloseTime("2021-01-30T23:00:00Z+0800")
            .withIpdrrPhase(Alert.IpdrrPhaseEnum.fromValue("**Preparation**: Preparation stage. **Detection
and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication,
and recovery stage. **Post-Incident-Activity**: Post-incident activity stage."))
            .withSimulation("false")
            .withActor("Tom")
            .withOwner("MyXXX")
            .withCreator("MyXXX")
            .withCloseReason(Alert.CloseReasonEnum.fromValue("False positive; Resolved; Duplicate; Others"))
            .withCloseComment("False positive; Resolved; Duplicate; Others")
            .withMalware(malwareDataObject)
            .withSystemInfo(new Object())
            .withProcess(listDataObjectProcess)
            .withUserInfo(listDataObjectUserInfo)
            .withFileInfo(listDataObjectFileInfo)
            .withSystemAlertTable(new Object());
        body.withDataObject(dataObjectbody);
        request.withBody(body);
        try {
            CreateAlertResponse response = client.createAlert(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 an alert. Set the alert name to MyXXX, Tag to MyXXX, URL to http://xxx, number of occurrence times to 4, confidence to 4, and severity to tips.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateAlertRequest()
        request.workspace_id = "{workspace_id}"
        listFileInfoDataObject = [
            AlertFileInfo(
                file_path="MyXXX",
                file_content="MyXXX",
                file_new_path="MyXXX",
                file_hash="MyXXX",
                file_md5="MyXXX",
                file_sha256="MyXXX",
                file_attr="MyXXX"
            )
        ]
        listUserInfoDataObject = [
            AlertUserInfo(
                user_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
                user_name="MyXXX"
            )
        ]
        listProcessDataObject = [
            AlertProcess(
                process_name="MyXXX",
                process_path="MyXXX",
                process_pid=123,
                process_uid=123,
                process_cmdline="MyXXX"
            )
        ]
        malwareDataObject = AlertMalware(
            malware_family="family",
            malware_class="Malicious memory occupation."
        )
        remediationDataObject = AlertRemediation(
            recommendation="MyXXX",
            url="MyXXX"
        )
        listResourceListDataObject = [
            AlertResourceList(
                id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
                name="MyXXX",
                type="MyXXX",
                region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
                domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
                project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
                ep_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
                ep_name="MyXXX",
                tags="909494e3-558e-46b6-a9eb-07a8e18ca62f"
            )
        ]
        destGeoNetworkList = AlertDestGeo(
            latitude=90,
            longitude=180
        )
        srcGeoNetworkList = AlertSrcGeo(
```



```
        latitude=90,
        longitude=180
    )
    listNetworkListDataObject = [
        AlertNetworkList(
            direction="{}",
            protocol="TCP",
            src_ip="192.168.0.1",
            src_port=1,
            src_domain="xxx",
            src_geo=srcGeoNetworkList,
            dest_ip="192.168.0.1",
            dest_port="1",
            dest_domain="xxx",
            dest_geo=destGeoNetworkList
        )
    ]
    dataSourceDataObject = AlertDataSource(
        source_type=3,
        domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        product_name="test",
        product_feature="test"
    )
    environmentDataObject = AlertEnvironment(
        vendor_type="MyXXX",
        domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f"
    )
    dataObjectbody = Alert(
        version="1.0",
        id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        workspace_id="909494e3-558e-46b6-a9eb-07a8e18ca620",
        labels="MyXXX",
        environment=environmentDataObject,
        data_source=dataSourceDataObject,
        first_observed_time="2021-01-30T23:00:00Z+0800",
        last_observed_time="2021-01-30T23:00:00Z+0800",
        create_time="2021-01-30T23:00:00Z+0800",
        arrive_time="2021-01-30T23:00:00Z+0800",
        title="MyXXX",
        description="This my XXXX",
        source_url="http://xxx",
        count=4,
        confidence=4,
        severity="TIPS",
        criticality=4,
        network_list=listNetworkListDataObject,
        resource_list=listResourceListDataObject,
        remediation=remediationDataObject,
        verification_state="**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**.",
        handle_status="**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is **Open**.",
        sla=60000,
        update_time="2021-01-30T23:00:00Z+0800",
        close_time="2021-01-30T23:00:00Z+0800",
        ipdrr_phase="**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.",
        simulation="false",
        actor="Tom",
        owner="MyXXX",
        creator="MyXXX",
        close_reason="False positive; Resolved; Duplicate; Others",
        close_comment="False positive; Resolved; Duplicate; Others",
        malware=malwareDataObject,
```



```
            system_info={},
            process=listProcessDataObject,
            user_info=listUserInfoDataObject,
            file_info=listFileInfoDataObject,
            system_alert_table={}
        )
        request.body = CreateAlertRequestBody(
            data_object=dataObjectbody
        )
        response = client.create_alert(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 alert. Set the alert name to MyXXX, Tag to MyXXX, URL to http://xxx, number of occurrence times to 4, confidence to 4, and severity to tips.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateAlertRequest{}
    request.WorkspaceId = "{workspace_id}"
    filePathFileInfo:= "MyXXX"
    fileContentFileInfo:= "MyXXX"
    fileNewPathFileInfo:= "MyXXX"
    fileHashFileInfo:= "MyXXX"
    fileMd5FileInfo:= "MyXXX"
    fileSha256FileInfo:= "MyXXX"
    fileAttrFileInfo:= "MyXXX"
    var listFileInfoDataObject = []model.AlertFileInfo{
        {
            FilePath: &filePathFileInfo,
            FileContent: &fileContentFileInfo,
            FileNewPath: &fileNewPathFileInfo,
            FileHash: &fileHashFileInfo,
```



```
        FileMd5: &fileMd5FileInfo,
        FileSha256: &fileSha256FileInfo,
        FileAttr: &fileAttrFileInfo,
    },
}
userIdUserInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
userNameUserInfo:= "MyXXX"
var listUserInfoDataObject = []model.AlertUserInfo{
    {
        UserId: &userIdUserInfo,
        UserName: &userNameUserInfo,
    },
}
processNameProcess:= "MyXXX"
processPathProcess:= "MyXXX"
processPidProcess:= int32(123)
processUidProcess:= int32(123)
processCmdlineProcess:= "MyXXX"
var listProcessDataObject = []model.AlertProcess{
    {
        ProcessName: &processNameProcess,
        ProcessPath: &processPathProcess,
        ProcessPid: &processPidProcess,
        ProcessUid: &processUidProcess,
        ProcessCmdline: &processCmdlineProcess,
    },
}
malwareFamilyMalware:= "family"
malwareClassMalware:= "Malicious memory occupation."
malwareDataObject := &model.AlertMalware{
    MalwareFamily: &malwareFamilyMalware,
    MalwareClass: &malwareClassMalware,
}
recommendationRemediation:= "MyXXX"
urlRemediation:= "MyXXX"
remediationDataObject := &model.AlertRemediation{
    Recommendation: &recommendationRemediation,
    Url: &urlRemediation,
}
idResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
nameResourceList:= "MyXXX"
typeResourceList:= "MyXXX"
regionIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
domainIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
projectIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
epIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
epNameResourceList:= "MyXXX"
tagsResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
var listResourceListDataObject = []model.AlertResourceList{
    {
        Id: &idResourceList,
        Name: &nameResourceList,
        Type: &typeResourceList,
        RegionId: &regionIdResourceList,
        DomainId: &domainIdResourceList,
        ProjectId: &projectIdResourceList,
        EpId: &epIdResourceList,
        EpName: &epNameResourceList,
        Tags: &tagsResourceList,
    },
}
latitudeDestGeo:= float32(90)
longitudeDestGeo:= float32(180)
destGeoNetworkList := &model.AlertDestGeo{
    Latitude: &latitudeDestGeo,
    Longitude: &longitudeDestGeo,
}
latitudeSrcGeo:= float32(90)
longitudeSrcGeo:= float32(180)
```



```
    srcGeoNetworkList := &model.AlertSrcGeo{
        Latitude: &latitudeSrcGeo,
        Longitude: &longitudeSrcGeo,
    }
    directionNetworkList:= model.GetAlertNetworkListDirectionEnum().{}
    protocolNetworkList:= "TCP"
    srcIpNetworkList:= "192.168.0.1"
    srcPortNetworkList:= int32(1)
    srcDomainNetworkList:= "xxx"
    destIpNetworkList:= "192.168.0.1"
    destPortNetworkList:= "1"
    destDomainNetworkList:= "xxx"
    var listNetworkListDataObject = []model.AlertNetworkList{
        {
            Direction: &directionNetworkList,
            Protocol: &protocolNetworkList,
            SrcIp: &srcIpNetworkList,
            SrcPort: &srcPortNetworkList,
            SrcDomain: &srcDomainNetworkList,
            SrcGeo: srcGeoNetworkList,
            DestIp: &destIpNetworkList,
            DestPort: &destPortNetworkList,
            DestDomain: &destDomainNetworkList,
            DestGeo: destGeoNetworkList,
        },
    }
    sourceTypeDataSource:= int32(3)
    domainIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    projectIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    regionIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    productNameDataSource:= "test"
    productFeatureDataSource:= "test"
    dataSourceDataObject := &model.AlertDataSource{
        SourceType: &sourceTypeDataSource,
        DomainId: &domainIdDataSource,
        ProjectId: &projectIdDataSource,
        RegionId: &regionIdDataSource,
        ProductName: &productNameDataSource,
        ProductFeature: &productFeatureDataSource,
    }
    vendorTypeEnvironment:= "MyXXX"
    domainIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    regionIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    projectIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    environmentDataObject := &model.AlertEnvironment{
        VendorType: &vendorTypeEnvironment,
        DomainId: &domainIdEnvironment,
        RegionId: &regionIdEnvironment,
        ProjectId: &projectIdEnvironment,
    }
    versionDataObject:= "1.0"
    idDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    workspaceIdDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca620"
    labelsDataObject:= "MyXXX"
    firstObservedTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    lastObservedTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    createTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    arriveTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    titleDataObject:= "MyXXX"
    descriptionDataObject:= "This my XXXX"
    sourceUrlDataObject:= "http://xxx"
    countDataObject:= int32(4)
    confidenceDataObject:= int32(4)
    severityDataObject:= model.GetAlertSeverityEnum().TIPS
    criticalityDataObject:= int32(4)
    verificationStateDataObject:=
model.GetAlertVerificationStateEnum().**UNKNOWN**_UNKNOWN;_**TRUE_POSITIVE**_POSITIVE;_**FALSE_
POSITIVE**_FALSE_POSITIVE__THE_DEFAULT_VALUE_IS_**UNKNOWN**_
    handleStatusDataObject:=
```



```
model.GetAlertHandleStatusEnum().**OPEN**_OPEN;_**BLOCK**_PENDING;_**CLOSED**_CLOSED__THE_DEFA
ULT_VALUE_IS_**OPEN**_
    slaDataObject:= int32(60000)
    updateTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    closeTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    ipdrrPhaseDataObject:=
model.GetAlertIpdrrPhaseEnum().**PREPARATION**_PREPARATION_STAGE__**DETECTION_AND_ANALYSIS**_
DETECTION_AND_ANALYSIS_STAGE__**CONTAIN,_ERADICATION&_RECOVERY**_CONTAINMENT,_ERADICATI
ON,_AND_RECOVERY_STAGE__**POST_INCIDENT_ACTIVITY**_POST_INCIDENT_ACTIVITY_STAGE_
    simulationDataObject:= "false"
    actorDataObject:= "Tom"
    ownerDataObject:= "MyXXX"
    creatorDataObject:= "MyXXX"
    closeReasonDataObject:=
model.GetAlertCloseReasonEnum().FALSE_POSITIVE;_RESOLVED;_DUPLICATE;_OTHERS
    closeCommentDataObject:= "False positive; Resolved; Duplicate; Others"
    var systemInfoDataObject interface{} = make(map[string]string)
    var systemAlertTableDataObject interface{} = make(map[string]string)
    dataObjectbody := &model.Alert{
        Version: &versionDataObject,
        Id: &idDataObject,
        WorkspaceId: &workspaceIdDataObject,
        Labels: &labelsDataObject,
        Environment: environmentDataObject,
        DataSource: dataSourceDataObject,
        FirstObservedTime: &firstObservedTimeDataObject,
        LastObservedTime: &lastObservedTimeDataObject,
        CreateTime: &createTimeDataObject,
        ArriveTime: &arriveTimeDataObject,
        Title: &titleDataObject,
        Description: &descriptionDataObject,
        SourceUrl: &sourceUrlDataObject,
        Count: &countDataObject,
        Confidence: &confidenceDataObject,
        Severity: &severityDataObject,
        Criticality: &criticalityDataObject,
        NetworkList: &listNetworkListDataObject,
        ResourceList: &listResourceListDataObject,
        Remediation: remediationDataObject,
        VerificationState: &verificationStateDataObject,
        HandleStatus: &handleStatusDataObject,
        Sla: &slaDataObject,
        UpdateTime: &updateTimeDataObject,
        CloseTime: &closeTimeDataObject,
        IpdrrPhase: &ipdrrPhaseDataObject,
        Simulation: &simulationDataObject,
        Actor: &actorDataObject,
        Owner: &ownerDataObject,
        Creator: &creatorDataObject,
        CloseReason: &closeReasonDataObject,
        CloseComment: &closeCommentDataObject,
        Malware: malwareDataObject,
        SystemInfo: &systemInfoDataObject,
        Process: &listProcessDataObject,
        UserInfo: &listUserInfoDataObject,
        FileInfo: &listFileInfoDataObject,
        SystemAlertTable: &systemAlertTableDataObject,
    }
    request.Body = &model.CreateAlertRequestBody{
        DataObject: dataObjectbody,
    }
    response, err := client.CreateAlert(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	Response body of requests for creating alerts.
400	Response body for a failed request for creating alerts.

Error Codes

See **Error Codes**.

4.1.3 Deleting an Alert

Function

This API is used to delete an alert.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/alerts

Table 4-60 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-61 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.
content-type	Yes	String	Content type.

Table 4-62 Request body parameters

Parameter	Mandatory	Type	Description
batch_ids	No	Array of strings	IDs of deleted alerts.

Response Parameters

Status code: 200

Table 4-63 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-64 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**BatchOperateAlertResult** object	Returned object for batch operation on alerts.

Table 4-65 BatchOperateAlertResult

Parameter	Type	Description
error_ids	Array of strings	Failed IDs.
success_ids	Array of strings	Succeeded IDs.

Status code: 400

Table 4-66 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-67 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Delete the alert whose ID is 909494e3-558e-46b6-a9eb-07a8e18ca621.

```
{
  "batch_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
}
```

Example Responses

Status code: 200

Response body of the request for deleting alerts.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "success_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
    "error_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Delete the alert whose ID is 909494e3-558e-46b6-a9eb-07a8e18ca621.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class DeleteAlertSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteAlertRequest request = new DeleteAlertRequest();
        request.withWorkspaceId("{workspace_id}");
        DeleteAlertRequestBody body = new DeleteAlertRequestBody();
        List<String> listbodyBatchIds = new ArrayList<>();
        listbodyBatchIds.add("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withBatchIds(listbodyBatchIds);
        request.withBody(body);
        try {
            DeleteAlertResponse response = client.deleteAlert(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 alert whose ID is 909494e3-558e-46b6-a9eb-07a8e18ca621.

```
# coding: utf-8
```



```
import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteAlertRequest()
        request.workspace_id = "{workspace_id}"
        listBatchIdsbody = [
            "909494e3-558e-46b6-a9eb-07a8e18ca62f"
        ]
        request.body = DeleteAlertRequestBody(
            batch_ids=listBatchIdsbody
        )
        response = client.delete_alert(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 alert whose ID is 909494e3-558e-46b6-a9eb-07a8e18ca621.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteAlertRequest{}
    request.WorkspaceId = "{workspace_id}"
    var listBatchIdsbody = []string{
        "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    }
    request.Body = &model.DeleteAlertRequestBody{
        BatchIds: &listBatchIdsbody,
    }
    response, err := client.DeleteAlert(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	Response body of the request for deleting alerts.
400	Response body of the failed request for deleting alerts.

Error Codes

See **Error Codes**.

4.1.4 Converting an Alert into an Incident

Function

This API is used to convert alerts into incidents.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/batch-order

Table 4-68 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-69 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.
content-type	Yes	String	Content type.

Table 4-70 Request body parameters

Parameter	Mandatory	Type	Description
ids	No	Array of strings	IDs of the alerts to be converted into incidents.
incident_content	No	**incident_content** object	Incident content.

Table 4-71 incident_content

Parameter	Mandatory	Type	Description
title	No	String	Incident name.
incident_type	No	**incident_type** object	Incident type.

Table 4-72 incident_type

Parameter	Mandatory	Type	Description
id	No	String	Incident type ID.

Parameter	Mandatory	Type	Description
category	No	String	Parent incident type.
incident_type	No	String	Child incident type.

Response Parameters

Status code: 200

Table 4-73 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-74 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**BatchOperateAlertResult** object	Returned object for batch operation on alerts.

Table 4-75 BatchOperateAlertResult

Parameter	Type	Description
error_ids	Array of strings	Failed IDs.
success_ids	Array of strings	Succeeded IDs.

Status code: 400

Table 4-76 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-77 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Convert an alert into an incident, set Alert ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, Incident ID to 909494e3-558e-46b6-a9eb-07a8e18ca621, Alert status to Closed, and Mark as Evidence to No.

```
{
  "ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
  "incident_content" : {
    "title" : "XXX",
    "incident_type" : {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "category" : "DDoS attack",
      "incident_type" : "DNS protocol attacks"
    }
  }
}
```

Example Responses

Status code: 200

Response body for converting alerts into incidents.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "error_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
    "success_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Convert an alert into an incident, set Alert ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, Incident ID to 909494e3-558e-46b6-a9eb-07a8e18ca621, Alert status to Closed, and Mark as Evidence to No.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
```



```
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class CreateBatchOrderAlertsSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateBatchOrderAlertsRequest request = new CreateBatchOrderAlertsRequest();
        request.withWorkspaceId("{workspace_id}");
        OrderAlert body = new OrderAlert();
        OrderAlertIncidentContentIncidentType incidentTypeIncidentContent = new OrderAlertIncidentContentIncidentType();
        incidentTypeIncidentContent.withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withCategory("DDoS attack")
            .withIncidentType("DNS protocol attacks");
        OrderAlertIncidentContent incidentContentbody = new OrderAlertIncidentContent();
        incidentContentbody.withTitle("XXX")
            .withIncidentType(incidentTypeIncidentContent);
        List<String> listbodyIds = new ArrayList<>();
        listbodyIds.add("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withIncidentContent(incidentContentbody);
        body.withIds(listbodyIds);
        request.withBody(body);
        try {
            CreateBatchOrderAlertsResponse response = client.createBatchOrderAlerts(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

Convert an alert into an incident, set Alert ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, Incident ID to 909494e3-558e-46b6-a9eb-07a8e18ca621, Alert status to Closed, and Mark as Evidence to No.

```
# coding: utf-8

import os
```



```
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateBatchOrderAlertsRequest()
        request.workspace_id = "{workspace_id}"
        incidentTypeIncidentContent = OrderAlertIncidentContentIncidentType(
            id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            category="DDoS attack",
            incident_type="DNS protocol attacks"
        )
        incidentContentbody = OrderAlertIncidentContent(
            title="XXX",
            incident_type=incidentTypeIncidentContent
        )
        listIdsbody = [
            "909494e3-558e-46b6-a9eb-07a8e18ca62f"
        ]
        request.body = OrderAlert(
            incident_content=incidentContentbody,
            ids=listIdsbody
        )
        response = client.create_batch_order_alerts(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

Convert an alert into an incident, set Alert ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, Incident ID to 909494e3-558e-46b6-a9eb-07a8e18ca621, Alert status to Closed, and Mark as Evidence to No.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateBatchOrderAlertsRequest{}
    request.WorkspaceId = "{workspace_id}"
    idIncidentType:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    categoryIncidentType:= "DDoS attack"
    incidentTypeIncidentType:= "DNS protocol attacks"
    incidentTypeIncidentContent := &model.OrderAlertIncidentContentIncidentType{
        Id: &idIncidentType,
        Category: &categoryIncidentType,
        IncidentType: &incidentTypeIncidentType,
    }
    titleIncidentContent:= "XXX"
    incidentContentbody := &model.OrderAlertIncidentContent{
        Title: &titleIncidentContent,
        IncidentType: incidentTypeIncidentContent,
    }
    var listIdsbody = []string{
        "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    }
    request.Body = &model.OrderAlert{
        IncidentContent: incidentContentbody,
        Ids: &listIdsbody,
    }
    response, err := client.CreateBatchOrderAlerts(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	Response body for converting alerts into incidents.
400	Response body for the failed request for converting alerts into incidents.

Error Codes

See **Error Codes**.

4.1.5 Obtain Alert Details

Function

This API is used to obtain alert details.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/{alert_id}

Table 4-78 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
alert_id	Yes	String	Alert ID.

Request Parameters

Table 4-79 Request header parameters

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

Response Parameters

Status code: 200

Table 4-80 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-81 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**AlertDetail** object	Alert details object.

Table 4-82 AlertDetail

Parameter	Type	Description
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
data_object	**Alert** object	Alert entity information.
dataclass_ref	**dataclass_ref** object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
type	String	Data type.
project_id	String	ID of the current project.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
version	Integer	Version.

Parameter	Type	Description
workspace_id	String	ID of the current workspace.

Table 4-83 Alert

Parameter	Type	Description
version	String	Version of the data source of an alert. The value must be one officially released by the SSA service.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	String	ID of the region where the account to whom the data is delivered and hosted.
workspace_id	String	ID of the current workspace.
labels	String	Tag (display only).
environment	**environment** object	Coordinates of the environment where the alert was generated.
data_source	**data_source** object	Data source reported for the first time.
first_observed_time	String	First discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
last_observed_time	String	Latest discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Parameter	Type	Description
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
arrive_time	String	Receiving time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
title	String	Alert title.
description	String	Alert description.
source_url	String	Alert URL, which points to the page of the current incident description in the data source product.
count	Integer	Incident occurrences.
confidence	Integer	Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or problem. Value range: 0 to 100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.
severity	String	Severity level. Value range: Tips | Low | Medium | High | Fatal Note: **0**: Tips. No threats are found. **1**: Low. No actions are required for the threat. **2**: Medium. The threat needs to be handled but is not urgent. **3**: High. The threat must be handled preferentially. **4**: Fatal. The threat must be handled immediately to prevent further damage.

Parameter	Type	Description
criticality	Integer	Criticality, which specifies the importance level of the resources involved in an incident. Value range: 0 to 100. **0** indicates that the resource is not critical, and **100** indicates that the resource is critical.
alert_type	**alert_type** object	Alert classification. For details, see the *Alert Type Definition*.
network_list	Array of **network_list** objects	Network information.
resource_list	Array of **resource_list** objects	Affected resources.
remediation	**remediation** object	Remedy measure.
verification_state	String	Event verification status, which identifies the accuracy of the incident. The options are as follows: **Unknown**: The incident is unknown. **True_Positive**: The incident is confirmed. **False_Positive**: The incident is a false positive. The default value is **Unknown**.
handle_status	String	Incident handling status. The options are as follows: **Open**: Default status. **Block** **Closed** The default value is **Open**.
sla	Integer	Closure time: The deadline by which the incident must be resolved. Unit: hour.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Parameter	Type	Description
close_time	String	Closure time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
ipdrr_phase	String	Period/Handling phase No. **Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.
simulation	String	Debugging field.
actor	String	Alert investigator.
owner	String	Owner and service owner.
creator	String	Creator.
close_reason	String	Closure reason. False detection Resolved Repeated Other
close_comment	String	Comment for the closure.
malware	**malware** object	Malware.
system_info	Object	System information.
process	Array of **process** objects	Process information.
user_info	Array of **user_info** objects	User information.
file_info	Array of **file_info** objects	File information.
system_alert_table	Object	Layout fields in the alert list.

Table 4-84 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Account ID.
region_id	String	Region ID. **global** is returned for global services.
cross_workspace_id	String	Source workspace ID before data delivery. In the source workspace, the value is null. After data delivery, the value is the ID of the delegated user.
project_id	String	Project ID. The default value is null for global services.

Table 4-85 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows: **1**: Cloud service **2**: Third-party product **3**: Private product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source product is located. For details about the value range, see "Regions and Endpoints".
company_name	String	Name of the company to which the data source product belongs.
product_name	String	Name of the data source product.
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection model list.

Table 4-86 alert_type

Parameter	Type	Description
category	String	Category.
alert_type	String	Alert type.

Table 4-87 network_list

Parameter	Type	Description
direction	String	Direction. The value can be **IN** or **OUT**.
protocol	String	Protocol, including Layer 7 and Layer 4 protocols. Reference: IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml
src_ip	String	Source IP address.
src_port	Integer	Source port. Value range: 0 - 65535.
src_domain	String	Source domain name.
src_geo	**src_geo** object	Geographical location of the source IP address.
dest_ip	String	Destination IP address.
dest_port	String	Destination port. Value range: 0 to 65535.
dest_domain	String	Destination domain name.
dest_geo	**dest_geo** object	Geographical location of the destination IP address.

Table 4-88 src_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-89 dest_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-90 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type, which is the same as the **type** field in the RMS service.
provider	String	Cloud service name, which is the same as the **provider** field in the RMS service.
region_id	String	Region. Enter the value based on the cloud region ID.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the project to which the resource belongs, in UUID format.
ep_id	String	Enterprise project ID.
ep_name	String	Enterprise project name.
tags	String	Resource tags. 1. A maximum of 50 key-value pairs are supported. 2. The value can contain a maximum of 255 characters, including letters, digits, spaces, and special characters (+, -, =, ., _, :, /,@).

Table 4-91 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.
url	String	URL, which points to the general handling details for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-92 malware

Parameter	Type	Description
malware_family	String	Malicious family.
malware_class	String	Malware classification.

Table 4-93 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Path of the process execution file.
process_pid	Integer	Process ID.
process_uid	Integer	User ID associated with the process.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.
process_parent_path	String	Path of the parent process execution file.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	User ID associated with the parent process.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Path of the subprocess execution file.

Parameter	Type	Description
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	User ID associated with the subprocess.
process_child_cmdline	String	Subprocess command line.
process_launche_time	String	Process start time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
process_terminate_time	String	Process end time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Table 4-94 user_info

Parameter	Type	Description
user_id	String	User ID (UID).
user_name	String	Username.

Table 4-95 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File content.
file_new_path	String	New file path/name.
file_hash	String	File hash value.
file_md5	String	File MD5 value.
file_sha256	String	SHA256 value of the file.
file_attr	String	File attributes.

Table 4-96 dataclass_ref

Parameter	Type	Description
id	String	Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.
name	String	Data class name.

Status code: 400

Table 4-97 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-98 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response body for obtaining alert details.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "data_object" : {
      "version" : "1.0",
      "environment" : {
        "vendor_type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "data_source" : {
        "source_type" : 3,
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
```



```
    },
    "first_observed_time" : "2021-01-30T23:00:00Z+0800",
    "last_observed_time" : "2021-01-30T23:00:00Z+0800",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "arrive_time" : "2021-01-30T23:00:00Z+0800",
    "title" : "MyXXX",
    "description" : "This my XXXX",
    "source_url" : "http://xxx",
    "count" : "4",
    "confidence" : 4,
    "severity" : "TIPS",
    "criticality" : 4,
    "alert_type" : { },
    "network_list" : [ {
      "direction" : {
        "IN" : null
      },
      "protocol" : "TCP",
      "src_ip" : "192.168.0.1",
      "src_port" : "1",
      "src_domain" : "xxx",
      "dest_ip" : "192.168.0.1",
      "dest_port" : "1",
      "dest_domain" : "xxx",
      "src_geo" : {
        "latitude" : 90,
        "longitude" : 180
      },
      "dest_geo" : {
        "latitude" : 90,
        "longitude" : 180
      }
    } ],
    "resource_list" : [ {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_name" : "MyXXX",
      "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    } ],
    "remediation" : {
      "recommendation" : "MyXXX",
      "url" : "MyXXX"
    },
    "verification_state" : "**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**.",
    "handle_status" : "**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is **Open**.",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.",
    "simulation" : "false",
    "actor" : "Tom",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "False positive; Resolved; Duplicate; Others",
    "close_comment" : "False positive; Resolved; Duplicate; Others",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "Malicious memory occupation."
    },
    "system_info" : { },
    "process" : [ {
```

```
      "process_name" : "MyXXX",
      "process_path" : "MyXXX",
      "process_pid" : 123,
      "process_uid" : 123,
      "process_cmdline" : "MyXXX"
    } ],
    "user_info" : [ {
      "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "user_name" : "MyXXX"
    } ],
    "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
    } ],
    "system_alert_table" : { },
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "id" : "MyXXX",
  "version" : 11,
  "format_version" : 11,
  "dataclass_ref" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX"
  }
 }
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowAlertSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
            .withCredential(auth)
            .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
            .build();
        ShowAlertRequest request = new ShowAlertRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withAlertId("{alert_id}");
        try {
            ShowAlertResponse response = client.showAlert(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowAlertRequest()
        request.workspace_id = "{workspace_id}"
        request.alert_id = "{alert_id}"
        response = client.show_alert(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowAlertRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.AlertId = "{alert_id}"
    response, err := client.ShowAlert(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	Response body for obtaining alert details.
400	Response body for the failed request for obtaining alert details.

Error Codes

See **Error Codes**.

4.1.6 Updating an Alert

Function

This API is used to update alerts based on attribute changes. The update works on only changed columns.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/{alert_id}

Table 4-99 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
alert_id	Yes	String	Alert ID.

Request Parameters

Table 4-100 Request header parameters

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

Table 4-101 Request body parameters

Parameter	Mandatory	Type	Description
batch_ids	No	Array of strings	IDs of updated alerts.
data_object	No	**Alert** object	Alert entity information.

Table 4-102 Alert

Parameter	Mandatory	Type	Description
version	No	String	Version of the data source of an alert. The value must be one officially released by the SSA service.
id	No	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	No	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	No	String	ID of the region where the account to whom the data is delivered and hosted.
workspace_id	No	String	ID of the current workspace.
labels	No	String	Tag (display only).
environment	No	**environment** object	Coordinates of the environment where the alert was generated.
data_source	No	**data_source** object	Data source reported for the first time.
first_observed_time	No	String	First discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
last_observed_time	No	String	Latest discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Parameter	Mandatory	Type	Description
create_time	No	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
arrive_time	No	String	Receiving time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
title	No	String	Alert title.
description	No	String	Alert description.
source_url	No	String	Alert URL, which points to the page of the current incident description in the data source product.
count	No	Integer	Incident occurrences.
confidence	No	Integer	Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or problem. Value range: 0 to 100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.

Parameter	Mandatory	Type	Description
severity	No	String	Severity level. Value range: Tips | Low | Medium | High | Fatal Note: **0**: Tips. No threats are found. **1**: Low. No actions are required for the threat. **2**: Medium. The threat needs to be handled but is not urgent. **3**: High. The threat must be handled preferentially. **4**: Fatal. The threat must be handled immediately to prevent further damage.
criticality	No	Integer	Criticality, which specifies the importance level of the resources involved in an incident. Value range: 0 to 100. **0** indicates that the resource is not critical, and **100** indicates that the resource is critical.
alert_type	No	**alert_type** object	Alert classification. For details, see the *Alert Type Definition*.
network_list	No	Array of **network_list** objects	Network information.
resource_list	No	Array of **resource_list** objects	Affected resources.
remediation	No	**remediation** object	Remedy measure.

Parameter	Mandatory	Type	Description
verification_state	No	String	Event verification status, which identifies the accuracy of the incident. The options are as follows: **Unknown**: The incident is unknown. **True_Positive**: The incident is confirmed. **False_Positive**: The incident is a false positive. The default value is **Unknown**.
handle_status	No	String	Incident handling status. The options are as follows: **Open**: Default status. **Block** **Closed** The default value is **Open**.
sla	No	Integer	Closure time: The deadline by which the incident must be resolved. Unit: hour.
update_time	No	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
close_time	No	String	Closure time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Parameter	Mandatory	Type	Description
ipdrr_phase	No	String	Period/Handling phase No. **Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.
simulation	No	String	Debugging field.
actor	No	String	Alert investigator.
owner	No	String	Owner and service owner.
creator	No	String	Creator.
close_reason	No	String	Closure reason. False detection Resolved Repeated Other
close_comment	No	String	Comment for the closure.
malware	No	**malware** object	Malware.
system_info	No	Object	System information.
process	No	Array of **process** objects	Process information.
user_info	No	Array of **user_info** objects	User information.
file_info	No	Array of **file_info** objects	File information.
system_alert_table	No	Object	Layout fields in the alert list.

Table 4-103 environment

Parameter	Mandatory	Type	Description
vendor_type	No	String	Environment provider.
domain_id	No	String	Account ID.
region_id	No	String	Region ID. **global** is returned for global services.
cross_workspace_id	No	String	Source workspace ID before data delivery. In the source workspace, the value is null. After data delivery, the value is the ID of the delegated user.
project_id	No	String	Project ID. The default value is null for global services.

Table 4-104 data_source

Parameter	Mandatory	Type	Description
source_type	No	Integer	Data source type. The options are as follows: **1**: Cloud service **2**: Third-party product **3**: Private product
domain_id	No	String	Account ID to which the data source product belongs.
project_id	No	String	ID of the project to which the data source product belongs.
region_id	No	String	Region where the data source product is located. For details about the value range, see "Regions and Endpoints".
company_name	No	String	Name of the company to which the data source product belongs.
product_name	No	String	Name of the data source product.
product_feature	No	String	Name of the feature of the product that detects the incident.
product_module	No	String	Threat detection model list.

Table 4-105 alert_type

Parameter	Mandatory	Type	Description
category	No	String	Category.
alert_type	No	String	Alert type.

Table 4-106 network_list

Parameter	Mandatory	Type	Description
direction	No	String	Direction. The value can be **IN** or **OUT**.
protocol	No	String	Protocol, including Layer 7 and Layer 4 protocols. Reference: IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml
src_ip	No	String	Source IP address.
src_port	No	Integer	Source port. Value range: 0 - 65535.
src_domain	No	String	Source domain name.
src_geo	No	**src_geo** object	Geographical location of the source IP address.
dest_ip	No	String	Destination IP address.
dest_port	No	String	Destination port. Value range: 0 to 65535.
dest_domain	No	String	Destination domain name.
dest_geo	No	**dest_geo** object	Geographical location of the destination IP address.

Table 4-107 src_geo

Parameter	Mandatory	Type	Description
latitude	No	Number	Latitude.
longitude	No	Number	Longitude.
city_code	No	String	City Code.

Parameter	Mandatory	Type	Description
country_code	No	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-108 dest_geo

Parameter	Mandatory	Type	Description
latitude	No	Number	Latitude.
longitude	No	Number	Longitude.
city_code	No	String	City Code.
country_code	No	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-109 resource_list

Parameter	Mandatory	Type	Description
id	No	String	Cloud service resource ID.
name	No	String	Resource name.
type	No	String	Resource type, which is the same as the **type** field in the RMS service.
provider	No	String	Cloud service name, which is the same as the **provider** field in the RMS service.
region_id	No	String	Region. Enter the value based on the cloud region ID.
domain_id	No	String	ID of the account to which the resource belongs, in UUID format.
project_id	No	String	ID of the project to which the resource belongs, in UUID format.
ep_id	No	String	Enterprise project ID.
ep_name	No	String	Enterprise project name.

Parameter	Mandatory	Type	Description
tags	No	String	Resource tags. 1. A maximum of 50 key-value pairs are supported. 2. The value can contain a maximum of 255 characters, including letters, digits, spaces, and special characters (+, -, =, ., _, :, /,@).

Table 4-110 remediation

Parameter	Mandatory	Type	Description
recommendation	No	String	Recommended solution.
url	No	String	URL, which points to the general handling details for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-111 malware

Parameter	Mandatory	Type	Description
malware_family	No	String	Malicious family.
malware_class	No	String	Malware classification.

Table 4-112 process

Parameter	Mandatory	Type	Description
process_name	No	String	Process name.
process_path	No	String	Path of the process execution file.
process_pid	No	Integer	Process ID.
process_uid	No	Integer	User ID associated with the process.

Parameter	Mandatory	Type	Description
process_cmdline	No	String	Process command line.
process_parent_name	No	String	Parent process name.
process_parent_path	No	String	Path of the parent process execution file.
process_parent_pid	No	Integer	Parent process ID.
process_parent_uid	No	Integer	User ID associated with the parent process.
process_parent_cmdline	No	String	Parent process command line.
process_child_name	No	String	Subprocess name.
process_child_path	No	String	Path of the subprocess execution file.
process_child_pid	No	Integer	Subprocess ID.
process_child_uid	No	Integer	User ID associated with the subprocess.
process_child_cmdline	No	String	Subprocess command line.
process_launche_time	No	String	Process start time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
process_terminate_time	No	String	Process end time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Table 4-113 user_info

Parameter	Mandatory	Type	Description
user_id	No	String	User ID (UID).
user_name	No	String	Username.

Table 4-114 file_info

Parameter	Mandatory	Type	Description
file_path	No	String	File path/name.
file_content	No	String	File content.
file_new_path	No	String	New file path/name.
file_hash	No	String	File hash value.
file_md5	No	String	File MD5 value.
file_sha256	No	String	SHA256 value of the file.
file_attr	No	String	File attributes.

Response Parameters

Status code: 200

Table 4-115 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-116 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**AlertDetail** object	Alert details object.

Table 4-117 AlertDetail

Parameter	Type	Description
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
data_object	**Alert** object	Alert entity information.
dataclass_ref	**dataclass_ref** object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
type	String	Data type.
project_id	String	ID of the current project.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-118 Alert

Parameter	Type	Description
version	String	Version of the data source of an alert. The value must be one officially released by the SSA service.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	String	ID of the account (domain_id) to whom the data is delivered and hosted.

Parameter	Type	Description
region_id	String	ID of the region where the account to whom the data is delivered and hosted.
workspace_id	String	ID of the current workspace.
labels	String	Tag (display only).
environment	**environment** object	Coordinates of the environment where the alert was generated.
data_source	**data_source** object	Data source reported for the first time.
first_observed_time	String	First discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
last_observed_time	String	Latest discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
arrive_time	String	Receiving time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
title	String	Alert title.
description	String	Alert description.
source_url	String	Alert URL, which points to the page of the current incident description in the data source product.
count	Integer	Incident occurrences.

Parameter	Type	Description
confidence	Integer	Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or problem. Value range: 0 to 100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.
severity	String	Severity level. Value range: Tips | Low | Medium | High | Fatal Note: **0**: Tips. No threats are found. **1**: Low. No actions are required for the threat. **2**: Medium. The threat needs to be handled but is not urgent. **3**: High. The threat must be handled preferentially. **4**: Fatal. The threat must be handled immediately to prevent further damage.
criticality	Integer	Criticality, which specifies the importance level of the resources involved in an incident. Value range: 0 to 100. **0** indicates that the resource is not critical, and **100** indicates that the resource is critical.
alert_type	**alert_type** object	Alert classification. For details, see the *Alert Type Definition*.
network_list	Array of **network_list** objects	Network information.
resource_list	Array of **resource_list** objects	Affected resources.
remediation	**remediation** object	Remedy measure.

Parameter	Type	Description
verification_state	String	Event verification status, which identifies the accuracy of the incident. The options are as follows: **Unknown**: The incident is unknown. **True_Positive**: The incident is confirmed. **False_Positive**: The incident is a false positive. The default value is **Unknown**.
handle_status	String	Incident handling status. The options are as follows: **Open**: Default status. **Block** **Closed** The default value is **Open**.
sla	Integer	Closure time: The deadline by which the incident must be resolved. Unit: hour.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
close_time	String	Closure time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
ipdrr_phase	String	Period/Handling phase No. **Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.
simulation	String	Debugging field.
actor	String	Alert investigator.
owner	String	Owner and service owner.

Parameter	Type	Description
creator	String	Creator.
close_reason	String	Closure reason. False detection Resolved Repeated Other
close_comment	String	Comment for the closure.
malware	**malware** object	Malware.
system_info	Object	System information.
process	Array of **process** objects	Process information.
user_info	Array of **user_info** objects	User information.
file_info	Array of **file_info** objects	File information.
system_alert_table	Object	Layout fields in the alert list.

Table 4-119 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Account ID.
region_id	String	Region ID. **global** is returned for global services.
cross_workspace_id	String	Source workspace ID before data delivery. In the source workspace, the value is null. After data delivery, the value is the ID of the delegated user.
project_id	String	Project ID. The default value is null for global services.

Table 4-120 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows: **1**: Cloud service **2**: Third-party product **3**: Private product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source product is located. For details about the value range, see "Regions and Endpoints".
company_name	String	Name of the company to which the data source product belongs.
product_name	String	Name of the data source product.
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection model list.

Table 4-121 alert_type

Parameter	Type	Description
category	String	Category.
alert_type	String	Alert type.

Table 4-122 network_list

Parameter	Type	Description
direction	String	Direction. The value can be **IN** or **OUT**.
protocol	String	Protocol, including Layer 7 and Layer 4 protocols. Reference: IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Parameter	Type	Description
src_ip	String	Source IP address.
src_port	Integer	Source port. Value range: 0 - 65535.
src_domain	String	Source domain name.
src_geo	**src_geo** object	Geographical location of the source IP address.
dest_ip	String	Destination IP address.
dest_port	String	Destination port. Value range: 0 to 65535.
dest_domain	String	Destination domain name.
dest_geo	**dest_geo** object	Geographical location of the destination IP address.

Table 4-123 src_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-124 dest_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-125 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type, which is the same as the **type** field in the RMS service.
provider	String	Cloud service name, which is the same as the **provider** field in the RMS service.
region_id	String	Region. Enter the value based on the cloud region ID.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the project to which the resource belongs, in UUID format.
ep_id	String	Enterprise project ID.
ep_name	String	Enterprise project name.
tags	String	Resource tags. 1. A maximum of 50 key-value pairs are supported. 2. The value can contain a maximum of 255 characters, including letters, digits, spaces, and special characters (+, -, =, ., _, :, /,@).

Table 4-126 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.
url	String	URL, which points to the general handling details for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-127 malware

Parameter	Type	Description
malware_family	String	Malicious family.
malware_class	String	Malware classification.

Table 4-128 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Path of the process execution file.
process_pid	Integer	Process ID.
process_uid	Integer	User ID associated with the process.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.
process_parent_path	String	Path of the parent process execution file.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	User ID associated with the parent process.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Path of the subprocess execution file.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	User ID associated with the subprocess.
process_child_cmdline	String	Subprocess command line.

Parameter	Type	Description
process_launche_time	String	Process start time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
process_terminate_time	String	Process end time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Table 4-129 user_info

Parameter	Type	Description
user_id	String	User ID (UID).
user_name	String	Username.

Table 4-130 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File content.
file_new_path	String	New file path/name.
file_hash	String	File hash value.
file_md5	String	File MD5 value.
file_sha256	String	SHA256 value of the file.
file_attr	String	File attributes.

Table 4-131 dataclass_ref

Parameter	Type	Description
id	String	Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.

Parameter	Type	Description
name	String	Data class name.

Status code: 400

Table 4-132 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-133 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Update an alert. Set Alert Name to MyXXX, URL to http://xxx, the number of occurrences to 4, Confidence to 4, and Severity to tips.

```
{
  "data_object" : {
    "version" : "1.0",
    "environment" : {
      "vendor_type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "data_source" : {
      "source_type" : 3,
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "first_observed_time" : "2021-01-30T23:00:00Z+0800",
    "last_observed_time" : "2021-01-30T23:00:00Z+0800",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "arrive_time" : "2021-01-30T23:00:00Z+0800",
    "title" : "MyXXX",
    "description" : "This my XXXX",
    "source_url" : "http://xxx",
    "count" : 4,
    "confidence" : 4,
    "severity" : "TIPS",
    "criticality" : 4,
    "alert_type" : { },
    "network_list" : [ {
      "direction" : {
        "IN" : null
```



```
    },
    "protocol" : "TCP",
    "src_ip" : "192.168.0.1",
    "src_port" : "1",
    "src_domain" : "xxx",
    "dest_ip" : "192.168.0.1",
    "dest_port" : "1",
    "dest_domain" : "xxx",
    "src_geo" : {
      "latitude" : 90,
      "longitude" : 180
    },
    "dest_geo" : {
      "latitude" : 90,
      "longitude" : 180
    }
  } ],
  "resource_list" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "type" : "MyXXX",
    "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ep_name" : "MyXXX",
    "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  } ],
  "remediation" : {
    "recommendation" : "MyXXX",
    "url" : "MyXXX"
  },
  "verification_state" : "**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**.",
  "handle_status" : "**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is **Open**.",
  "sla" : 60000,
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "close_time" : "2021-01-30T23:00:00Z+0800",
  "ipdrr_phase" : "**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.",
  "simulation" : "false",
  "actor" : "Tom",
  "owner" : "MyXXX",
  "creator" : "MyXXX",
  "close_reason" : "False positive; Resolved; Duplicate; Others",
  "close_comment" : "False positive; Resolved; Duplicate; Others",
  "malware" : {
    "malware_family" : "family",
    "malware_class" : "Malicious memory occupation."
  },
  "system_info" : { },
  "process" : [ {
    "process_name" : "MyXXX",
    "process_path" : "MyXXX",
    "process_pid" : 123,
    "process_uid" : 123,
    "process_cmdline" : "MyXXX"
  } ],
  "user_info" : [ {
    "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "user_name" : "MyXXX"
  } ],
  "file_info" : [ {
    "file_path" : "MyXXX",
    "file_content" : "MyXXX",
    "file_new_path" : "MyXXX",
    "file_hash" : "MyXXX",
    "file_md5" : "MyXXX",
```



```
    "file_sha256" : "MyXXX",
    "file_attr" : "MyXXX"
   } ],
   "system_alert_table" : { },
   "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
   "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  }
}
```

Example Responses

Status code: 200

Response body of requests for updating alerts.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "data_object" : {
      "version" : "1.0",
      "environment" : {
        "vendor_type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "data_source" : {
        "source_type" : 3,
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "first_observed_time" : "2021-01-30T23:00:00Z+0800",
      "last_observed_time" : "2021-01-30T23:00:00Z+0800",
      "create_time" : "2021-01-30T23:00:00Z+0800",
      "arrive_time" : "2021-01-30T23:00:00Z+0800",
      "title" : "MyXXX",
      "description" : "This my XXXX",
      "source_url" : "http://xxx",
      "count" : 4,
      "confidence" : 4,
      "severity" : "TIPS",
      "criticality" : 4,
      "alert_type" : { },
      "network_list" : [ {
        "direction" : {
          "IN" : null
        },
        "protocol" : "TCP",
        "src_ip" : "192.168.0.1",
        "src_port" : "1",
        "src_domain" : "xxx",
        "dest_ip" : "192.168.0.1",
        "dest_port" : "1",
        "dest_domain" : "xxx",
        "src_geo" : {
          "latitude" : 90,
          "longitude" : 180
        },
        "dest_geo" : {
          "latitude" : 90,
          "longitude" : 180
        }
      } ],
      "resource_list" : [ {
        "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "name" : "MyXXX",
        "type" : "MyXXX",
```



```
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_name" : "MyXXX",
      "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    } ],
    "remediation" : {
      "recommendation" : "MyXXX",
      "url" : "MyXXX"
    },
    "verification_state" : "**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**.",
    "handle_status" : "**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is **Open**.",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.",
    "simulation" : "false",
    "actor" : "Tom",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "False positive; Resolved; Duplicate; Others",
    "close_comment" : "False positive; Resolved; Duplicate; Others",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "Malicious memory occupation."
    },
    "system_info" : { },
    "process" : [ {
      "process_name" : "MyXXX",
      "process_path" : "MyXXX",
      "process_pid" : 123,
      "process_uid" : 123,
      "process_cmdline" : "MyXXX"
    } ],
    "user_info" : [ {
      "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "user_name" : "MyXXX"
    } ],
    "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
    } ],
    "system_alert_table" : { },
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "id" : "MyXXX",
  "version" : 11,
  "format_version" : 11,
  "dataclass_ref" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX"
  }
 }
}
```


SDK Sample Code

The SDK sample code is as follows.

Java

Update an alert. Set Alert Name to MyXXX, URL to http://xxx, the number of occurrences to 4, Confidence to 4, and Severity to tips.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class ChangeAlertSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ChangeAlertRequest request = new ChangeAlertRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withAlertId("{alert_id}");
        ChangeAlertRequestBody body = new ChangeAlertRequestBody();
        List<AlertFileInfo> listDataObjectFileInfo = new ArrayList<>();
        listDataObjectFileInfo.add(
            new AlertFileInfo()
                .withFilePath("MyXXX")
                .withFileContent("MyXXX")
                .withFileNewPath("MyXXX")
                .withFileHash("MyXXX")
                .withFileMd5("MyXXX")
                .withFileSha256("MyXXX")
                .withFileAttr("MyXXX")
        );
        List<AlertUserInfo> listDataObjectUserInfo = new ArrayList<>();
        listDataObjectUserInfo.add(
            new AlertUserInfo()
                .withUserId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withUserName("MyXXX")
        );
        List<AlertProcess> listDataObjectProcess = new ArrayList<>();
        listDataObjectProcess.add(
            new AlertProcess()
```



```
        .withProcessName("MyXXX")
        .withProcessPath("MyXXX")
        .withProcessPid(123)
        .withProcessUid(123)
        .withProcessCmdline("MyXXX")
);
AlertMalware malwareDataObject = new AlertMalware();
malwareDataObject.withMalwareFamily("family")
    .withMalwareClass("Malicious memory occupation.");
AlertRemediation remediationDataObject = new AlertRemediation();
remediationDataObject.withRecommendation("MyXXX")
    .withUrl("MyXXX");
List<AlertResourceList> listDataObjectResourceList = new ArrayList<>();
listDataObjectResourceList.add(
    new AlertResourceList()
        .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withName("MyXXX")
        .withType("MyXXX")
        .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withEpId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withEpName("MyXXX")
        .withTags("909494e3-558e-46b6-a9eb-07a8e18ca62f")
);
AlertDestGeo destGeoNetworkList = new AlertDestGeo();
destGeoNetworkList.withLatitude(java.math.BigDecimal.valueOf(90))
    .withLongitude(java.math.BigDecimal.valueOf(180));
AlertSrcGeo srcGeoNetworkList = new AlertSrcGeo();
srcGeoNetworkList.withLatitude(java.math.BigDecimal.valueOf(90))
    .withLongitude(java.math.BigDecimal.valueOf(180));
List<AlertNetworkList> listDataObjectNetworkList = new ArrayList<>();
listDataObjectNetworkList.add(
    new AlertNetworkList()
        .withDirection(AlertNetworkList.DirectionEnum.fromValue("{}"))
        .withProtocol("TCP")
        .withSrcIp("192.168.0.1")
        .withSrcPort(1)
        .withSrcDomain("xxx")
        .withSrcGeo(srcGeoNetworkList)
        .withDestIp("192.168.0.1")
        .withDestPort("1")
        .withDestDomain("xxx")
        .withDestGeo(destGeoNetworkList)
);
AlertDataSource dataSourceDataObject = new AlertDataSource();
dataSourceDataObject.withSourceType(3)
    .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
AlertEnvironment environmentDataObject = new AlertEnvironment();
environmentDataObject.withVendorType("MyXXX")
    .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
Alert dataObjectbody = new Alert();
dataObjectbody.withVersion("1.0")
    .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withWorkspaceId("909494e3-558e-46b6-a9eb-07a8e18ca620")
    .withEnvironment(environmentDataObject)
    .withDataSource(dataSourceDataObject)
    .withFirstObservedTime("2021-01-30T23:00:00Z+0800")
    .withLastObservedTime("2021-01-30T23:00:00Z+0800")
    .withCreateTime("2021-01-30T23:00:00Z+0800")
    .withArriveTime("2021-01-30T23:00:00Z+0800")
    .withTitle("MyXXX")
    .withDescription("This my XXXX")
    .withSourceUrl("http://xxx")
    .withCount(4)
```



```
            .withConfidence(4)
            .withSeverity(Alert.SeverityEnum.fromValue("TIPS"))
            .withCriticality(4)
            .withNetworkList(listDataObjectNetworkList)
            .withResourceList(listDataObjectResourceList)
            .withRemediation(remediationDataObject)
            .withVerificationState(Alert.VerificationStateEnum.fromValue("**Unknown**: Unknown;
**True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**."))
            .withHandleStatus(Alert.HandleStatusEnum.fromValue("**Open**: Open; **Block**: Pending;
**Closed**: Closed. The default value is **Open**."))
            .withSla(60000)
            .withUpdateTime("2021-01-30T23:00:00Z+0800")
            .withCloseTime("2021-01-30T23:00:00Z+0800")
            .withIpdrrPhase(Alert.IpdrrPhaseEnum.fromValue("**Preparation**: Preparation stage. **Detection
and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication,
and recovery stage. **Post-Incident-Activity**: Post-incident activity stage."))
            .withSimulation("false")
            .withActor("Tom")
            .withOwner("MyXXX")
            .withCreator("MyXXX")
            .withCloseReason(Alert.CloseReasonEnum.fromValue("False positive; Resolved; Duplicate; Others"))
            .withCloseComment("False positive; Resolved; Duplicate; Others")
            .withMalware(malwareDataObject)
            .withSystemInfo(new Object())
            .withProcess(listDataObjectProcess)
            .withUserInfo(listDataObjectUserInfo)
            .withFileInfo(listDataObjectFileInfo)
            .withSystemAlertTable(new Object());
        body.withDataObject(dataObjectbody);
        request.withBody(body);
        try {
            ChangeAlertResponse response = client.changeAlert(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 an alert. Set Alert Name to MyXXX, URL to http://xxx, the number of occurrences to 4, Confidence to 4, and Severity to tips.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ChangeAlertRequest()
    request.workspace_id = "{workspace_id}"
    request.alert_id = "{alert_id}"
    listFileInfoDataObject = [
        AlertFileInfo(
            file_path="MyXXX",
            file_content="MyXXX",
            file_new_path="MyXXX",
            file_hash="MyXXX",
            file_md5="MyXXX",
            file_sha256="MyXXX",
            file_attr="MyXXX"
        )
    ]
    listUserInfoDataObject = [
        AlertUserInfo(
            user_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            user_name="MyXXX"
        )
    ]
    listProcessDataObject = [
        AlertProcess(
            process_name="MyXXX",
            process_path="MyXXX",
            process_pid=123,
            process_uid=123,
            process_cmdline="MyXXX"
        )
    ]
    malwareDataObject = AlertMalware(
        malware_family="family",
        malware_class="Malicious memory occupation."
    )
    remediationDataObject = AlertRemediation(
        recommendation="MyXXX",
        url="MyXXX"
    )
    listResourceListDataObject = [
        AlertResourceList(
            id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            name="MyXXX",
            type="MyXXX",
            region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            ep_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            ep_name="MyXXX",
            tags="909494e3-558e-46b6-a9eb-07a8e18ca62f"
        )
    ]
    destGeoNetworkList = AlertDestGeo(
        latitude=90,
        longitude=180
    )
    srcGeoNetworkList = AlertSrcGeo(
        latitude=90,
        longitude=180
    )
    listNetworkListDataObject = [
        AlertNetworkList(
```



```
            direction="{}",
            protocol="TCP",
            src_ip="192.168.0.1",
            src_port=1,
            src_domain="xxx",
            src_geo=srcGeoNetworkList,
            dest_ip="192.168.0.1",
            dest_port="1",
            dest_domain="xxx",
            dest_geo=destGeoNetworkList
        )
    ]
    dataSourceDataObject = AlertDataSource(
        source_type=3,
        domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f"
    )
    environmentDataObject = AlertEnvironment(
        vendor_type="MyXXX",
        domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f"
    )
    dataObjectbody = Alert(
        version="1.0",
        id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        workspace_id="909494e3-558e-46b6-a9eb-07a8e18ca620",
        environment=environmentDataObject,
        data_source=dataSourceDataObject,
        first_observed_time="2021-01-30T23:00:00Z+0800",
        last_observed_time="2021-01-30T23:00:00Z+0800",
        create_time="2021-01-30T23:00:00Z+0800",
        arrive_time="2021-01-30T23:00:00Z+0800",
        title="MyXXX",
        description="This my XXXX",
        source_url="http://xxx",
        count=4,
        confidence=4,
        severity="TIPS",
        criticality=4,
        network_list=listNetworkListDataObject,
        resource_list=listResourceListDataObject,
        remediation=remediationDataObject,
        verification_state="**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**.",
        handle_status="**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is **Open**.",
        sla=60000,
        update_time="2021-01-30T23:00:00Z+0800",
        close_time="2021-01-30T23:00:00Z+0800",
        ipdrr_phase="**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.",
        simulation="false",
        actor="Tom",
        owner="MyXXX",
        creator="MyXXX",
        close_reason="False positive; Resolved; Duplicate; Others",
        close_comment="False positive; Resolved; Duplicate; Others",
        malware=malwareDataObject,
        system_info={},
        process=listProcessDataObject,
        user_info=listUserInfoDataObject,
        file_info=listFileInfoDataObject,
        system_alert_table={}
    )
    request.body = ChangeAlertRequestBody(
        data_object=dataObjectbody
```



```
        )
        response = client.change_alert(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 an alert. Set Alert Name to MyXXX, URL to http://xxx, the number of occurrences to 4, Confidence to 4, and Severity to tips.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ChangeAlertRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.AlertId = "{alert_id}"
    filePathFileInfo:= "MyXXX"
    fileContentFileInfo:= "MyXXX"
    fileNewPathFileInfo:= "MyXXX"
    fileHashFileInfo:= "MyXXX"
    fileMd5FileInfo:= "MyXXX"
    fileSha256FileInfo:= "MyXXX"
    fileAttrFileInfo:= "MyXXX"
    var listFileInfoDataObject = []model.AlertFileInfo{
        {
            FilePath: &filePathFileInfo,
            FileContent: &fileContentFileInfo,
            FileNewPath: &fileNewPathFileInfo,
            FileHash: &fileHashFileInfo,
            FileMd5: &fileMd5FileInfo,
            FileSha256: &fileSha256FileInfo,
            FileAttr: &fileAttrFileInfo,
        },
    }
    userIdUserInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    userNameUserInfo:= "MyXXX"
```



```
var listUserInfoDataObject = []model.AlertUserInfo{
    {
        UserId: &userIdUserInfo,
        UserName: &userNameUserInfo,
    },
}
processNameProcess:= "MyXXX"
processPathProcess:= "MyXXX"
processPidProcess:= int32(123)
processUidProcess:= int32(123)
processCmdlineProcess:= "MyXXX"
var listProcessDataObject = []model.AlertProcess{
    {
        ProcessName: &processNameProcess,
        ProcessPath: &processPathProcess,
        ProcessPid: &processPidProcess,
        ProcessUid: &processUidProcess,
        ProcessCmdline: &processCmdlineProcess,
    },
}
malwareFamilyMalware:= "family"
malwareClassMalware:= "Malicious memory occupation."
malwareDataObject := &model.AlertMalware{
    MalwareFamily: &malwareFamilyMalware,
    MalwareClass: &malwareClassMalware,
}
recommendationRemediation:= "MyXXX"
urlRemediation:= "MyXXX"
remediationDataObject := &model.AlertRemediation{
    Recommendation: &recommendationRemediation,
    Url: &urlRemediation,
}
idResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
nameResourceList:= "MyXXX"
typeResourceList:= "MyXXX"
regionIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
domainIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
projectIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
epIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
epNameResourceList:= "MyXXX"
tagsResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
var listResourceListDataObject = []model.AlertResourceList{
    {
        Id: &idResourceList,
        Name: &nameResourceList,
        Type: &typeResourceList,
        RegionId: &regionIdResourceList,
        DomainId: &domainIdResourceList,
        ProjectId: &projectIdResourceList,
        EpId: &epIdResourceList,
        EpName: &epNameResourceList,
        Tags: &tagsResourceList,
    },
}
latitudeDestGeo:= float32(90)
longitudeDestGeo:= float32(180)
destGeoNetworkList := &model.AlertDestGeo{
    Latitude: &latitudeDestGeo,
    Longitude: &longitudeDestGeo,
}
latitudeSrcGeo:= float32(90)
longitudeSrcGeo:= float32(180)
srcGeoNetworkList := &model.AlertSrcGeo{
    Latitude: &latitudeSrcGeo,
    Longitude: &longitudeSrcGeo,
}
directionNetworkList:= model.GetAlertNetworkListDirectionEnum().{}
protocolNetworkList:= "TCP"
srcIpNetworkList:= "192.168.0.1"
```



```
    srcPortNetworkList:= int32(1)
    srcDomainNetworkList:= "xxx"
    destIpNetworkList:= "192.168.0.1"
    destPortNetworkList:= "1"
    destDomainNetworkList:= "xxx"
    var listNetworkListDataObject = []model.AlertNetworkList{
        {
            Direction: &directionNetworkList,
            Protocol: &protocolNetworkList,
            SrcIp: &srcIpNetworkList,
            SrcPort: &srcPortNetworkList,
            SrcDomain: &srcDomainNetworkList,
            SrcGeo: srcGeoNetworkList,
            DestIp: &destIpNetworkList,
            DestPort: &destPortNetworkList,
            DestDomain: &destDomainNetworkList,
            DestGeo: destGeoNetworkList,
        },
    }
    sourceTypeDataSource:= int32(3)
    domainIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    projectIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    regionIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    dataSourceDataObject := &model.AlertDataSource{
        SourceType: &sourceTypeDataSource,
        DomainId: &domainIdDataSource,
        ProjectId: &projectIdDataSource,
        RegionId: &regionIdDataSource,
    }
    vendorTypeEnvironment:= "MyXXX"
    domainIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    regionIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    projectIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    environmentDataObject := &model.AlertEnvironment{
        VendorType: &vendorTypeEnvironment,
        DomainId: &domainIdEnvironment,
        RegionId: &regionIdEnvironment,
        ProjectId: &projectIdEnvironment,
    }
    versionDataObject:= "1.0"
    idDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    workspaceIdDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca620"
    firstObservedTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    lastObservedTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    createTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    arriveTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    titleDataObject:= "MyXXX"
    descriptionDataObject:= "This my XXXX"
    sourceUrlDataObject:= "http://xxx"
    countDataObject:= int32(4)
    confidenceDataObject:= int32(4)
    severityDataObject:= model.GetAlertSeverityEnum().TIPS
    criticalityDataObject:= int32(4)
    verificationStateDataObject:=
model.GetAlertVerificationStateEnum().**UNKNOWN**_UNKNOWN;_**TRUE_POSITIVE**_POSITIVE;_**FALSE_
POSITIVE**_FALSE_POSITIVE__THE_DEFAULT_VALUE_IS_**UNKNOWN**_
    handleStatusDataObject:=
model.GetAlertHandleStatusEnum().**OPEN**_OPEN;_**BLOCK**_PENDING;_**CLOSED**_CLOSED__THE_DEFA
ULT_VALUE_IS_**OPEN**_
    slaDataObject:= int32(60000)
    updateTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    closeTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    ipdrrPhaseDataObject:=
model.GetAlertIpdrrPhaseEnum().**PREPARATION**_PREPARATION_STAGE__**DETECTION_AND_ANALYSIS**_
DETECTION_AND_ANALYSIS_STAGE__**CONTAIN,_ERADICATION&_RECOVERY**_CONTAINMENT,_ERADICATI
ON,_AND_RECOVERY_STAGE__**POST_INCIDENT_ACTIVITY**_POST_INCIDENT_ACTIVITY_STAGE_
    simulationDataObject:= "false"
    actorDataObject:= "Tom"
    ownerDataObject:= "MyXXX"
```



```
    creatorDataObject:= "MyXXX"
    closeReasonDataObject:=
model.GetAlertCloseReasonEnum().FALSE_POSITIVE;_RESOLVED;_DUPLICATE;_OTHERS
    closeCommentDataObject:= "False positive; Resolved; Duplicate; Others"
    var systemInfoDataObject interface{} = make(map[string]string)
    var systemAlertTableDataObject interface{} = make(map[string]string)
    dataObjectbody := &model.Alert{
        Version: &versionDataObject,
        Id: &idDataObject,
        WorkspaceId: &workspaceIdDataObject,
        Environment: environmentDataObject,
        DataSource: dataSourceDataObject,
        FirstObservedTime: &firstObservedTimeDataObject,
        LastObservedTime: &lastObservedTimeDataObject,
        CreateTime: &createTimeDataObject,
        ArriveTime: &arriveTimeDataObject,
        Title: &titleDataObject,
        Description: &descriptionDataObject,
        SourceUrl: &sourceUrlDataObject,
        Count: &countDataObject,
        Confidence: &confidenceDataObject,
        Severity: &severityDataObject,
        Criticality: &criticalityDataObject,
        NetworkList: &listNetworkListDataObject,
        ResourceList: &listResourceListDataObject,
        Remediation: remediationDataObject,
        VerificationState: &verificationStateDataObject,
        HandleStatus: &handleStatusDataObject,
        Sla: &slaDataObject,
        UpdateTime: &updateTimeDataObject,
        CloseTime: &closeTimeDataObject,
        IpdrrPhase: &ipdrrPhaseDataObject,
        Simulation: &simulationDataObject,
        Actor: &actorDataObject,
        Owner: &ownerDataObject,
        Creator: &creatorDataObject,
        CloseReason: &closeReasonDataObject,
        CloseComment: &closeCommentDataObject,
        Malware: malwareDataObject,
        SystemInfo: &systemInfoDataObject,
        Process: &listProcessDataObject,
        UserInfo: &listUserInfoDataObject,
        FileInfo: &listFileInfoDataObject,
        SystemAlertTable: &systemAlertTableDataObject,
    }
    request.Body = &model.ChangeAlertRequestBody{
        DataObject: dataObjectbody,
    }
    response, err := client.ChangeAlert(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	Response body of requests for updating alerts.
400	Response body for failed requests for updating alerts.

Error Codes

See **Error Codes**.

4.2 Incident Management

4.2.1 Querying the Incident List

Function

This API is used to query the incident list.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/search

Table 4-134 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-135 Request header parameters

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

Table 4-136 Request body parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	The number of records on each page.
offset	No	Integer	Offset.
sort_by	No	String	Sorting field: create_time | update_time
order	No	String	Sorting order. Options: **DESC** and **ASC**.
from_date	No	String	Search start time, for example, 2023-02-20T00:00:00.000Z.
to_date	No	String	Search end time, for example, 2023-02-27T23:59:59.999Z.
condition	No	**condition** object	Search condition expression.

Table 4-137 condition

Parameter	Mandatory	Type	Description
conditions	No	Array of **conditions** objects	Expression list.
logics	No	Array of strings	Expression name list.

Table 4-138 conditions

Parameter	Mandatory	Type	Description
name	No	String	Expression name.
data	No	Array of strings	Expression content list.

Response Parameters

Status code: 200

Table 4-139 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-140 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
total	Integer	Total number of incidents.
limit	Integer	The number of records on each page.
offset	Integer	Offset.
success	Boolean	Successful or not.
data	Array of **IncidentDetail** objects	Incident list.

Table 4-141 IncidentDetail

Parameter	Type	Description
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
data_object	**Incident** object	Incident entity information.
dataclass_ref	**dataclass_ref** object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
project_id	String	ID of the current project.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the alert was generated. If this parameter cannot be parsed, the default time zone GMT+8 is used.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-142 Incident

Parameter	Type	Description
version	String	Version of the incident object. The value must be the one released by the SSA service.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	String	ID of the region where the account to whom the data is delivered and hosted.

Parameter	Type	Description
workspace_id	String	ID of the current workspace.
labels	String	Tag (display only).
environment	**environment** object	Coordinates of the environment where the incident was generated.
data_source	**data_source** object	Data source reported for the first time.
first_observed_time	String	First discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
last_observed_time	String	Latest discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
arrive_time	String	Receiving time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
title	String	Incident title.
description	String	Incident description.
source_url	String	Incident URL, which points to the page displaying the current incident description in the data source product.
count	Integer	Incident occurrences.

Parameter	Type	Description
confidence	Integer	Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or problem. Value range: 0 to 100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.
severity	String	Severity level. Value range: Tips | Low | Medium | High | Fatal Note: **0**: Tips. No threats are found. **1**: Low. No actions are required for the threat. **2**: Medium. The threat needs to be handled but is not urgent. **3**: High. The threat must be handled preferentially. **4**: Fatal. The threat must be handled immediately to prevent further damage.
criticality	Integer	Criticality, which specifies the importance level of the resources involved in an incident. Value range: 0 to 100. **0** indicates that the resource is not critical, and **100** indicates that the resource is critical.
incident_type	**incident_type** object	Incident classification. For details, see the *Alert and Incident Type Definition*.
network_list	Array of **network_list** objects	Network information.
resource_list	Array of **resource_list** objects	Affected resources.
remediation	**remediation** object	Remedy measure.

Parameter	Type	Description
verification_state	String	Verification status, which identifies the accuracy of the incident. The options are as follows: **Unknown**: The incident is unknown **True_Positive**: The incident is confirmed. **False_Positive**: The incident is a false positive. The default value is **Unknown**.
handle_status	String	Incident handling status. The options are as follows: **Open**: Default status. **Block** **Closed** The default value is **Open**.
sla	Integer	Closure time: The deadline by which the incident must be resolved. Unit: hour.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
close_time	String	Closure time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
ipdrr_phase	String	Period/Handling phase No. **Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.
simulation	String	Debugging field.
actor	String	Incident investigator.
owner	String	Owner and service owner.

Parameter	Type	Description
creator	String	Creator.
close_reason	String	Closure reason. False detection Resolved Repeated Other
close_comment	String	Comment for the closure.
malware	**malware** object	Malware.
system_info	Object	System information.
process	Array of **process** objects	Process information.
user_info	Array of **user_info** objects	User information.
file_info	Array of **file_info** objects	File information.
system_alert_table	Object	Layout fields in the incident list.

Table 4-143 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Account ID.
region_id	String	Region ID. **global** is returned for global services.
cross_workspace_id	String	Source workspace ID before data delivery. In the source workspace, the value is null. After data delivery, the value is the ID of the delegated user.
project_id	String	Project ID. The default value is null for global services.

Table 4-144 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows: **1**: Cloud service **2**: Third-party product **3**: Private product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source product is located. For details about the value range, see "Regions and Endpoints".
company_name	String	Name of the company to which the data source product belongs.
product_name	String	Name of the data source product.
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection model list.

Table 4-145 incident_type

Parameter	Type	Description
category	String	Category.
incident_type	String	Incident type.

Table 4-146 network_list

Parameter	Type	Description
direction	String	Direction. The value can be **IN** or **OUT**.
protocol	String	Protocol, including Layer 7 and Layer 4 protocols. Reference: IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Parameter	Type	Description
src_ip	String	Source IP address.
src_port	Integer	Source port. Value range: 0 - 65535.
src_domain	String	Source domain name.
src_geo	**src_geo** object	Geographical location of the source IP address.
dest_ip	String	Destination IP address.
dest_port	String	Destination port. Value range: 0 to 65535.
dest_domain	String	Destination domain name.
dest_geo	**dest_geo** object	Geographical location of the destination IP address.

Table 4-147 src_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-148 dest_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-149 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type, which reuses the RMS type field.
provider	String	Cloud service name, which is the same as the **provider** field in the RMS service.
region_id	String	Region. Enter the value based on the cloud region ID.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the project to which the resource belongs, in UUID format.
ep_id	String	Enterprise project ID.
ep_name	String	Enterprise project name.
tags	String	Resource tags. 1. A maximum of 50 key-value pairs are supported. 2. The value can contain a maximum of 255 characters, including letters, digits, spaces, and special characters (+, -, =, ., _, :, /,@).

Table 4-150 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.
url	String	URL, which points to the general handling details for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-151 malware

Parameter	Type	Description
malware_family	String	Malicious family.
malware_class	String	Malware classification.

Table 4-152 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Path of the process execution file.
process_pid	Integer	Process ID.
process_uid	Integer	User ID associated with the process.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.
process_parent_path	String	Path of the parent process execution file.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	User ID associated with the parent process.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Path of the subprocess execution file.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	User ID associated with the subprocess.
process_child_cmdline	String	Subprocess command line.

Parameter	Type	Description
process_launche_time	String	Process start time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
process_terminate_time	String	Process end time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Table 4-153 user_info

Parameter	Type	Description
user_id	String	User ID (UID).
user_name	String	Username.

Table 4-154 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File content.
file_new_path	String	New file path/name.
file_hash	String	File hashes.
file_md5	String	File MD5 value.
file_sha256	String	SHA256 value of the file.
file_attr	String	File attributes.

Table 4-155 dataclass_ref

Parameter	Type	Description
id	String	Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.

Parameter	Type	Description
name	String	Data class name.

Status code: 400

Table 4-156 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-157 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Query the incident list. Time range: January 20, 2024 to January 26, 2024. Incident severity: Medium. Handling status: Open. Sorting order: By creation time in descending order. Page size: 10 records on each page. Return only the first page.

```
{
  "limit" : 10,
  "offset" : 0,
  "sort_by" : "create_time",
  "order" : "DESC",
  "condition" : {
    "conditions" : [ {
      "name" : "severity",
      "data" : [ "severity", "=", "Medium" ]
    }, {
      "name" : "handle_status",
      "data" : [ "handle_status", "=", "Open" ]
    } ],
    "logics" : [ "severity", "and", "handle_status" ]
  },
  "from_date" : "2024-01-20T00:00:00.000Z+0800",
  "to_date" : "2024-01-26T23:59:59.999Z+0800"
}
```

Example Responses

Status code: 200

Response body of the request for querying the incident list.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
```



```
"message" : "Error message",
"total" : 41,
"limit" : 2,
"offset" : 1,
"success" : true,
"data" : [ {
  "data_object" : {
    "version" : "1.0",
    "environment" : {
      "vendor_type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "data_source" : {
      "source_type" : 3,
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "first_observed_time" : "2021-01-30T23:00:00Z+0800",
    "last_observed_time" : "2021-01-30T23:00:00Z+0800",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "arrive_time" : "2021-01-30T23:00:00Z+0800",
    "title" : "MyXXX",
    "description" : "This my XXXX",
    "source_url" : "http://xxx",
    "count" : 4,
    "confidence" : 4,
    "severity" : "TIPS",
    "criticality" : 4,
    "incident_type" : { },
    "network_list" : [ {
      "direction" : {
        "IN" : null
      },
      "protocol" : "TCP",
      "src_ip" : "192.168.0.1",
      "src_port" : "1",
      "src_domain" : "xxx",
      "dest_ip" : "192.168.0.1",
      "dest_port" : "1",
      "dest_domain" : "xxx",
      "src_geo" : {
        "latitude" : 90,
        "longitude" : 180
      },
      "dest_geo" : {
        "latitude" : 90,
        "longitude" : 180
      }
    } ],
    "resource_list" : [ {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_name" : "MyXXX",
      "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    } ],
    "remediation" : {
      "recommendation" : "MyXXX",
      "url" : "MyXXX"
    },
    "verification_state" : "**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False
positive. The default value is **Unknown**.",
```

```
    "handle_status" : "**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is **Open**.",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.",
    "simulation" : "false",
    "actor" : "Tom",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "False positive; Resolved; Duplicate; Others",
    "close_comment" : "False positive; Resolved; Duplicate; Others",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "Malicious memory occupation."
    },
    "system_info" : { },
    "process" : [ {
      "process_name" : "MyXXX",
      "process_path" : "MyXXX",
      "process_pid" : 123,
      "process_uid" : 123,
      "process_cmdline" : "MyXXX"
    } ],
    "user_info" : [ {
      "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "user_name" : "MyXXX"
    } ],
    "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
    } ],
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
 } ]
}
```


SDK Sample Code

The SDK sample code is as follows.

Java

Query the incident list. Time range: January 20, 2024 to January 26, 2024. Incident severity: Medium. Handling status: Open. Sorting order: By creation time in descending order. Page size: 10 records on each page. Return only the first page.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
```



```
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class ListIncidentsSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListIncidentsRequest request = new ListIncidentsRequest();
        request.withWorkspaceId("{workspace_id}");
        DataobjectSearch body = new DataobjectSearch();
        List<String> listConditionLogics = new ArrayList<>();
        listConditionLogics.add("severity");
        listConditionLogics.add("and");
        listConditionLogics.add("handle_status");
        List<String> listConditionsData = new ArrayList<>();
        listConditionsData.add("handle_status");
        listConditionsData.add("=");
        listConditionsData.add("Open");
        List<String> listConditionsData1 = new ArrayList<>();
        listConditionsData1.add("severity");
        listConditionsData1.add("=");
        listConditionsData1.add("Medium");
        List<DataobjectSearchConditionConditions> listConditionConditions = new ArrayList<>();
        listConditionConditions.add(
            new DataobjectSearchConditionConditions()
                .withName("severity")
                .withData(listConditionsData1)
        );
        listConditionConditions.add(
            new DataobjectSearchConditionConditions()
                .withName("handle_status")
                .withData(listConditionsData)
        );
        DataobjectSearchCondition conditionbody = new DataobjectSearchCondition();
        conditionbody.withConditions(listConditionConditions)
            .withLogics(listConditionLogics);
        body.withCondition(conditionbody);
        body.withToDate("2024-01-26T23:59:59.999Z+0800");
        body.withFromDate("2024-01-20T00:00:00.000Z+0800");
        body.withOrder(DataobjectSearch.OrderEnum.fromValue("DESC"));
        body.withSortBy("create_time");
        body.withOffset(0);
        body.withLimit(10);
        request.withBody(body);
        try {
            ListIncidentsResponse response = client.listIncidents(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 incident list. Time range: January 20, 2024 to January 26, 2024. Incident severity: Medium. Handling status: Open. Sorting order: By creation time in descending order. Page size: 10 records on each page. Return only the first page.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListIncidentsRequest()
        request.workspace_id = "{workspace_id}"
        listLogicsCondition = [
            "severity",
            "and",
            "handle_status"
        ]
        listDataConditions = [
            "handle_status",
            "=",
            "Open"
        ]
        listDataConditions1 = [
            "severity",
            "=",
            "Medium"
        ]
        listConditionsCondition = [
            DataobjectSearchConditionConditions(
                name="severity",
                data=listDataConditions1
            ),
            DataobjectSearchConditionConditions(
                name="handle_status",
                data=listDataConditions
```



```
            )
        ]
        conditionbody = DataobjectSearchCondition(
            conditions=listConditionsCondition,
            logics=listLogicsCondition
        )
        request.body = DataobjectSearch(
            condition=conditionbody,
            to_date="2024-01-26T23:59:59.999Z+0800",
            from_date="2024-01-20T00:00:00.000Z+0800",
            order="DESC",
            sort_by="create_time",
            offset=0,
            limit=10
        )
        response = client.list_incidents(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 incident list. Time range: January 20, 2024 to January 26, 2024. Incident severity: Medium. Handling status: Open. Sorting order: By creation time in descending order. Page size: 10 records on each page. Return only the first page.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListIncidentsRequest{}
    request.WorkspaceId = "{workspace_id}"
    var listLogicsCondition = []string{
        "severity",
        "and",
        "handle_status",
    }
```



```
    var listDataConditions = []string{
        "handle_status",
        "=",
        "Open",
    }
    var listDataConditions1 = []string{
        "severity",
        "=",
        "Medium",
    }
    nameConditions:= "severity"
    nameConditions1:= "handle_status"
    var listConditionsCondition = []model.DataobjectSearchConditionConditions{
        {
            Name: &nameConditions,
            Data: &listDataConditions1,
        },
        {
            Name: &nameConditions1,
            Data: &listDataConditions,
        },
    }
    conditionbody := &model.DataobjectSearchCondition{
        Conditions: &listConditionsCondition,
        Logics: &listLogicsCondition,
    }
    toDateDataobjectSearch:= "2024-01-26T23:59:59.999Z+0800"
    fromDateDataobjectSearch:= "2024-01-20T00:00:00.000Z+0800"
    orderDataobjectSearch:= model.GetDataobjectSearchOrderEnum().DESC
    sortByDataobjectSearch:= "create_time"
    offsetDataobjectSearch:= int32(0)
    limitDataobjectSearch:= int32(10)
    request.Body = &model.DataobjectSearch{
        Condition: conditionbody,
        ToDate: &toDateDataobjectSearch,
        FromDate: &fromDateDataobjectSearch,
        Order: &orderDataobjectSearch,
        SortBy: &sortByDataobjectSearch,
        Offset: &offsetDataobjectSearch,
        Limit: &limitDataobjectSearch,
    }
    response, err := client.ListIncidents(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	Response body of the request for querying the incident list.
400	Response body of failed requests for querying the incident list.

Error Codes

See **Error Codes**.

4.2.2 Creating an Incident

Function

This API is used to create an incident.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents

Table 4-158 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-159 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.
content-type	Yes	String	Content type.

Table 4-160 Request body parameters

Parameter	Mandatory	Type	Description
data_object	No	**Incident** object	Incident entity information.

Table 4-161 Incident

Parameter	Mandatory	Type	Description
version	No	String	Version of the incident object. The value must be the one released by the SSA service.
id	No	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	No	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	No	String	ID of the region where the account to whom the data is delivered and hosted.
workspace_id	No	String	ID of the current workspace.
labels	No	String	Tag (display only).
environment	No	**environment** object	Coordinates of the environment where the incident was generated.
data_source	No	**data_source** object	Data source reported for the first time.
first_observed_time	No	String	First discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
last_observed_time	No	String	Latest discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Parameter	Mandatory	Type	Description
create_time	No	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
arrive_time	No	String	Receiving time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
title	No	String	Incident title.
description	No	String	Incident description.
source_url	No	String	Incident URL, which points to the page displaying the current incident description in the data source product.
count	No	Integer	Incident occurrences.
confidence	No	Integer	Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or problem. Value range: 0 to 100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.

Parameter	Mandatory	Type	Description
severity	No	String	Severity level. Value range: Tips | Low | Medium | High | Fatal Note: **0**: Tips. No threats are found. **1**: Low. No actions are required for the threat. **2**: Medium. The threat needs to be handled but is not urgent. **3**: High. The threat must be handled preferentially. **4**: Fatal. The threat must be handled immediately to prevent further damage.
criticality	No	Integer	Criticality, which specifies the importance level of the resources involved in an incident. Value range: 0 to 100. **0** indicates that the resource is not critical, and **100** indicates that the resource is critical.
incident_type	No	**incident_type** object	Incident classification. For details, see the *Alert and Incident Type Definition*.
network_list	No	Array of **network_list** objects	Network information.
resource_list	No	Array of **resource_list** objects	Affected resources.
remediation	No	**remediation** object	Remedy measure.

Parameter	Mandatory	Type	Description
verification_state	No	String	Verification status, which identifies the accuracy of the incident. The options are as follows: **Unknown**: The incident is unknown **True_Positive**: The incident is confirmed. **False_Positive**: The incident is a false positive. The default value is **Unknown**.
handle_status	No	String	Incident handling status. The options are as follows: **Open**: Default status. **Block** **Closed** The default value is **Open**.
sla	No	Integer	Closure time: The deadline by which the incident must be resolved. Unit: hour.
update_time	No	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
close_time	No	String	Closure time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Parameter	Mandatory	Type	Description
ipdrr_phase	No	String	Period/Handling phase No. **Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.
simulation	No	String	Debugging field.
actor	No	String	Incident investigator.
owner	No	String	Owner and service owner.
creator	No	String	Creator.
close_reason	No	String	Closure reason. False detection Resolved Repeated Other
close_comment	No	String	Comment for the closure.
malware	No	**malware** object	Malware.
system_info	No	Object	System information.
process	No	Array of **process** objects	Process information.
user_info	No	Array of **user_info** objects	User information.
file_info	No	Array of **file_info** objects	File information.
system_alert_table	No	Object	Layout fields in the incident list.

Table 4-162 environment

Parameter	Mandatory	Type	Description
vendor_type	No	String	Environment provider.
domain_id	No	String	Account ID.
region_id	No	String	Region ID. **global** is returned for global services.
cross_workspace_id	No	String	Source workspace ID before data delivery. In the source workspace, the value is null. After data delivery, the value is the ID of the delegated user.
project_id	No	String	Project ID. The default value is null for global services.

Table 4-163 data_source

Parameter	Mandatory	Type	Description
source_type	No	Integer	Data source type. The options are as follows: **1**: Cloud service **2**: Third-party product **3**: Private product
domain_id	No	String	Account ID to which the data source product belongs.
project_id	No	String	ID of the project to which the data source product belongs.
region_id	No	String	Region where the data source product is located. For details about the value range, see "Regions and Endpoints".
company_name	No	String	Name of the company to which the data source product belongs.
product_name	No	String	Name of the data source product.
product_feature	No	String	Name of the feature of the product that detects the incident.
product_module	No	String	Threat detection model list.

Table 4-164 incident_type

Parameter	Mandatory	Type	Description
category	No	String	Category.
incident_type	No	String	Incident type.

Table 4-165 network_list

Parameter	Mandatory	Type	Description
direction	No	String	Direction. The value can be **IN** or **OUT**.
protocol	No	String	Protocol, including Layer 7 and Layer 4 protocols. Reference: IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml
src_ip	No	String	Source IP address.
src_port	No	Integer	Source port. Value range: 0 - 65535.
src_domain	No	String	Source domain name.
src_geo	No	**src_geo** object	Geographical location of the source IP address.
dest_ip	No	String	Destination IP address.
dest_port	No	String	Destination port. Value range: 0 to 65535.
dest_domain	No	String	Destination domain name.
dest_geo	No	**dest_geo** object	Geographical location of the destination IP address.

Table 4-166 src_geo

Parameter	Mandatory	Type	Description
latitude	No	Number	Latitude.
longitude	No	Number	Longitude.
city_code	No	String	City Code.

Parameter	Mandatory	Type	Description
country_code	No	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-167 dest_geo

Parameter	Mandatory	Type	Description
latitude	No	Number	Latitude.
longitude	No	Number	Longitude.
city_code	No	String	City Code.
country_code	No	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-168 resource_list

Parameter	Mandatory	Type	Description
id	No	String	Cloud service resource ID.
name	No	String	Resource name.
type	No	String	Resource type, which reuses the RMS type field.
provider	No	String	Cloud service name, which is the same as the **provider** field in the RMS service.
region_id	No	String	Region. Enter the value based on the cloud region ID.
domain_id	No	String	ID of the account to which the resource belongs, in UUID format.
project_id	No	String	ID of the project to which the resource belongs, in UUID format.
ep_id	No	String	Enterprise project ID.
ep_name	No	String	Enterprise project name.

Parameter	Mandatory	Type	Description
tags	No	String	Resource tags. 1. A maximum of 50 key-value pairs are supported. 2. The value can contain a maximum of 255 characters, including letters, digits, spaces, and special characters (+, -, =, ., _, :, /,@).

Table 4-169 remediation

Parameter	Mandatory	Type	Description
recommendation	No	String	Recommended solution.
url	No	String	URL, which points to the general handling details for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-170 malware

Parameter	Mandatory	Type	Description
malware_family	No	String	Malicious family.
malware_class	No	String	Malware classification.

Table 4-171 process

Parameter	Mandatory	Type	Description
process_name	No	String	Process name.
process_path	No	String	Path of the process execution file.
process_pid	No	Integer	Process ID.
process_uid	No	Integer	User ID associated with the process.

Parameter	Mandatory	Type	Description
process_cmdline	No	String	Process command line.
process_parent_name	No	String	Parent process name.
process_parent_path	No	String	Path of the parent process execution file.
process_parent_pid	No	Integer	Parent process ID.
process_parent_uid	No	Integer	User ID associated with the parent process.
process_parent_cmdline	No	String	Parent process command line.
process_child_name	No	String	Subprocess name.
process_child_path	No	String	Path of the subprocess execution file.
process_child_pid	No	Integer	Subprocess ID.
process_child_uid	No	Integer	User ID associated with the subprocess.
process_child_cmdline	No	String	Subprocess command line.
process_launche_time	No	String	Process start time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
process_terminate_time	No	String	Process end time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Table 4-172 user_info

Parameter	Mandatory	Type	Description
user_id	No	String	User ID (UID).
user_name	No	String	Username.

Table 4-173 file_info

Parameter	Mandatory	Type	Description
file_path	No	String	File path/name.
file_content	No	String	File content.
file_new_path	No	String	New file path/name.
file_hash	No	String	File hashes.
file_md5	No	String	File MD5 value.
file_sha256	No	String	SHA256 value of the file.
file_attr	No	String	File attributes.

Response Parameters

Status code: 200

Table 4-174 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-175 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**IncidentDetail** object	Incident details object.

Table 4-176 IncidentDetail

Parameter	Type	Description
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
data_object	**Incident** object	Incident entity information.
dataclass_ref	**dataclass_ref** object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
project_id	String	ID of the current project.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the alert was generated. If this parameter cannot be parsed, the default time zone GMT+8 is used.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-177 Incident

Parameter	Type	Description
version	String	Version of the incident object. The value must be the one released by the SSA service.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	String	ID of the region where the account to whom the data is delivered and hosted.

Parameter	Type	Description
workspace_id	String	ID of the current workspace.
labels	String	Tag (display only).
environment	**environment** object	Coordinates of the environment where the incident was generated.
data_source	**data_source** object	Data source reported for the first time.
first_observed_time	String	First discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
last_observed_time	String	Latest discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
arrive_time	String	Receiving time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
title	String	Incident title.
description	String	Incident description.
source_url	String	Incident URL, which points to the page displaying the current incident description in the data source product.
count	Integer	Incident occurrences.

Parameter	Type	Description
confidence	Integer	Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or problem. Value range: 0 to 100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.
severity	String	Severity level. Value range: Tips | Low | Medium | High | Fatal Note: **0**: Tips. No threats are found. **1**: Low. No actions are required for the threat. **2**: Medium. The threat needs to be handled but is not urgent. **3**: High. The threat must be handled preferentially. **4**: Fatal. The threat must be handled immediately to prevent further damage.
criticality	Integer	Criticality, which specifies the importance level of the resources involved in an incident. Value range: 0 to 100. **0** indicates that the resource is not critical, and **100** indicates that the resource is critical.
incident_type	**incident_type** object	Incident classification. For details, see the *Alert and Incident Type Definition*.
network_list	Array of **network_list** objects	Network information.
resource_list	Array of **resource_list** objects	Affected resources.
remediation	**remediation** object	Remedy measure.

Parameter	Type	Description
verification_state	String	Verification status, which identifies the accuracy of the incident. The options are as follows: **Unknown**: The incident is unknown **True_Positive**: The incident is confirmed. **False_Positive**: The incident is a false positive. The default value is **Unknown**.
handle_status	String	Incident handling status. The options are as follows: **Open**: Default status. **Block** **Closed** The default value is **Open**.
sla	Integer	Closure time: The deadline by which the incident must be resolved. Unit: hour.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
close_time	String	Closure time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
ipdrr_phase	String	Period/Handling phase No. **Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.
simulation	String	Debugging field.
actor	String	Incident investigator.
owner	String	Owner and service owner.

Parameter	Type	Description
creator	String	Creator.
close_reason	String	Closure reason. False detection Resolved Repeated Other
close_comment	String	Comment for the closure.
malware	**malware** object	Malware.
system_info	Object	System information.
process	Array of **process** objects	Process information.
user_info	Array of **user_info** objects	User information.
file_info	Array of **file_info** objects	File information.
system_alert_table	Object	Layout fields in the incident list.

Table 4-178 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Account ID.
region_id	String	Region ID. **global** is returned for global services.
cross_workspace_id	String	Source workspace ID before data delivery. In the source workspace, the value is null. After data delivery, the value is the ID of the delegated user.
project_id	String	Project ID. The default value is null for global services.

Table 4-179 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows: **1**: Cloud service **2**: Third-party product **3**: Private product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source product is located. For details about the value range, see "Regions and Endpoints".
company_name	String	Name of the company to which the data source product belongs.
product_name	String	Name of the data source product.
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection model list.

Table 4-180 incident_type

Parameter	Type	Description
category	String	Category.
incident_type	String	Incident type.

Table 4-181 network_list

Parameter	Type	Description
direction	String	Direction. The value can be **IN** or **OUT**.
protocol	String	Protocol, including Layer 7 and Layer 4 protocols. Reference: IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Parameter	Type	Description
src_ip	String	Source IP address.
src_port	Integer	Source port. Value range: 0 - 65535.
src_domain	String	Source domain name.
src_geo	**src_geo** object	Geographical location of the source IP address.
dest_ip	String	Destination IP address.
dest_port	String	Destination port. Value range: 0 to 65535.
dest_domain	String	Destination domain name.
dest_geo	**dest_geo** object	Geographical location of the destination IP address.

Table 4-182 src_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-183 dest_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-184 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type, which reuses the RMS type field.
provider	String	Cloud service name, which is the same as the **provider** field in the RMS service.
region_id	String	Region. Enter the value based on the cloud region ID.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the project to which the resource belongs, in UUID format.
ep_id	String	Enterprise project ID.
ep_name	String	Enterprise project name.
tags	String	Resource tags. 1. A maximum of 50 key-value pairs are supported. 2. The value can contain a maximum of 255 characters, including letters, digits, spaces, and special characters (+, -, =, ., _, :, /,@).

Table 4-185 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.
url	String	URL, which points to the general handling details for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-186 malware

Parameter	Type	Description
malware_family	String	Malicious family.
malware_class	String	Malware classification.

Table 4-187 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Path of the process execution file.
process_pid	Integer	Process ID.
process_uid	Integer	User ID associated with the process.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.
process_parent_path	String	Path of the parent process execution file.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	User ID associated with the parent process.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Path of the subprocess execution file.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	User ID associated with the subprocess.
process_child_cmdline	String	Subprocess command line.

Parameter	Type	Description
process_launche_time	String	Process start time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
process_terminate_time	String	Process end time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Table 4-188 user_info

Parameter	Type	Description
user_id	String	User ID (UID).
user_name	String	Username.

Table 4-189 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File content.
file_new_path	String	New file path/name.
file_hash	String	File hashes.
file_md5	String	File MD5 value.
file_sha256	String	SHA256 value of the file.
file_attr	String	File attributes.

Table 4-190 dataclass_ref

Parameter	Type	Description
id	String	Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.

Parameter	Type	Description
name	String	Data class name.

Status code: 400

Table 4-191 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-192 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Create an incident. Set the incident title to MyXXX, tag to MyXXX, severity to tips, and occurrence times to 4.

```
{
  "data_object" : {
    "version" : "1.0",
    "environment" : {
      "vendor_type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "data_source" : {
      "source_type" : 3,
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "product_name" : "test",
      "product_feature" : "test"
    },
    "first_observed_time" : "2021-01-30T23:00:00Z+0800",
    "last_observed_time" : "2021-01-30T23:00:00Z+0800",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "arrive_time" : "2021-01-30T23:00:00Z+0800",
    "title" : "MyXXX",
    "labels" : "MyXXX",
    "description" : "This my XXXX",
    "source_url" : "http://xxx",
    "count" : 4,
    "confidence" : 4,
    "severity" : "TIPS",
    "criticality" : 4,
    "incident_type" : {
```



```
    "incident_type" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "category" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  },
  "network_list" : [ {
    "direction" : {
      "IN" : null
    },
    "protocol" : "TCP",
    "src_ip" : "192.168.0.1",
    "src_port" : "1",
    "src_domain" : "xxx",
    "dest_ip" : "192.168.0.1",
    "dest_port" : "1",
    "dest_domain" : "xxx",
    "src_geo" : {
      "latitude" : 90,
      "longitude" : 180
    },
    "dest_geo" : {
      "latitude" : 90,
      "longitude" : 180
    }
  } ],
  "resource_list" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "type" : "MyXXX",
    "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ep_name" : "MyXXX",
    "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  } ],
  "remediation" : {
    "recommendation" : "MyXXX",
    "url" : "MyXXX"
  },
  "verification_state" : "**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**.",
  "handle_status" : "**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is **Open**.",
  "sla" : 60000,
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "close_time" : "2021-01-30T23:00:00Z+0800",
  "ipdrr_phase" : "**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.",
  "simulation" : "false",
  "actor" : "Tom",
  "owner" : "MyXXX",
  "creator" : "MyXXX",
  "close_reason" : "False positive; Resolved; Duplicate; Others",
  "close_comment" : "False positive; Resolved; Duplicate; Others",
  "malware" : {
    "malware_family" : "family",
    "malware_class" : "Malicious memory occupation."
  },
  "system_info" : { },
  "process" : [ {
    "process_name" : "MyXXX",
    "process_path" : "MyXXX",
    "process_pid" : 123,
    "process_uid" : 123,
    "process_cmdline" : "MyXXX"
  } ],
  "user_info" : [ {
    "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "user_name" : "MyXXX"
  } ],
```



```
    "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
    } ],
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  }
}
```

Example Responses

Status code: 200

Response body for requests for creating incidents.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "data_object" : {
      "version" : "1.0",
      "environment" : {
        "vendor_type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "data_source" : {
        "source_type" : 3,
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "first_observed_time" : "2021-01-30T23:00:00Z+0800",
      "last_observed_time" : "2021-01-30T23:00:00Z+0800",
      "create_time" : "2021-01-30T23:00:00Z+0800",
      "arrive_time" : "2021-01-30T23:00:00Z+0800",
      "title" : "MyXXX",
      "description" : "This my XXXX",
      "source_url" : "http://xxx",
      "count" : 4,
      "confidence" : 4,
      "severity" : "TIPS",
      "criticality" : 4,
      "incident_type" : { },
      "network_list" : [ {
        "direction" : {
          "IN" : null
        },
        "protocol" : "TCP",
        "src_ip" : "192.168.0.1",
        "src_port" : "1",
        "src_domain" : "xxx",
        "dest_ip" : "192.168.0.1",
        "dest_port" : "1",
        "dest_domain" : "xxx",
        "src_geo" : {
          "latitude" : 90,
          "longitude" : 180
        },
        "dest_geo" : {
          "latitude" : 90,
          "longitude" : 180
        }
```



```
    } ],
    "resource_list" : [ {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_name" : "MyXXX",
      "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    } ],
    "remediation" : {
      "recommendation" : "MyXXX",
      "url" : "MyXXX"
    },
    "verification_state" : "**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**.",
    "handle_status" : "**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is **Open**.",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.",
    "simulation" : "false",
    "actor" : "Tom",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "False positive; Resolved; Duplicate; Others",
    "close_comment" : "False positive; Resolved; Duplicate; Others",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "Malicious memory occupation."
    },
    "system_info" : { },
    "process" : [ {
      "process_name" : "MyXXX",
      "process_path" : "MyXXX",
      "process_pid" : 123,
      "process_uid" : 123,
      "process_cmdline" : "MyXXX"
    } ],
    "user_info" : [ {
      "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "user_name" : "MyXXX"
    } ],
    "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
    } ],
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
 }
}
```


SDK Sample Code

The SDK sample code is as follows.

Java

Create an incident. Set the incident title to MyXXX, tag to MyXXX, severity to tips, and occurrence times to 4.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class CreateIncidentSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateIncidentRequest request = new CreateIncidentRequest();
        request.withWorkspaceId("{workspace_id}");
        CreateIncidentRequestBody body = new CreateIncidentRequestBody();
        List<IncidentFileInfo> listDataObjectFileInfo = new ArrayList<>();
        listDataObjectFileInfo.add(
            new IncidentFileInfo()
                .withFilePath("MyXXX")
                .withFileContent("MyXXX")
                .withFileNewPath("MyXXX")
                .withFileHash("MyXXX")
                .withFileMd5("MyXXX")
                .withFileSha256("MyXXX")
                .withFileAttr("MyXXX")
        );
        List<IncidentUserInfo> listDataObjectUserInfo = new ArrayList<>();
        listDataObjectUserInfo.add(
            new IncidentUserInfo()
                .withUserId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withUserName("MyXXX")
        );
        List<IncidentProcess> listDataObjectProcess = new ArrayList<>();
        listDataObjectProcess.add(
            new IncidentProcess()
                .withProcessName("MyXXX")
                .withProcessPath("MyXXX")
                .withProcessPid(123)
                .withProcessUid(123)
                .withProcessCmdline("MyXXX")
        );
```



```
IncidentMalware malwareDataObject = new IncidentMalware();
malwareDataObject.withMalwareFamily("family")
    .withMalwareClass("Malicious memory occupation.");
IncidentRemediation remediationDataObject = new IncidentRemediation();
remediationDataObject.withRecommendation("MyXXX")
    .withUrl("MyXXX");
List<IncidentResourceList> listDataObjectResourceList = new ArrayList<>();
listDataObjectResourceList.add(
    new IncidentResourceList()
        .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withName("MyXXX")
        .withType("MyXXX")
        .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withEpId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        .withEpName("MyXXX")
        .withTags("909494e3-558e-46b6-a9eb-07a8e18ca62f")
);
IncidentDestGeo destGeoNetworkList = new IncidentDestGeo();
destGeoNetworkList.withLatitude(java.math.BigDecimal.valueOf(90))
    .withLongitude(java.math.BigDecimal.valueOf(180));
IncidentSrcGeo srcGeoNetworkList = new IncidentSrcGeo();
srcGeoNetworkList.withLatitude(java.math.BigDecimal.valueOf(90))
    .withLongitude(java.math.BigDecimal.valueOf(180));
List<IncidentNetworkList> listDataObjectNetworkList = new ArrayList<>();
listDataObjectNetworkList.add(
    new IncidentNetworkList()
        .withDirection(IncidentNetworkList.DirectionEnum.fromValue("{}"))
        .withProtocol("TCP")
        .withSrcIp("192.168.0.1")
        .withSrcPort(1)
        .withSrcDomain("xxx")
        .withSrcGeo(srcGeoNetworkList)
        .withDestIp("192.168.0.1")
        .withDestPort("1")
        .withDestDomain("xxx")
        .withDestGeo(destGeoNetworkList)
);
IncidentIncidentType incidentTypeDataObject = new IncidentIncidentType();
incidentTypeDataObject.withCategory("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withIncidentType("909494e3-558e-46b6-a9eb-07a8e18ca62f");
IncidentDataSource dataSourceDataObject = new IncidentDataSource();
dataSourceDataObject.withSourceType(3)
    .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withProductName("test")
    .withProductFeature("test");
IncidentEnvironment environmentDataObject = new IncidentEnvironment();
environmentDataObject.withVendorType("MyXXX")
    .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
Incident dataObjectbody = new Incident();
dataObjectbody.withVersion("1.0")
    .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
    .withWorkspaceId("909494e3-558e-46b6-a9eb-07a8e18ca620")
    .withLabels("MyXXX")
    .withEnvironment(environmentDataObject)
    .withDataSource(dataSourceDataObject)
    .withFirstObservedTime("2021-01-30T23:00:00Z+0800")
    .withLastObservedTime("2021-01-30T23:00:00Z+0800")
    .withCreateTime("2021-01-30T23:00:00Z+0800")
    .withArriveTime("2021-01-30T23:00:00Z+0800")
    .withTitle("MyXXX")
    .withDescription("This my XXXX")
    .withSourceUrl("http://xxx")
    .withCount(4)
```



```
            .withConfidence(4)
            .withSeverity(Incident.SeverityEnum.fromValue("TIPS"))
            .withCriticality(4)
            .withIncidentType(incidentTypeDataObject)
            .withNetworkList(listDataObjectNetworkList)
            .withResourceList(listDataObjectResourceList)
            .withRemediation(remediationDataObject)
            .withVerificationState(Incident.VerificationStateEnum.fromValue("**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**."))
            .withHandleStatus(Incident.HandleStatusEnum.fromValue("**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is **Open**."))
            .withSla(60000)
            .withUpdateTime("2021-01-30T23:00:00Z+0800")
            .withCloseTime("2021-01-30T23:00:00Z+0800")
            .withIpdrrPhase(Incident.IpdrrPhaseEnum.fromValue("**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage."))
            .withSimulation("false")
            .withActor("Tom")
            .withOwner("MyXXX")
            .withCreator("MyXXX")
            .withCloseReason(Incident.CloseReasonEnum.fromValue("False positive; Resolved; Duplicate; Others"))
            .withCloseComment("False positive; Resolved; Duplicate; Others")
            .withMalware(malwareDataObject)
            .withSystemInfo(new Object())
            .withProcess(listDataObjectProcess)
            .withUserInfo(listDataObjectUserInfo)
            .withFileInfo(listDataObjectFileInfo);
        body.withDataObject(dataObjectbody);
        request.withBody(body);
        try {
            CreateIncidentResponse response = client.createIncident(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 an incident. Set the incident title to MyXXX, tag to MyXXX, severity to tips, and occurrence times to 4.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = CreateIncidentRequest()
    request.workspace_id = "{workspace_id}"
    listFileInfoDataObject = [
        IncidentFileInfo(
            file_path="MyXXX",
            file_content="MyXXX",
            file_new_path="MyXXX",
            file_hash="MyXXX",
            file_md5="MyXXX",
            file_sha256="MyXXX",
            file_attr="MyXXX"
        )
    ]
    listUserInfoDataObject = [
        IncidentUserInfo(
            user_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            user_name="MyXXX"
        )
    ]
    listProcessDataObject = [
        IncidentProcess(
            process_name="MyXXX",
            process_path="MyXXX",
            process_pid=123,
            process_uid=123,
            process_cmdline="MyXXX"
        )
    ]
    malwareDataObject = IncidentMalware(
        malware_family="family",
        malware_class="Malicious memory occupation."
    )
    remediationDataObject = IncidentRemediation(
        recommendation="MyXXX",
        url="MyXXX"
    )
    listResourceListDataObject = [
        IncidentResourceList(
            id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            name="MyXXX",
            type="MyXXX",
            region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            ep_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            ep_name="MyXXX",
            tags="909494e3-558e-46b6-a9eb-07a8e18ca62f"
        )
    ]
    destGeoNetworkList = IncidentDestGeo(
        latitude=90,
        longitude=180
    )
    srcGeoNetworkList = IncidentSrcGeo(
        latitude=90,
        longitude=180
    )
    listNetworkListDataObject = [
        IncidentNetworkList(
```



```
            direction="{}",
            protocol="TCP",
            src_ip="192.168.0.1",
            src_port=1,
            src_domain="xxx",
            src_geo=srcGeoNetworkList,
            dest_ip="192.168.0.1",
            dest_port="1",
            dest_domain="xxx",
            dest_geo=destGeoNetworkList
        )
    ]
    incidentTypeDataObject = IncidentIncidentType(
        category="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        incident_type="909494e3-558e-46b6-a9eb-07a8e18ca62f"
    )
    dataSourceDataObject = IncidentDataSource(
        source_type=3,
        domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        product_name="test",
        product_feature="test"
    )
    environmentDataObject = IncidentEnvironment(
        vendor_type="MyXXX",
        domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f"
    )
    dataObjectbody = Incident(
        version="1.0",
        id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        workspace_id="909494e3-558e-46b6-a9eb-07a8e18ca620",
        labels="MyXXX",
        environment=environmentDataObject,
        data_source=dataSourceDataObject,
        first_observed_time="2021-01-30T23:00:00Z+0800",
        last_observed_time="2021-01-30T23:00:00Z+0800",
        create_time="2021-01-30T23:00:00Z+0800",
        arrive_time="2021-01-30T23:00:00Z+0800",
        title="MyXXX",
        description="This my XXXX",
        source_url="http://xxx",
        count=4,
        confidence=4,
        severity="TIPS",
        criticality=4,
        incident_type=incidentTypeDataObject,
        network_list=listNetworkListDataObject,
        resource_list=listResourceListDataObject,
        remediation=remediationDataObject,
        verification_state="**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False
positive. The default value is **Unknown**.",
        handle_status="**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is
**Open**.",
        sla=60000,
        update_time="2021-01-30T23:00:00Z+0800",
        close_time="2021-01-30T23:00:00Z+0800",
        ipdrr_phase="**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis
stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-
Activity**: Post-incident activity stage.",
        simulation="false",
        actor="Tom",
        owner="MyXXX",
        creator="MyXXX",
        close_reason="False positive; Resolved; Duplicate; Others",
        close_comment="False positive; Resolved; Duplicate; Others",
        malware=malwareDataObject,
```



```
            system_info={},
            process=listProcessDataObject,
            user_info=listUserInfoDataObject,
            file_info=listFileInfoDataObject
        )
        request.body = CreateIncidentRequestBody(
            data_object=dataObjectbody
        )
        response = client.create_incident(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 incident. Set the incident title to MyXXX, tag to MyXXX, severity to tips, and occurrence times to 4.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateIncidentRequest{}
    request.WorkspaceId = "{workspace_id}"
    filePathFileInfo:= "MyXXX"
    fileContentFileInfo:= "MyXXX"
    fileNewPathFileInfo:= "MyXXX"
    fileHashFileInfo:= "MyXXX"
    fileMd5FileInfo:= "MyXXX"
    fileSha256FileInfo:= "MyXXX"
    fileAttrFileInfo:= "MyXXX"
    var listFileInfoDataObject = []model.IncidentFileInfo{
        {
            FilePath: &filePathFileInfo,
            FileContent: &fileContentFileInfo,
            FileNewPath: &fileNewPathFileInfo,
            FileHash: &fileHashFileInfo,
            FileMd5: &fileMd5FileInfo,
```



```
        FileSha256: &fileSha256FileInfo,
        FileAttr: &fileAttrFileInfo,
    },
}
userIdUserInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
userNameUserInfo:= "MyXXX"
var listUserInfoDataObject = []model.IncidentUserInfo{
    {
        UserId: &userIdUserInfo,
        UserName: &userNameUserInfo,
    },
}
processNameProcess:= "MyXXX"
processPathProcess:= "MyXXX"
processPidProcess:= int32(123)
processUidProcess:= int32(123)
processCmdlineProcess:= "MyXXX"
var listProcessDataObject = []model.IncidentProcess{
    {
        ProcessName: &processNameProcess,
        ProcessPath: &processPathProcess,
        ProcessPid: &processPidProcess,
        ProcessUid: &processUidProcess,
        ProcessCmdline: &processCmdlineProcess,
    },
}
malwareFamilyMalware:= "family"
malwareClassMalware:= "Malicious memory occupation."
malwareDataObject := &model.IncidentMalware{
    MalwareFamily: &malwareFamilyMalware,
    MalwareClass: &malwareClassMalware,
}
recommendationRemediation:= "MyXXX"
urlRemediation:= "MyXXX"
remediationDataObject := &model.IncidentRemediation{
    Recommendation: &recommendationRemediation,
    Url: &urlRemediation,
}
idResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
nameResourceList:= "MyXXX"
typeResourceList:= "MyXXX"
regionIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
domainIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
projectIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
epIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
epNameResourceList:= "MyXXX"
tagsResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
var listResourceListDataObject = []model.IncidentResourceList{
    {
        Id: &idResourceList,
        Name: &nameResourceList,
        Type: &typeResourceList,
        RegionId: &regionIdResourceList,
        DomainId: &domainIdResourceList,
        ProjectId: &projectIdResourceList,
        EpId: &epIdResourceList,
        EpName: &epNameResourceList,
        Tags: &tagsResourceList,
    },
}
latitudeDestGeo:= float32(90)
longitudeDestGeo:= float32(180)
destGeoNetworkList := &model.IncidentDestGeo{
    Latitude: &latitudeDestGeo,
    Longitude: &longitudeDestGeo,
}
latitudeSrcGeo:= float32(90)
longitudeSrcGeo:= float32(180)
srcGeoNetworkList := &model.IncidentSrcGeo{
```



```
    Latitude: &latitudeSrcGeo,
    Longitude: &longitudeSrcGeo,
}
directionNetworkList:= model.GetIncidentNetworkListDirectionEnum().{}
protocolNetworkList:= "TCP"
srcIpNetworkList:= "192.168.0.1"
srcPortNetworkList:= int32(1)
srcDomainNetworkList:= "xxx"
destIpNetworkList:= "192.168.0.1"
destPortNetworkList:= "1"
destDomainNetworkList:= "xxx"
var listNetworkListDataObject = []model.IncidentNetworkList{
    {
        Direction: &directionNetworkList,
        Protocol: &protocolNetworkList,
        SrcIp: &srcIpNetworkList,
        SrcPort: &srcPortNetworkList,
        SrcDomain: &srcDomainNetworkList,
        SrcGeo: srcGeoNetworkList,
        DestIp: &destIpNetworkList,
        DestPort: &destPortNetworkList,
        DestDomain: &destDomainNetworkList,
        DestGeo: destGeoNetworkList,
    },
}
categoryIncidentType:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
incidentTypeIncidentType:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
incidentTypeDataObject := &model.IncidentIncidentType{
    Category: &categoryIncidentType,
    IncidentType: &incidentTypeIncidentType,
}
sourceTypeDataSource:= int32(3)
domainIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
projectIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
regionIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
productNameDataSource:= "test"
productFeatureDataSource:= "test"
dataSourceDataObject := &model.IncidentDataSource{
    SourceType: &sourceTypeDataSource,
    DomainId: &domainIdDataSource,
    ProjectId: &projectIdDataSource,
    RegionId: &regionIdDataSource,
    ProductName: &productNameDataSource,
    ProductFeature: &productFeatureDataSource,
}
vendorTypeEnvironment:= "MyXXX"
domainIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
regionIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
projectIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
environmentDataObject := &model.IncidentEnvironment{
    VendorType: &vendorTypeEnvironment,
    DomainId: &domainIdEnvironment,
    RegionId: &regionIdEnvironment,
    ProjectId: &projectIdEnvironment,
}
versionDataObject:= "1.0"
idDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
workspaceIdDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca620"
labelsDataObject:= "MyXXX"
firstObservedTimeDataObject:= "2021-01-30T23:00:00Z+0800"
lastObservedTimeDataObject:= "2021-01-30T23:00:00Z+0800"
createTimeDataObject:= "2021-01-30T23:00:00Z+0800"
arriveTimeDataObject:= "2021-01-30T23:00:00Z+0800"
titleDataObject:= "MyXXX"
descriptionDataObject:= "This my XXXX"
sourceUrlDataObject:= "http://xxx"
countDataObject:= int32(4)
confidenceDataObject:= int32(4)
severityDataObject:= model.GetIncidentSeverityEnum().TIPS
```



```
    criticalityDataObject:= int32(4)
    verificationStateDataObject:=
model.GetIncidentVerificationStateEnum().**UNKNOWN**_UNKNOWN;_**TRUE_POSITIVE**_POSITIVE;_**FAL
SE_POSITIVE**_FALSE_POSITIVE__THE_DEFAULT_VALUE_IS_**UNKNOWN**_
    handleStatusDataObject:=
model.GetIncidentHandleStatusEnum().**OPEN**_OPEN;_**BLOCK**_PENDING;_**CLOSED**_CLOSED__THE_D
EFAULT_VALUE_IS_**OPEN**_
    slaDataObject:= int32(60000)
    updateTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    closeTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    ipdrrPhaseDataObject:=
model.GetIncidentIpdrrPhaseEnum().**PREPARATION**_PREPARATION_STAGE__**DETECTION_AND_ANALYSI
S**_DETECTION_AND_ANALYSIS_STAGE__**CONTAIN,_ERADICATION&_RECOVERY**_CONTAINMENT,_ERADIC
ATION,_AND_RECOVERY_STAGE__**POST_INCIDENT_ACTIVITY**_POST_INCIDENT_ACTIVITY_STAGE_
    simulationDataObject:= "false"
    actorDataObject:= "Tom"
    ownerDataObject:= "MyXXX"
    creatorDataObject:= "MyXXX"
    closeReasonDataObject:=
model.GetIncidentCloseReasonEnum().FALSE_POSITIVE;_RESOLVED;_DUPLICATE;_OTHERS
    closeCommentDataObject:= "False positive; Resolved; Duplicate; Others"
    var systemInfoDataObject interface{} = make(map[string]string)
    dataObjectbody := &model.Incident{
        Version: &versionDataObject,
        Id: &idDataObject,
        WorkspaceId: &workspaceIdDataObject,
        Labels: &labelsDataObject,
        Environment: environmentDataObject,
        DataSource: dataSourceDataObject,
        FirstObservedTime: &firstObservedTimeDataObject,
        LastObservedTime: &lastObservedTimeDataObject,
        CreateTime: &createTimeDataObject,
        ArriveTime: &arriveTimeDataObject,
        Title: &titleDataObject,
        Description: &descriptionDataObject,
        SourceUrl: &sourceUrlDataObject,
        Count: &countDataObject,
        Confidence: &confidenceDataObject,
        Severity: &severityDataObject,
        Criticality: &criticalityDataObject,
        IncidentType: incidentTypeDataObject,
        NetworkList: &listNetworkListDataObject,
        ResourceList: &listResourceListDataObject,
        Remediation: remediationDataObject,
        VerificationState: &verificationStateDataObject,
        HandleStatus: &handleStatusDataObject,
        Sla: &slaDataObject,
        UpdateTime: &updateTimeDataObject,
        CloseTime: &closeTimeDataObject,
        IpdrrPhase: &ipdrrPhaseDataObject,
        Simulation: &simulationDataObject,
        Actor: &actorDataObject,
        Owner: &ownerDataObject,
        Creator: &creatorDataObject,
        CloseReason: &closeReasonDataObject,
        CloseComment: &closeCommentDataObject,
        Malware: malwareDataObject,
        SystemInfo: &systemInfoDataObject,
        Process: &listProcessDataObject,
        UserInfo: &listUserInfoDataObject,
        FileInfo: &listFileInfoDataObject,
    }
    request.Body = &model.CreateIncidentRequestBody{
        DataObject: dataObjectbody,
    }
    response, err := client.CreateIncident(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	Response body for requests for creating incidents.
400	Response body for a failed request for creating incidents.

Error Codes

See **Error Codes**.

4.2.3 Deleting an Incident

Function

This API is used to delete an incident.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/incidents

Table 4-193 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-194 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.
content-type	Yes	String	Content type.

Table 4-195 Request body parameters

Parameter	Mandatory	Type	Description
batch_ids	No	Array of strings	IDs of deleted incidents.

Response Parameters

Status code: 200

Table 4-196 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-197 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**data** object	Returned objects for batch deleting incidents.

Table 4-198 data

Parameter	Type	Description
error_ids	Array of strings	Failed IDs.
success_ids	Array of strings	Succeeded IDs.

Status code: 400

Table 4-199 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-200 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Delete the incident whose ID is 909494e3-558e-46b6-a9eb-07a8e18ca621.

```
{
  "batch_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
}
```

Example Responses

Status code: 200

Incident deletion result.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "error_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
    "success_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Delete the incident whose ID is 909494e3-558e-46b6-a9eb-07a8e18ca621.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class DeleteIncidentSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteIncidentRequest request = new DeleteIncidentRequest();
        request.withWorkspaceId("{workspace_id}");
        DeleteIncidentRequestBody body = new DeleteIncidentRequestBody();
        List<String> listbodyBatchIds = new ArrayList<>();
        listbodyBatchIds.add("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withBatchIds(listbodyBatchIds);
        request.withBody(body);
        try {
            DeleteIncidentResponse response = client.deleteIncident(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 incident whose ID is 909494e3-558e-46b6-a9eb-07a8e18ca621.

```
# coding: utf-8
```



```
import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteIncidentRequest()
        request.workspace_id = "{workspace_id}"
        listBatchIdsbody = [
            "909494e3-558e-46b6-a9eb-07a8e18ca62f"
        ]
        request.body = DeleteIncidentRequestBody(
            batch_ids=listBatchIdsbody
        )
        response = client.delete_incident(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 incident whose ID is 909494e3-558e-46b6-a9eb-07a8e18ca621.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteIncidentRequest{}
    request.WorkspaceId = "{workspace_id}"
    var listBatchIdsbody = []string{
        "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    }
    request.Body = &model.DeleteIncidentRequestBody{
        BatchIds: &listBatchIdsbody,
    }
    response, err := client.DeleteIncident(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	Incident deletion result.
400	Response body for failed requests for deleting incidents.

Error Codes

See **Error Codes**.

4.2.4 Querying Details About an Incident

Function

This API is used to obtain the details about an incident.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/{incident_id}

Table 4-201 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
incident_id	Yes	String	Incident ID.

Request Parameters

Table 4-202 Request header parameters

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

Response Parameters

Status code: 200

Table 4-203 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**IncidentDetail** object	Incident details object.

Table 4-204 IncidentDetail

Parameter	Type	Description
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
data_object	**Incident** object	Incident entity information.
dataclass_ref	**dataclass_ref** object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
project_id	String	ID of the current project.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the alert was generated. If this parameter cannot be parsed, the default time zone GMT+8 is used.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-205 Incident

Parameter	Type	Description
version	String	Version of the incident object. The value must be the one released by the SSA service.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	String	ID of the region where the account to whom the data is delivered and hosted.

Parameter	Type	Description
workspace_id	String	ID of the current workspace.
labels	String	Tag (display only).
environment	**environment** object	Coordinates of the environment where the incident was generated.
data_source	**data_source** object	Data source reported for the first time.
first_observed_time	String	First discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
last_observed_time	String	Latest discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
arrive_time	String	Receiving time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
title	String	Incident title.
description	String	Incident description.
source_url	String	Incident URL, which points to the page displaying the current incident description in the data source product.
count	Integer	Incident occurrences.

Parameter	Type	Description
confidence	Integer	Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or problem. Value range: 0 to 100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.
severity	String	Severity level. Value range: Tips | Low | Medium | High | Fatal Note: **0**: Tips. No threats are found. **1**: Low. No actions are required for the threat. **2**: Medium. The threat needs to be handled but is not urgent. **3**: High. The threat must be handled preferentially. **4**: Fatal. The threat must be handled immediately to prevent further damage.
criticality	Integer	Criticality, which specifies the importance level of the resources involved in an incident. Value range: 0 to 100. **0** indicates that the resource is not critical, and **100** indicates that the resource is critical.
incident_type	**incident_type** object	Incident classification. For details, see the *Alert and Incident Type Definition*.
network_list	Array of **network_list** objects	Network information.
resource_list	Array of **resource_list** objects	Affected resources.
remediation	**remediation** object	Remedy measure.

Parameter	Type	Description
verification_state	String	Verification status, which identifies the accuracy of the incident. The options are as follows: **Unknown**: The incident is unknown **True_Positive**: The incident is confirmed. **False_Positive**: The incident is a false positive. The default value is **Unknown**.
handle_status	String	Incident handling status. The options are as follows: **Open**: Default status. **Block** **Closed** The default value is **Open**.
sla	Integer	Closure time: The deadline by which the incident must be resolved. Unit: hour.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
close_time	String	Closure time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
ipdrr_phase	String	Period/Handling phase No. **Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.
simulation	String	Debugging field.
actor	String	Incident investigator.
owner	String	Owner and service owner.

Parameter	Type	Description
creator	String	Creator.
close_reason	String	Closure reason. False detection Resolved Repeated Other
close_comment	String	Comment for the closure.
malware	**malware** object	Malware.
system_info	Object	System information.
process	Array of **process** objects	Process information.
user_info	Array of **user_info** objects	User information.
file_info	Array of **file_info** objects	File information.
system_alert_table	Object	Layout fields in the incident list.

Table 4-206 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Account ID.
region_id	String	Region ID. **global** is returned for global services.
cross_workspace_id	String	Source workspace ID before data delivery. In the source workspace, the value is null. After data delivery, the value is the ID of the delegated user.
project_id	String	Project ID. The default value is null for global services.

Table 4-207 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows: **1**: Cloud service **2**: Third-party product **3**: Private product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source product is located. For details about the value range, see "Regions and Endpoints".
company_name	String	Name of the company to which the data source product belongs.
product_name	String	Name of the data source product.
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection model list.

Table 4-208 incident_type

Parameter	Type	Description
category	String	Category.
incident_type	String	Incident type.

Table 4-209 network_list

Parameter	Type	Description
direction	String	Direction. The value can be **IN** or **OUT**.
protocol	String	Protocol, including Layer 7 and Layer 4 protocols. Reference: IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Parameter	Type	Description
src_ip	String	Source IP address.
src_port	Integer	Source port. Value range: 0 - 65535.
src_domain	String	Source domain name.
src_geo	**src_geo** object	Geographical location of the source IP address.
dest_ip	String	Destination IP address.
dest_port	String	Destination port. Value range: 0 to 65535.
dest_domain	String	Destination domain name.
dest_geo	**dest_geo** object	Geographical location of the destination IP address.

Table 4-210 src_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-211 dest_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-212 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type, which reuses the RMS type field.
provider	String	Cloud service name, which is the same as the **provider** field in the RMS service.
region_id	String	Region. Enter the value based on the cloud region ID.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the project to which the resource belongs, in UUID format.
ep_id	String	Enterprise project ID.
ep_name	String	Enterprise project name.
tags	String	Resource tags. 1. A maximum of 50 key-value pairs are supported. 2. The value can contain a maximum of 255 characters, including letters, digits, spaces, and special characters (+, -, =, ., _, :, /,@).

Table 4-213 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.
url	String	URL, which points to the general handling details for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-214 malware

Parameter	Type	Description
malware_family	String	Malicious family.
malware_class	String	Malware classification.

Table 4-215 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Path of the process execution file.
process_pid	Integer	Process ID.
process_uid	Integer	User ID associated with the process.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.
process_parent_path	String	Path of the parent process execution file.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	User ID associated with the parent process.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Path of the subprocess execution file.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	User ID associated with the subprocess.
process_child_cmdline	String	Subprocess command line.

Parameter	Type	Description
process_launche_time	String	Process start time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
process_terminate_time	String	Process end time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Table 4-216 user_info

Parameter	Type	Description
user_id	String	User ID (UID).
user_name	String	Username.

Table 4-217 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File content.
file_new_path	String	New file path/name.
file_hash	String	File hashes.
file_md5	String	File MD5 value.
file_sha256	String	SHA256 value of the file.
file_attr	String	File attributes.

Table 4-218 dataclass_ref

Parameter	Type	Description
id	String	Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.

Parameter	Type	Description
name	String	Data class name.

Status code: 400

Table 4-219 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response body for requests for querying incident details.


```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "data_object" : {
      "version" : "1.0",
      "environment" : {
        "vendor_type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "data_source" : {
        "source_type" : 3,
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "first_observed_time" : "2021-01-30T23:00:00Z+0800",
      "last_observed_time" : "2021-01-30T23:00:00Z+0800",
      "create_time" : "2021-01-30T23:00:00Z+0800",
      "arrive_time" : "2021-01-30T23:00:00Z+0800",
      "title" : "MyXXX",
      "description" : "This my XXXX",
      "source_url" : "http://xxx",
      "count" : "4",
      "confidence" : 4,
      "severity" : "TIPS",
      "criticality" : 4,
      "incident_type" : { },
      "network_list" : [ {
        "direction" : {
          "IN" : null
        },
        "protocol" : "TCP",
```



```
      "src_ip" : "192.168.0.1",
      "src_port" : "1",
      "src_domain" : "xxx",
      "dest_ip" : "192.168.0.1",
      "dest_port" : "1",
      "dest_domain" : "xxx",
      "src_geo" : {
        "latitude" : 90,
        "longitude" : 180
      },
      "dest_geo" : {
        "latitude" : 90,
        "longitude" : 180
      }
    } ],
    "resource_list" : [ {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_name" : "MyXXX",
      "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    } ],
    "remediation" : {
      "recommendation" : "MyXXX",
      "url" : "MyXXX"
    },
    "verification_state" : "**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**.",
    "handle_status" : "**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is **Open**.",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.",
    "simulation" : "false",
    "actor" : "Tom",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "False positive; Resolved; Duplicate; Others",
    "close_comment" : "False positive; Resolved; Duplicate; Others",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "Malicious memory occupation."
    },
    "system_info" : { },
    "process" : [ {
      "process_name" : "MyXXX",
      "process_path" : "MyXXX",
      "process_pid" : 123,
      "process_uid" : 123,
      "process_cmdline" : "MyXXX"
    } ],
    "user_info" : [ {
      "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "user_name" : "MyXXX"
    } ],
    "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
```



```
    } ],
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
 }
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowIncidentSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowIncidentRequest request = new ShowIncidentRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withIncidentId("{incident_id}");
        try {
            ShowIncidentResponse response = client.showIncident(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowIncidentRequest()
        request.workspace_id = "{workspace_id}"
        request.incident_id = "{incident_id}"
        response = client.show_incident(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowIncidentRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.IncidentId = "{incident_id}"
    response, err := client.ShowIncident(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	Response body for requests for querying incident details.
400	Response body for failed requests for querying incident details.

Error Codes

See **Error Codes**.

4.2.5 Updating an Incident

Function

This API is used to update an incident based on its attribute changes. The update works on only changed columns.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/{incident_id}

Table 4-220 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
incident_id	Yes	String	Incident ID.

Request Parameters

Table 4-221 Request header parameters

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

Table 4-222 Request body parameters

Parameter	Mandatory	Type	Description
batch_ids	No	Array of strings	IDs of updated incidents.
data_object	No	**Incident** object	Incident entity information.

Table 4-223 Incident

Parameter	Mandatory	Type	Description
version	No	String	Version of the incident object. The value must be the one released by the SSA service.
id	No	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.

Parameter	Mandatory	Type	Description
domain_id	No	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	No	String	ID of the region where the account to whom the data is delivered and hosted.
workspace_id	No	String	ID of the current workspace.
labels	No	String	Tag (display only).
environment	No	**environment** object	Coordinates of the environment where the incident was generated.
data_source	No	**data_source** object	Data source reported for the first time.
first_observed_time	No	String	First discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
last_observed_time	No	String	Latest discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
create_time	No	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Parameter	Mandatory	Type	Description
arrive_time	No	String	Receiving time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
title	No	String	Incident title.
description	No	String	Incident description.
source_url	No	String	Incident URL, which points to the page displaying the current incident description in the data source product.
count	No	Integer	Incident occurrences.
confidence	No	Integer	Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or problem. Value range: 0 to 100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.
severity	No	String	Severity level. Value range: Tips | Low | Medium | High | Fatal Note: **0**: Tips. No threats are found. **1**: Low. No actions are required for the threat. **2**: Medium. The threat needs to be handled but is not urgent. **3**: High. The threat must be handled preferentially. **4**: Fatal. The threat must be handled immediately to prevent further damage.

Parameter	Mandatory	Type	Description
criticality	No	Integer	Criticality, which specifies the importance level of the resources involved in an incident. Value range: 0 to 100. **0** indicates that the resource is not critical, and **100** indicates that the resource is critical.
incident_type	No	**incident_type** object	Incident classification. For details, see the *Alert and Incident Type Definition*.
network_list	No	Array of **network_list** objects	Network information.
resource_list	No	Array of **resource_list** objects	Affected resources.
remediation	No	**remediation** object	Remedy measure.
verification_state	No	String	Verification status, which identifies the accuracy of the incident. The options are as follows: **Unknown**: The incident is unknown **True_Positive**: The incident is confirmed. **False_Positive**: The incident is a false positive. The default value is **Unknown**.
handle_status	No	String	Incident handling status. The options are as follows: **Open**: Default status. **Block** **Closed** The default value is **Open**.
sla	No	Integer	Closure time: The deadline by which the incident must be resolved. Unit: hour.

Parameter	Mandatory	Type	Description
update_time	No	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
close_time	No	String	Closure time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
ipdrr_phase	No	String	Period/Handling phase No. **Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.
simulation	No	String	Debugging field.
actor	No	String	Incident investigator.
owner	No	String	Owner and service owner.
creator	No	String	Creator.
close_reason	No	String	Closure reason. False detection Resolved Repeated Other
close_comment	No	String	Comment for the closure.
malware	No	**malware** object	Malware.
system_info	No	Object	System information.

Parameter	Mandatory	Type	Description
process	No	Array of **process** objects	Process information.
user_info	No	Array of **user_info** objects	User information.
file_info	No	Array of **file_info** objects	File information.
system_alert_table	No	Object	Layout fields in the incident list.

Table 4-224 environment

Parameter	Mandatory	Type	Description
vendor_type	No	String	Environment provider.
domain_id	No	String	Account ID.
region_id	No	String	Region ID. **global** is returned for global services.
cross_workspace_id	No	String	Source workspace ID before data delivery. In the source workspace, the value is null. After data delivery, the value is the ID of the delegated user.
project_id	No	String	Project ID. The default value is null for global services.

Table 4-225 data_source

Parameter	Mandatory	Type	Description
source_type	No	Integer	Data source type. The options are as follows: **1**: Cloud service **2**: Third-party product **3**: Private product
domain_id	No	String	Account ID to which the data source product belongs.

Parameter	Mandatory	Type	Description
project_id	No	String	ID of the project to which the data source product belongs.
region_id	No	String	Region where the data source product is located. For details about the value range, see "Regions and Endpoints".
company_name	No	String	Name of the company to which the data source product belongs.
product_name	No	String	Name of the data source product.
product_feature	No	String	Name of the feature of the product that detects the incident.
product_module	No	String	Threat detection model list.

Table 4-226 incident_type

Parameter	Mandatory	Type	Description
category	No	String	Category.
incident_type	No	String	Incident type.

Table 4-227 network_list

Parameter	Mandatory	Type	Description
direction	No	String	Direction. The value can be **IN** or **OUT**.
protocol	No	String	Protocol, including Layer 7 and Layer 4 protocols. Reference: IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml
src_ip	No	String	Source IP address.

Parameter	Mandatory	Type	Description
src_port	No	Integer	Source port. Value range: 0 - 65535.
src_domain	No	String	Source domain name.
src_geo	No	**src_geo** object	Geographical location of the source IP address.
dest_ip	No	String	Destination IP address.
dest_port	No	String	Destination port. Value range: 0 to 65535.
dest_domain	No	String	Destination domain name.
dest_geo	No	**dest_geo** object	Geographical location of the destination IP address.

Table 4-228 src_geo

Parameter	Mandatory	Type	Description
latitude	No	Number	Latitude.
longitude	No	Number	Longitude.
city_code	No	String	City Code.
country_code	No	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-229 dest_geo

Parameter	Mandatory	Type	Description
latitude	No	Number	Latitude.
longitude	No	Number	Longitude.
city_code	No	String	City Code.
country_code	No	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-230 resource_list

Parameter	Mandatory	Type	Description
id	No	String	Cloud service resource ID.
name	No	String	Resource name.
type	No	String	Resource type, which reuses the RMS type field.
provider	No	String	Cloud service name, which is the same as the **provider** field in the RMS service.
region_id	No	String	Region. Enter the value based on the cloud region ID.
domain_id	No	String	ID of the account to which the resource belongs, in UUID format.
project_id	No	String	ID of the project to which the resource belongs, in UUID format.
ep_id	No	String	Enterprise project ID.
ep_name	No	String	Enterprise project name.
tags	No	String	Resource tags. 1. A maximum of 50 key-value pairs are supported. 2. The value can contain a maximum of 255 characters, including letters, digits, spaces, and special characters (+, -, =, ., _, :, /,@).

Table 4-231 remediation

Parameter	Mandatory	Type	Description
recommendation	No	String	Recommended solution.
url	No	String	URL, which points to the general handling details for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-232 malware

Parameter	Mandatory	Type	Description
malware_family	No	String	Malicious family.
malware_class	No	String	Malware classification.

Table 4-233 process

Parameter	Mandatory	Type	Description
process_name	No	String	Process name.
process_path	No	String	Path of the process execution file.
process_pid	No	Integer	Process ID.
process_uid	No	Integer	User ID associated with the process.
process_cmdline	No	String	Process command line.
process_parent_name	No	String	Parent process name.
process_parent_path	No	String	Path of the parent process execution file.
process_parent_pid	No	Integer	Parent process ID.
process_parent_uid	No	Integer	User ID associated with the parent process.
process_parent_cmdline	No	String	Parent process command line.
process_child_name	No	String	Subprocess name.
process_child_path	No	String	Path of the subprocess execution file.
process_child_pid	No	Integer	Subprocess ID.
process_child_uid	No	Integer	User ID associated with the subprocess.
process_child_cmdline	No	String	Subprocess command line.

Parameter	Mandatory	Type	Description
process_launche_time	No	String	Process start time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
process_terminate_time	No	String	Process end time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Table 4-234 user_info

Parameter	Mandatory	Type	Description
user_id	No	String	User ID (UID).
user_name	No	String	Username.

Table 4-235 file_info

Parameter	Mandatory	Type	Description
file_path	No	String	File path/name.
file_content	No	String	File content.
file_new_path	No	String	New file path/name.
file_hash	No	String	File hashes.
file_md5	No	String	File MD5 value.
file_sha256	No	String	SHA256 value of the file.
file_attr	No	String	File attributes.

Response Parameters

Status code: 200

Table 4-236 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-237 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**IncidentDetail** object	Incident details object.

Table 4-238 IncidentDetail

Parameter	Type	Description
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
data_object	**Incident** object	Incident entity information.
dataclass_ref	**dataclass_ref** object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
project_id	String	ID of the current project.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the alert was generated. If this parameter cannot be parsed, the default time zone GMT+8 is used.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-239 Incident

Parameter	Type	Description
version	String	Version of the incident object. The value must be the one released by the SSA service.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	String	ID of the region where the account to whom the data is delivered and hosted.
workspace_id	String	ID of the current workspace.
labels	String	Tag (display only).
environment	**environment** object	Coordinates of the environment where the incident was generated.
data_source	**data_source** object	Data source reported for the first time.
first_observed_time	String	First discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
last_observed_time	String	Latest discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Parameter	Type	Description
arrive_time	String	Receiving time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
title	String	Incident title.
description	String	Incident description.
source_url	String	Incident URL, which points to the page displaying the current incident description in the data source product.
count	Integer	Incident occurrences.
confidence	Integer	Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or problem. Value range: 0 to 100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.
severity	String	Severity level. Value range: Tips | Low | Medium | High | Fatal Note: **0**: Tips. No threats are found. **1**: Low. No actions are required for the threat. **2**: Medium. The threat needs to be handled but is not urgent. **3**: High. The threat must be handled preferentially. **4**: Fatal. The threat must be handled immediately to prevent further damage.
criticality	Integer	Criticality, which specifies the importance level of the resources involved in an incident. Value range: 0 to 100. **0** indicates that the resource is not critical, and **100** indicates that the resource is critical.
incident_type	**incident_type** object	Incident classification. For details, see the *Alert and Incident Type Definition*.
network_list	Array of **network_list** objects	Network information.

Parameter	Type	Description
resource_list	Array of **resource_list** objects	Affected resources.
remediation	**remediation** object	Remedy measure.
verification_state	String	Verification status, which identifies the accuracy of the incident. The options are as follows: **Unknown**: The incident is unknown **True_Positive**: The incident is confirmed. **False_Positive**: The incident is a false positive. The default value is **Unknown**.
handle_status	String	Incident handling status. The options are as follows: **Open**: Default status. **Block** **Closed** The default value is **Open**.
sla	Integer	Closure time: The deadline by which the incident must be resolved. Unit: hour.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
close_time	String	Closure time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
ipdrr_phase	String	Period/Handling phase No. **Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.

Parameter	Type	Description
simulation	String	Debugging field.
actor	String	Incident investigator.
owner	String	Owner and service owner.
creator	String	Creator.
close_reason	String	Closure reason. False detection Resolved Repeated Other
close_comment	String	Comment for the closure.
malware	**malware** object	Malware.
system_info	Object	System information.
process	Array of **process** objects	Process information.
user_info	Array of **user_info** objects	User information.
file_info	Array of **file_info** objects	File information.
system_alert_table	Object	Layout fields in the incident list.

Table 4-240 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Account ID.
region_id	String	Region ID. **global** is returned for global services.
cross_workspace_id	String	Source workspace ID before data delivery. In the source workspace, the value is null. After data delivery, the value is the ID of the delegated user.
project_id	String	Project ID. The default value is null for global services.

Table 4-241 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows: **1**: Cloud service **2**: Third-party product **3**: Private product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source product is located. For details about the value range, see "Regions and Endpoints".
company_name	String	Name of the company to which the data source product belongs.
product_name	String	Name of the data source product.
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection model list.

Table 4-242 incident_type

Parameter	Type	Description
category	String	Category.
incident_type	String	Incident type.

Table 4-243 network_list

Parameter	Type	Description
direction	String	Direction. The value can be **IN** or **OUT**.
protocol	String	Protocol, including Layer 7 and Layer 4 protocols. Reference: IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Parameter	Type	Description
src_ip	String	Source IP address.
src_port	Integer	Source port. Value range: 0 - 65535.
src_domain	String	Source domain name.
src_geo	**src_geo** object	Geographical location of the source IP address.
dest_ip	String	Destination IP address.
dest_port	String	Destination port. Value range: 0 to 65535.
dest_domain	String	Destination domain name.
dest_geo	**dest_geo** object	Geographical location of the destination IP address.

Table 4-244 src_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-245 dest_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-246 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type, which reuses the RMS type field.
provider	String	Cloud service name, which is the same as the **provider** field in the RMS service.
region_id	String	Region. Enter the value based on the cloud region ID.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the project to which the resource belongs, in UUID format.
ep_id	String	Enterprise project ID.
ep_name	String	Enterprise project name.
tags	String	Resource tags. 1. A maximum of 50 key-value pairs are supported. 2. The value can contain a maximum of 255 characters, including letters, digits, spaces, and special characters (+, -, =, ., _, :, /,@).

Table 4-247 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.
url	String	URL, which points to the general handling details for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-248 malware

Parameter	Type	Description
malware_family	String	Malicious family.
malware_class	String	Malware classification.

Table 4-249 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Path of the process execution file.
process_pid	Integer	Process ID.
process_uid	Integer	User ID associated with the process.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.
process_parent_path	String	Path of the parent process execution file.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	User ID associated with the parent process.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Path of the subprocess execution file.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	User ID associated with the subprocess.
process_child_cmdline	String	Subprocess command line.

Parameter	Type	Description
process_launche_time	String	Process start time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
process_terminate_time	String	Process end time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Table 4-250 user_info

Parameter	Type	Description
user_id	String	User ID (UID).
user_name	String	Username.

Table 4-251 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File content.
file_new_path	String	New file path/name.
file_hash	String	File hashes.
file_md5	String	File MD5 value.
file_sha256	String	SHA256 value of the file.
file_attr	String	File attributes.

Table 4-252 dataclass_ref

Parameter	Type	Description
id	String	Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.

Parameter	Type	Description
name	String	Data class name.

Status code: 400

Table 4-253 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-254 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Update an incident. Set the incident title to MyXXX, URL to http://xxx, occurrence times to 4, and confidence to 4.

```
{
  "data_object" : {
    "version" : "1.0",
    "environment" : {
      "vendor_type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "data_source" : {
      "source_type" : 3,
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "first_observed_time" : "2021-01-30T23:00:00Z+0800",
    "last_observed_time" : "2021-01-30T23:00:00Z+0800",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "arrive_time" : "2021-01-30T23:00:00Z+0800",
    "title" : "MyXXX",
    "description" : "This my XXXX",
    "source_url" : "http://xxx",
    "count" : 4,
    "confidence" : 4,
    "severity" : "TIPS",
    "criticality" : 4,
    "incident_type" : { },
    "network_list" : [ {
      "direction" : {
        "IN" : null
```



```
    },
    "protocol" : "TCP",
    "src_ip" : "192.168.0.1",
    "src_port" : "1",
    "src_domain" : "xxx",
    "dest_ip" : "192.168.0.1",
    "dest_port" : "1",
    "dest_domain" : "xxx",
    "src_geo" : {
      "latitude" : 90,
      "longitude" : 180
    },
    "dest_geo" : {
      "latitude" : 90,
      "longitude" : 180
    }
  } ],
  "resource_list" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "type" : "MyXXX",
    "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "ep_name" : "MyXXX",
    "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  } ],
  "remediation" : {
    "recommendation" : "MyXXX",
    "url" : "MyXXX"
  },
  "verification_state" : "**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**.",
  "handle_status" : "**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is **Open**.",
  "sla" : 60000,
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "close_time" : "2021-01-30T23:00:00Z+0800",
  "ipdrr_phase" : "**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.",
  "simulation" : "false",
  "actor" : "Tom",
  "owner" : "MyXXX",
  "creator" : "MyXXX",
  "close_reason" : "False positive; Resolved; Duplicate; Others",
  "close_comment" : "False positive; Resolved; Duplicate; Others",
  "malware" : {
    "malware_family" : "family",
    "malware_class" : "Malicious memory occupation."
  },
  "system_info" : { },
  "process" : [ {
    "process_name" : "MyXXX",
    "process_path" : "MyXXX",
    "process_pid" : 123,
    "process_uid" : 123,
    "process_cmdline" : "MyXXX"
  } ],
  "user_info" : [ {
    "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "user_name" : "MyXXX"
  } ],
  "file_info" : [ {
    "file_path" : "MyXXX",
    "file_content" : "MyXXX",
    "file_new_path" : "MyXXX",
    "file_hash" : "MyXXX",
    "file_md5" : "MyXXX",
```



```
    "file_sha256" : "MyXXX",
    "file_attr" : "MyXXX"
   } ],
   "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
   "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  }
}
```

Example Responses

Status code: 200

Response body of the request for updating an incident.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "data_object" : {
      "version" : "1.0",
      "environment" : {
        "vendor_type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "data_source" : {
        "source_type" : 3,
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
      },
      "first_observed_time" : "2021-01-30T23:00:00Z+0800",
      "last_observed_time" : "2021-01-30T23:00:00Z+0800",
      "create_time" : "2021-01-30T23:00:00Z+0800",
      "arrive_time" : "2021-01-30T23:00:00Z+0800",
      "title" : "MyXXX",
      "description" : "This my XXXX",
      "source_url" : "http://xxx",
      "count" : 4,
      "confidence" : 4,
      "severity" : "TIPS",
      "criticality" : 4,
      "incident_type" : { },
      "network_list" : [ {
        "direction" : {
          "IN" : null
        },
        "protocol" : "TCP",
        "src_ip" : "192.168.0.1",
        "src_port" : "1",
        "src_domain" : "xxx",
        "dest_ip" : "192.168.0.1",
        "dest_port" : "1",
        "dest_domain" : "xxx",
        "src_geo" : {
          "latitude" : 90,
          "longitude" : 180
        },
        "dest_geo" : {
          "latitude" : 90,
          "longitude" : 180
        }
      } ],
      "resource_list" : [ {
        "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        "name" : "MyXXX",
        "type" : "MyXXX",
        "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
```



```
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "ep_name" : "MyXXX",
      "tags" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    } ],
    "remediation" : {
      "recommendation" : "MyXXX",
      "url" : "MyXXX"
    },
    "verification_state" : "**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**.",
    "handle_status" : "**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is **Open**.",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.",
    "simulation" : "false",
    "actor" : "Tom",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "False positive; Resolved; Duplicate; Others",
    "close_comment" : "False positive; Resolved; Duplicate; Others",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "Malicious memory occupation."
    },
    "system_info" : { },
    "process" : [ {
      "process_name" : "MyXXX",
      "process_path" : "MyXXX",
      "process_pid" : 123,
      "process_uid" : 123,
      "process_cmdline" : "MyXXX"
    } ],
    "user_info" : [ {
      "user_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "user_name" : "MyXXX"
    } ],
    "file_info" : [ {
      "file_path" : "MyXXX",
      "file_content" : "MyXXX",
      "file_new_path" : "MyXXX",
      "file_hash" : "MyXXX",
      "file_md5" : "MyXXX",
      "file_sha256" : "MyXXX",
      "file_attr" : "MyXXX"
    } ],
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620"
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
 }
}
```


SDK Sample Code

The SDK sample code is as follows.

Java

Update an incident. Set the incident title to MyXXX, URL to http://xxx, occurrence times to 4, and confidence to 4.


```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class ChangeIncidentSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ChangeIncidentRequest request = new ChangeIncidentRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withIncidentId("{incident_id}");
        ChangeIncidentRequestBody body = new ChangeIncidentRequestBody();
        List<IncidentFileInfo> listDataObjectFileInfo = new ArrayList<>();
        listDataObjectFileInfo.add(
            new IncidentFileInfo()
                .withFilePath("MyXXX")
                .withFileContent("MyXXX")
                .withFileNewPath("MyXXX")
                .withFileHash("MyXXX")
                .withFileMd5("MyXXX")
                .withFileSha256("MyXXX")
                .withFileAttr("MyXXX")
        );
        List<IncidentUserInfo> listDataObjectUserInfo = new ArrayList<>();
        listDataObjectUserInfo.add(
            new IncidentUserInfo()
                .withUserId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withUserName("MyXXX")
        );
        List<IncidentProcess> listDataObjectProcess = new ArrayList<>();
        listDataObjectProcess.add(
            new IncidentProcess()
                .withProcessName("MyXXX")
                .withProcessPath("MyXXX")
                .withProcessPid(123)
                .withProcessUid(123)
                .withProcessCmdline("MyXXX")
        );
        IncidentMalware malwareDataObject = new IncidentMalware();
        malwareDataObject.withMalwareFamily("family")
            .withMalwareClass("Malicious memory occupation.");
        IncidentRemediation remediationDataObject = new IncidentRemediation();
```



```
        remediationDataObject.withRecommendation("MyXXX")
            .withUrl("MyXXX");
        List<IncidentResourceList> listDataObjectResourceList = new ArrayList<>();
        listDataObjectResourceList.add(
            new IncidentResourceList()
                .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withName("MyXXX")
                .withType("MyXXX")
                .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withEpId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withEpName("MyXXX")
                .withTags("909494e3-558e-46b6-a9eb-07a8e18ca62f")
        );
        IncidentDestGeo destGeoNetworkList = new IncidentDestGeo();
        destGeoNetworkList.withLatitude(java.math.BigDecimal.valueOf(90))
            .withLongitude(java.math.BigDecimal.valueOf(180));
        IncidentSrcGeo srcGeoNetworkList = new IncidentSrcGeo();
        srcGeoNetworkList.withLatitude(java.math.BigDecimal.valueOf(90))
            .withLongitude(java.math.BigDecimal.valueOf(180));
        List<IncidentNetworkList> listDataObjectNetworkList = new ArrayList<>();
        listDataObjectNetworkList.add(
            new IncidentNetworkList()
                .withDirection(IncidentNetworkList.DirectionEnum.fromValue("{}"))
                .withProtocol("TCP")
                .withSrcIp("192.168.0.1")
                .withSrcPort(1)
                .withSrcDomain("xxx")
                .withSrcGeo(srcGeoNetworkList)
                .withDestIp("192.168.0.1")
                .withDestPort("1")
                .withDestDomain("xxx")
                .withDestGeo(destGeoNetworkList)
        );
        IncidentDataSource dataSourceDataObject = new IncidentDataSource();
        dataSourceDataObject.withSourceType(3)
            .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        IncidentEnvironment environmentDataObject = new IncidentEnvironment();
        environmentDataObject.withVendorType("MyXXX")
            .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        Incident dataObjectbody = new Incident();
        dataObjectbody.withVersion("1.0")
            .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withWorkspaceId("909494e3-558e-46b6-a9eb-07a8e18ca620")
            .withEnvironment(environmentDataObject)
            .withDataSource(dataSourceDataObject)
            .withFirstObservedTime("2021-01-30T23:00:00Z+0800")
            .withLastObservedTime("2021-01-30T23:00:00Z+0800")
            .withCreateTime("2021-01-30T23:00:00Z+0800")
            .withArriveTime("2021-01-30T23:00:00Z+0800")
            .withTitle("MyXXX")
            .withDescription("This my XXXX")
            .withSourceUrl("http://xxx")
            .withCount(4)
            .withConfidence(4)
            .withSeverity(Incident.SeverityEnum.fromValue("TIPS"))
            .withCriticality(4)
            .withNetworkList(listDataObjectNetworkList)
            .withResourceList(listDataObjectResourceList)
            .withRemediation(remediationDataObject)
            .withVerificationState(Incident.VerificationStateEnum.fromValue("**Unknown**: Unknown;
**True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**."))
            .withHandleStatus(Incident.HandleStatusEnum.fromValue("**Open**: Open; **Block**: Pending;
**Closed**: Closed. The default value is **Open**."))
```



```
            .withSla(60000)
            .withUpdateTime("2021-01-30T23:00:00Z+0800")
            .withCloseTime("2021-01-30T23:00:00Z+0800")
            .withIpdrrPhase(Incident.IpdrrPhaseEnum.fromValue("**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage."))
            .withSimulation("false")
            .withActor("Tom")
            .withOwner("MyXXX")
            .withCreator("MyXXX")
            .withCloseReason(Incident.CloseReasonEnum.fromValue("False positive; Resolved; Duplicate; Others"))
            .withCloseComment("False positive; Resolved; Duplicate; Others")
            .withMalware(malwareDataObject)
            .withSystemInfo(new Object())
            .withProcess(listDataObjectProcess)
            .withUserInfo(listDataObjectUserInfo)
            .withFileInfo(listDataObjectFileInfo);
        body.withDataObject(dataObjectbody);
        request.withBody(body);
        try {
            ChangeIncidentResponse response = client.changeIncident(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 an incident. Set the incident title to MyXXX, URL to http://xxx, occurrence times to 4, and confidence to 4.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ChangeIncidentRequest()
```



```
request.workspace_id = "{workspace_id}"
request.incident_id = "{incident_id}"
listFileInfoDataObject = [
    IncidentFileInfo(
        file_path="MyXXX",
        file_content="MyXXX",
        file_new_path="MyXXX",
        file_hash="MyXXX",
        file_md5="MyXXX",
        file_sha256="MyXXX",
        file_attr="MyXXX"
    )
]
listUserInfoDataObject = [
    IncidentUserInfo(
        user_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        user_name="MyXXX"
    )
]
listProcessDataObject = [
    IncidentProcess(
        process_name="MyXXX",
        process_path="MyXXX",
        process_pid=123,
        process_uid=123,
        process_cmdline="MyXXX"
    )
]
malwareDataObject = IncidentMalware(
    malware_family="family",
    malware_class="Malicious memory occupation."
)
remediationDataObject = IncidentRemediation(
    recommendation="MyXXX",
    url="MyXXX"
)
listResourceListDataObject = [
    IncidentResourceList(
        id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        name="MyXXX",
        type="MyXXX",
        region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        ep_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        ep_name="MyXXX",
        tags="909494e3-558e-46b6-a9eb-07a8e18ca62f"
    )
]
destGeoNetworkList = IncidentDestGeo(
    latitude=90,
    longitude=180
)
srcGeoNetworkList = IncidentSrcGeo(
    latitude=90,
    longitude=180
)
listNetworkListDataObject = [
    IncidentNetworkList(
        direction="{}",
        protocol="TCP",
        src_ip="192.168.0.1",
        src_port=1,
        src_domain="xxx",
        src_geo=srcGeoNetworkList,
        dest_ip="192.168.0.1",
        dest_port="1",
        dest_domain="xxx",
        dest_geo=destGeoNetworkList
```



```
            )
        ]
        dataSourceDataObject = IncidentDataSource(
            source_type=3,
            domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f"
        )
        environmentDataObject = IncidentEnvironment(
            vendor_type="MyXXX",
            domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f"
        )
        dataObjectbody = Incident(
            version="1.0",
            id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            workspace_id="909494e3-558e-46b6-a9eb-07a8e18ca620",
            environment=environmentDataObject,
            data_source=dataSourceDataObject,
            first_observed_time="2021-01-30T23:00:00Z+0800",
            last_observed_time="2021-01-30T23:00:00Z+0800",
            create_time="2021-01-30T23:00:00Z+0800",
            arrive_time="2021-01-30T23:00:00Z+0800",
            title="MyXXX",
            description="This my XXXX",
            source_url="http://xxx",
            count=4,
            confidence=4,
            severity="TIPS",
            criticality=4,
            network_list=listNetworkListDataObject,
            resource_list=listResourceListDataObject,
            remediation=remediationDataObject,
            verification_state="**Unknown**: Unknown; **True_Positive**: Positive; **False_Positive**: False positive. The default value is **Unknown**.",
            handle_status="**Open**: Open; **Block**: Pending; **Closed**: Closed. The default value is **Open**.",
            sla=60000,
            update_time="2021-01-30T23:00:00Z+0800",
            close_time="2021-01-30T23:00:00Z+0800",
            ipdrr_phase="**Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.",
            simulation="false",
            actor="Tom",
            owner="MyXXX",
            creator="MyXXX",
            close_reason="False positive; Resolved; Duplicate; Others",
            close_comment="False positive; Resolved; Duplicate; Others",
            malware=malwareDataObject,
            system_info={},
            process=listProcessDataObject,
            user_info=listUserInfoDataObject,
            file_info=listFileInfoDataObject
        )
        request.body = ChangeIncidentRequestBody(
            data_object=dataObjectbody
        )
        response = client.change_incident(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 an incident. Set the incident title to MyXXX, URL to http://xxx, occurrence times to 4, and confidence to 4.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ChangeIncidentRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.IncidentId = "{incident_id}"
    filePathFileInfo:= "MyXXX"
    fileContentFileInfo:= "MyXXX"
    fileNewPathFileInfo:= "MyXXX"
    fileHashFileInfo:= "MyXXX"
    fileMd5FileInfo:= "MyXXX"
    fileSha256FileInfo:= "MyXXX"
    fileAttrFileInfo:= "MyXXX"
    var listFileInfoDataObject = []model.IncidentFileInfo{
        {
            FilePath: &filePathFileInfo,
            FileContent: &fileContentFileInfo,
            FileNewPath: &fileNewPathFileInfo,
            FileHash: &fileHashFileInfo,
            FileMd5: &fileMd5FileInfo,
            FileSha256: &fileSha256FileInfo,
            FileAttr: &fileAttrFileInfo,
        },
    }
    userIdUserInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    userNameUserInfo:= "MyXXX"
    var listUserInfoDataObject = []model.IncidentUserInfo{
        {
            UserId: &userIdUserInfo,
            UserName: &userNameUserInfo,
        },
    }
    processNameProcess:= "MyXXX"
    processPathProcess:= "MyXXX"
    processPidProcess:= int32(123)
```



```
processUidProcess:= int32(123)
processCmdlineProcess:= "MyXXX"
var listProcessDataObject = []model.IncidentProcess{
    {
        ProcessName: &processNameProcess,
        ProcessPath: &processPathProcess,
        ProcessPid: &processPidProcess,
        ProcessUid: &processUidProcess,
        ProcessCmdline: &processCmdlineProcess,
    },
}
malwareFamilyMalware:= "family"
malwareClassMalware:= "Malicious memory occupation."
malwareDataObject := &model.IncidentMalware{
    MalwareFamily: &malwareFamilyMalware,
    MalwareClass: &malwareClassMalware,
}
recommendationRemediation:= "MyXXX"
urlRemediation:= "MyXXX"
remediationDataObject := &model.IncidentRemediation{
    Recommendation: &recommendationRemediation,
    Url: &urlRemediation,
}
idResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
nameResourceList:= "MyXXX"
typeResourceList:= "MyXXX"
regionIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
domainIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
projectIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
epIdResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
epNameResourceList:= "MyXXX"
tagsResourceList:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
var listResourceListDataObject = []model.IncidentResourceList{
    {
        Id: &idResourceList,
        Name: &nameResourceList,
        Type: &typeResourceList,
        RegionId: &regionIdResourceList,
        DomainId: &domainIdResourceList,
        ProjectId: &projectIdResourceList,
        EpId: &epIdResourceList,
        EpName: &epNameResourceList,
        Tags: &tagsResourceList,
    },
}
latitudeDestGeo:= float32(90)
longitudeDestGeo:= float32(180)
destGeoNetworkList := &model.IncidentDestGeo{
    Latitude: &latitudeDestGeo,
    Longitude: &longitudeDestGeo,
}
latitudeSrcGeo:= float32(90)
longitudeSrcGeo:= float32(180)
srcGeoNetworkList := &model.IncidentSrcGeo{
    Latitude: &latitudeSrcGeo,
    Longitude: &longitudeSrcGeo,
}
directionNetworkList:= model.GetIncidentNetworkListDirectionEnum().{}
protocolNetworkList:= "TCP"
srcIpNetworkList:= "192.168.0.1"
srcPortNetworkList:= int32(1)
srcDomainNetworkList:= "xxx"
destIpNetworkList:= "192.168.0.1"
destPortNetworkList:= "1"
destDomainNetworkList:= "xxx"
var listNetworkListDataObject = []model.IncidentNetworkList{
    {
        Direction: &directionNetworkList,
        Protocol: &protocolNetworkList,
```



```
            SrcIp: &srcIpNetworkList,
            SrcPort: &srcPortNetworkList,
            SrcDomain: &srcDomainNetworkList,
            SrcGeo: srcGeoNetworkList,
            DestIp: &destIpNetworkList,
            DestPort: &destPortNetworkList,
            DestDomain: &destDomainNetworkList,
            DestGeo: destGeoNetworkList,
        },
    }
    sourceTypeDataSource:= int32(3)
    domainIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    projectIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    regionIdDataSource:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    dataSourceDataObject := &model.IncidentDataSource{
        SourceType: &sourceTypeDataSource,
        DomainId: &domainIdDataSource,
        ProjectId: &projectIdDataSource,
        RegionId: &regionIdDataSource,
    }
    vendorTypeEnvironment:= "MyXXX"
    domainIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    regionIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    projectIdEnvironment:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    environmentDataObject := &model.IncidentEnvironment{
        VendorType: &vendorTypeEnvironment,
        DomainId: &domainIdEnvironment,
        RegionId: &regionIdEnvironment,
        ProjectId: &projectIdEnvironment,
    }
    versionDataObject:= "1.0"
    idDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    workspaceIdDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca620"
    firstObservedTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    lastObservedTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    createTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    arriveTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    titleDataObject:= "MyXXX"
    descriptionDataObject:= "This my XXXX"
    sourceUrlDataObject:= "http://xxx"
    countDataObject:= int32(4)
    confidenceDataObject:= int32(4)
    severityDataObject:= model.GetIncidentSeverityEnum().TIPS
    criticalityDataObject:= int32(4)
    verificationStateDataObject:=
model.GetIncidentVerificationStateEnum().**UNKNOWN**_UNKNOWN;_**TRUE_POSITIVE**_POSITIVE;_**FAL
SE_POSITIVE**_FALSE_POSITIVE__THE_DEFAULT_VALUE_IS_**UNKNOWN**_
    handleStatusDataObject:=
model.GetIncidentHandleStatusEnum().**OPEN**_OPEN;_**BLOCK**_PENDING;_**CLOSED**_CLOSED__THE_D
EFAULT_VALUE_IS_**OPEN**_
    slaDataObject:= int32(60000)
    updateTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    closeTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    ipdrrPhaseDataObject:=
model.GetIncidentIpdrrPhaseEnum().**PREPARATION**_PREPARATION_STAGE__**DETECTION_AND_ANALYSI
S**_DETECTION_AND_ANALYSIS_STAGE__**CONTAIN,_ERADICATION&_RECOVERY**_CONTAINMENT,_ERADIC
ATION,_AND_RECOVERY_STAGE__**POST_INCIDENT_ACTIVITY**_POST_INCIDENT_ACTIVITY_STAGE_
    simulationDataObject:= "false"
    actorDataObject:= "Tom"
    ownerDataObject:= "MyXXX"
    creatorDataObject:= "MyXXX"
    closeReasonDataObject:=
model.GetIncidentCloseReasonEnum().FALSE_POSITIVE;_RESOLVED;_DUPLICATE;_OTHERS
    closeCommentDataObject:= "False positive; Resolved; Duplicate; Others"
    var systemInfoDataObject interface{} = make(map[string]string)
    dataObjectbody := &model.Incident{
        Version: &versionDataObject,
        Id: &idDataObject,
        WorkspaceId: &workspaceIdDataObject,
```



```
        Environment: environmentDataObject,
        DataSource: dataSourceDataObject,
        FirstObservedTime: &firstObservedTimeDataObject,
        LastObservedTime: &lastObservedTimeDataObject,
        CreateTime: &createTimeDataObject,
        ArriveTime: &arriveTimeDataObject,
        Title: &titleDataObject,
        Description: &descriptionDataObject,
        SourceUrl: &sourceUrlDataObject,
        Count: &countDataObject,
        Confidence: &confidenceDataObject,
        Severity: &severityDataObject,
        Criticality: &criticalityDataObject,
        NetworkList: &listNetworkListDataObject,
        ResourceList: &listResourceListDataObject,
        Remediation: remediationDataObject,
        VerificationState: &verificationStateDataObject,
        HandleStatus: &handleStatusDataObject,
        Sla: &slaDataObject,
        UpdateTime: &updateTimeDataObject,
        CloseTime: &closeTimeDataObject,
        IpdrrPhase: &ipdrrPhaseDataObject,
        Simulation: &simulationDataObject,
        Actor: &actorDataObject,
        Owner: &ownerDataObject,
        Creator: &creatorDataObject,
        CloseReason: &closeReasonDataObject,
        CloseComment: &closeCommentDataObject,
        Malware: malwareDataObject,
        SystemInfo: &systemInfoDataObject,
        Process: &listProcessDataObject,
        UserInfo: &listUserInfoDataObject,
        FileInfo: &listFileInfoDataObject,
    }
    request.Body = &model.ChangeIncidentRequestBody{
        DataObject: dataObjectbody,
    }
    response, err := client.ChangeIncident(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	Response body of the request for updating an incident.
400	Response body of the failed request for updating an incident.

Error Codes

See **Error Codes**.

4.3 Threat Indicator Management

4.3.1 Querying the Indicator List

Function

This API is used to query the indicator list.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/search

Table 4-255 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-256 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-257 Request body parameters

Parameter	Mandatory	Type	Description
ids	No	Array of strings	Threat indicator list.
dataclass_id	No	String	Data class ID.
condition	Yes	**condition** object	Search condition expression.

Parameter	Mandatory	Type	Description
offset	Yes	Integer	request offset, from 0
limit	Yes	Integer	request limit size
sort_by	No	String	sort by property, create_time.
from_date	No	String	Query start time, for example, 2024-01-20T00:00:00.000Z +0800.
to_date	No	String	Query end time, for example, 2024-01-26T23:59:59.999Z +0800.

Table 4-258 condition

Parameter	Mandatory	Type	Description
conditions	No	Array of **conditions** objects	Expression list.
logics	No	Array of strings	Expression name list.

Table 4-259 conditions

Parameter	Mandatory	Type	Description
name	No	String	Expression name.
data	No	Array of strings	Expression content list.

Response Parameters

Status code: 200

Table 4-260 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-261 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
total	Integer	Total number.
data	Array of **IndicatorDetail** objects	List of indicators.

Table 4-262 IndicatorDetail

Parameter	Type	Description
id	String	Threat indicator ID.
name	String	Threat indicator name.
data_object	**IndicatorDataObjectDetail** object	Indicator details.
workspace_id	String	Workspace ID.
project_id	String	Project ID.
dataclass_ref	**DataClassRefPojo** object	Data class object information.
create_time	String	Creation time.
update_time	String	Update time.

Table 4-263 IndicatorDataObjectDetail

Parameter	Type	Description
indicator_type	**indicator_type** object	Indicator type object.
value	String	Value, for example, **ip**, **url**, and **domain**.
update_time	String	Update time.
create_time	String	Creation time.
environment	**environment** object	Environment information.

Parameter	Type	Description
data_source	data_source object	Data source information.
first_report_time	String	First occurrence time.
is_deleted	Boolean	Whether to delete.
last_report_time	String	Last occurrence time.
granular_marking	Integer	Granularity (confidentiality level). **1**: First discovery; **2**: Self-produced data; **3**: Purchase required; and **4**: Direct query from the external network.
name	String	Name.
id	String	Threat indicator ID.
project_id	String	Project ID.
revoked	Boolean	Whether to discard.
status	String	Status. The options are **Open**, **Closed**, and **Revoked**.
verdict	String	Threat degree. The options are **Black**, **White**, and **Gray**.
workspace_id	String	Workspace ID.
confidence	Integer	Confidence. Value range: 80 to 100.

Table 4-264 indicator_type

Parameter	Type	Description
indicator_type	String	Indicator type.
id	String	Indicator type ID.

Table 4-265 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Account ID.
region_id	String	Region ID.
project_id	String	Project ID.

Table 4-266 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The value can be **1**, **2**, or **3**. **1**: Huawei Cloud product; **2**: Third-party products, and **3**: Your in-house products.
domain_id	String	Account ID.
project_id	String	Project ID.
region_id	String	Region ID.

Table 4-267 DataClassRefPojo

Parameter	Type	Description
id	String	Data class ID.
name	String	Data class name.

Status code: 400

Table 4-268 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-269 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Query the threat indicator list. IDs: id1 and id2; Name: indicator name; Type: DATA_SOURCE; Data class ID: 28f61af50fc9452aa0ed5ea25c3cc3d3; Offset: 0. A maximum of 10 indicators can be included. Returned indicators are sorted by create_time.

```
{
  "ids" : [ "id1", "id2" ],
```



```
 "dataclass_id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
 "condition" : {
  "conditions" : [ {
   "name" : "name",
   "data" : [ "name", "=", "Threat indicator name." ]
  } ],
  "logics" : [ "title" ]
 },
 "offset" : 0,
 "limit" : 10,
 "sort_by" : "create_time",
 "from_date" : "2024-01-20T00:00:00.000Z+0800",
 "to_date" : "2024-01-26T23:59:59.999Z+0800"
}
```

Example Responses

Status code: 200

Response to a successful request.

```
{
 "code" : "00000000",
 "data" : [ {
  "create_time" : "2023-07-24T20:54:19Z+0800",
  "data_object" : {
   "indicator_type" : {
    "indicator_type" : "ipv6",
    "id" : "ac794b2dfab9fe8c0676587301a636d3"
   },
   "revoked" : false,
   "workspace_id" : "d5baeef8-3e75-4e91-9826-fb208ac58987",
   "update_time" : "2023-07-24T20:54:19.038Z+0800",
   "project_id" : "15645222e8744afa985c93dab6341da6",
   "first_report_time" : "2023-07-31T20:54:12.000Z+0800",
   "id" : "ff61d1f8-0de4-4077-9e9b-e312f6829c6d",
   "granular_marking" : 1,
   "value" : "{}",
   "create_time" : "2023-07-24T20:54:19.038Z+0800",
   "confidence" : 80,
   "last_report_time" : "2023-07-25T20:54:15.000Z+0800",
   "data_source" : {
    "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
    "project_id" : "15645222e8744afa985c93dab6341da6",
    "region_id" : "xxx",
    "source_type" : 1
   },
   "environment" : {
    "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
    "project_id" : "15645222e8744afa985c93dab6341da6",
    "region_id" : "xxx",
    "vendor_type" : "xxx"
   },
   "verdict" : "Black",
   "name" : "test",
   "status" : "Open"
  },
  "dataclass_ref" : {
   "id" : "97ccf890-7480-31f6-a961-cf8da1f2f040",
   "name" : "name"
  },
  "id" : "ff61d1f8-0de4-4077-9e9b-e312f6829c6d",
  "update_time" : "2023-07-24T20:54:19Z+0800"
 } ],
 "message" : "",
 "total" : 2
}
```


SDK Sample Code

The SDK sample code is as follows.

Java

Query the threat indicator list. IDs: id1 and id2; Name: indicator name; Type: DATA_SOURCE; Data class ID: 28f61af50fc9452aa0ed5ea25c3cc3d3; Offset: 0. A maximum of 10 indicators can be included. Returned indicators are sorted by create_time.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class ListIndicatorsSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListIndicatorsRequest request = new ListIndicatorsRequest();
        request.withWorkspaceId("{workspace_id}");
        IndicatorListSearchRequest body = new IndicatorListSearchRequest();
        List<String> listConditionLogics = new ArrayList<>();
        listConditionLogics.add("title");
        List<String> listConditionsData = new ArrayList<>();
        listConditionsData.add("name");
        listConditionsData.add("=");
        listConditionsData.add("Threat indicator name.");
        List<IndicatorListSearchRequestConditionConditions> listConditionConditions = new ArrayList<>();
        listConditionConditions.add(
            new IndicatorListSearchRequestConditionConditions()
                .withName("name")
                .withData(listConditionsData)
        );
        IndicatorListSearchRequestCondition conditionbody = new IndicatorListSearchRequestCondition();
        conditionbody.withConditions(listConditionConditions)
            .withLogics(listConditionLogics);
        List<String> listbodyIds = new ArrayList<>();
        listbodyIds.add("id1");
        listbodyIds.add("id2");
```



```
        body.withToDate("2024-01-26T23:59:59.999Z+0800");
        body.withFromDate("2024-01-20T00:00:00.000Z+0800");
        body.withSortBy("create_time");
        body.withLimit(10);
        body.withOffset(0);
        body.withCondition(conditionbody);
        body.withDataclassId("28f61af50fc9452aa0ed5ea25c3cc3d3");
        body.withIds(listbodyIds);
        request.withBody(body);
        try {
            ListIndicatorsResponse response = client.listIndicators(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 threat indicator list. IDs: id1 and id2; Name: indicator name; Type: DATA_SOURCE; Data class ID: 28f61af50fc9452aa0ed5ea25c3cc3d3; Offset: 0. A maximum of 10 indicators can be included. Returned indicators are sorted by create_time.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListIndicatorsRequest()
        request.workspace_id = "{workspace_id}"
        listLogicsCondition = [
            "title"
        ]
        listDataConditions = [
            "name",
            "=",
            "Threat indicator name."
```



```
        ]
        listConditionsCondition = [
            IndicatorListSearchRequestConditionConditions(
                name="name",
                data=listDataConditions
            )
        ]
        conditionbody = IndicatorListSearchRequestCondition(
            conditions=listConditionsCondition,
            logics=listLogicsCondition
        )
        listIdsbody = [
            "id1",
            "id2"
        ]
        request.body = IndicatorListSearchRequest(
            to_date="2024-01-26T23:59:59.999Z+0800",
            from_date="2024-01-20T00:00:00.000Z+0800",
            sort_by="create_time",
            limit=10,
            offset=0,
            condition=conditionbody,
            dataclass_id="28f61af50fc9452aa0ed5ea25c3cc3d3",
            ids=listIdsbody
        )
        response = client.list_indicators(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 threat indicator list. IDs: id1 and id2; Name: indicator name; Type: DATA_SOURCE; Data class ID: 28f61af50fc9452aa0ed5ea25c3cc3d3; Offset: 0. A maximum of 10 indicators can be included. Returned indicators are sorted by create_time.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
```



```
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

    request := &model.ListIndicatorsRequest{}
    request.WorkspaceId = "{workspace_id}"
    var listLogicsCondition = []string{
        "title",
    }
    var listDataConditions = []string{
        "name",
        "=",
        "Threat indicator name.",
    }
    nameConditions:= "name"
    var listConditionsCondition = []model.IndicatorListSearchRequestConditionConditions{
        {
            Name: &nameConditions,
            Data: &listDataConditions,
        },
    }
    conditionbody := &model.IndicatorListSearchRequestCondition{
        Conditions: &listConditionsCondition,
        Logics: &listLogicsCondition,
    }
    var listIdsbody = []string{
        "id1",
        "id2",
    }
    toDateIndicatorListSearchRequest:= "2024-01-26T23:59:59.999Z+0800"
    fromDateIndicatorListSearchRequest:= "2024-01-20T00:00:00.000Z+0800"
    sortByIndicatorListSearchRequest:= "create_time"
    dataclassIdIndicatorListSearchRequest:= "28f61af50fc9452aa0ed5ea25c3cc3d3"
    request.Body = &model.IndicatorListSearchRequest{
        ToDate: &toDateIndicatorListSearchRequest,
        FromDate: &fromDateIndicatorListSearchRequest,
        SortBy: &sortByIndicatorListSearchRequest,
        Limit: int32(10),
        Offset: int32(0),
        Condition: conditionbody,
        DataclassId: &dataclassIdIndicatorListSearchRequest,
        Ids: &listIdsbody,
    }
    response, err := client.ListIndicators(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.3.2 Creating a Threat Indicator

Function

This API is used to create a threat indicator.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators

Table 4-270 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-271 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-272 Request body parameters

Parameter	Mandatory	Type	Description
data_object	Yes	**CreateIndicatorDetail** object	Indicator details.

Table 4-273 CreateIndicatorDetail

Parameter	Mandatory	Type	Description
data_source	Yes	**data_source** object	Data source information.
verdict	Yes	String	Threat level.
confidence	No	Integer	Confidence.
status	No	String	Status.
labels	No	String	Tag.
value	Yes	String	Value.
granular_marking	Yes	String	Granularity (confidentiality level). **1**: First discovery; **2**: Self-produced data; **3**: Purchase required; and **4**: Direct query from the external network.
environment	Yes	**environment** object	Environment information.
defanged	Yes	Boolean	Invalid or not.
first_report_time	Yes	String	First occurrence time.
last_report_time	No	String	Last occurrence time.
id	No	String	Threat indicator ID.
indicator_type	Yes	**indicator_type** object	Threat indicator type.
name	Yes	String	Threat indicator name.
dataclass_id	No	String	Data class ID.
workspace_id	Yes	String	workspace id
project_id	No	String	Project id value
dataclass	No	**DataClassRefPojo** object	Data class object information.
create_time	No	String	Create time
update_time	No	String	Update time

Table 4-274 data_source

Parameter	Mandatory	Type	Description
source_type	Yes	Integer	current page count
domain_id	Yes	String	Id value
project_id	Yes	String	Id value
region_id	Yes	String	Id value
product_name	Yes	String	Id value
product_feature	Yes	String	Id value

Table 4-275 environment

Parameter	Mandatory	Type	Description
vendor_type	Yes	String	Environment provider.
domain_id	Yes	String	Account ID.
region_id	Yes	String	Region ID.
project_id	Yes	String	Project ID.

Table 4-276 indicator_type

Parameter	Mandatory	Type	Description
indicator_type	Yes	String	Threat indicator type.
id	Yes	String	Indicator type ID.

Table 4-277 DataClassRefPojo

Parameter	Mandatory	Type	Description
id	Yes	String	Data class ID.
name	No	String	Data class name.

Response Parameters

Status code: 200

Table 4-278 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-279 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**IndicatorDetail** object	Indicator details.

Table 4-280 IndicatorDetail

Parameter	Type	Description
id	String	Threat indicator ID.
name	String	Threat indicator name.
data_object	**IndicatorDataObjectDetail** object	Indicator details.
workspace_id	String	Workspace ID.
project_id	String	Project ID.
dataclass_ref	**DataClassRefPojo** object	Data class object information.
create_time	String	Creation time.
update_time	String	Update time.

Table 4-281 IndicatorDataObjectDetail

Parameter	Type	Description
indicator_type	**indicator_type** object	Indicator type object.
value	String	Value, for example, **ip**, **url**, and **domain**.
update_time	String	Update time.

Parameter	Type	Description
create_time	String	Creation time.
environment	**environment** object	Environment information.
data_source	**data_source** object	Data source information.
first_report_time	String	First occurrence time.
is_deleted	Boolean	Whether to delete.
last_report_time	String	Last occurrence time.
granular_marking	Integer	Granularity (confidentiality level). **1**: First discovery; **2**: Self-produced data; **3**: Purchase required; and **4**: Direct query from the external network.
name	String	Name.
id	String	Threat indicator ID.
project_id	String	Project ID.
revoked	Boolean	Whether to discard.
status	String	Status. The options are **Open**, **Closed**, and **Revoked**.
verdict	String	Threat degree. The options are **Black**, **White**, and **Gray**.
workspace_id	String	Workspace ID.
confidence	Integer	Confidence. Value range: 80 to 100.

Table 4-282 indicator_type

Parameter	Type	Description
indicator_type	String	Indicator type.
id	String	Indicator type ID.

Table 4-283 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Account ID.

Parameter	Type	Description
region_id	String	Region ID.
project_id	String	Project ID.

Table 4-284 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The value can be **1**, **2**, or **3**. **1**: Huawei Cloud product; **2**: Third-party products, and **3**: Your in-house products.
domain_id	String	Account ID.
project_id	String	Project ID.
region_id	String	Region ID.

Table 4-285 DataClassRefPojo

Parameter	Type	Description
id	String	Data class ID.
name	String	Data class name.

Status code: 400

Table 4-286 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-287 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Create a threat indicator. Set its name to Threat Indicator Name, version to 1, type to DATA_SOURCE, and trigger flag to No.

```
{
  "data_object" : {
    "data_source" : {
      "source_type" : 3,
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "product_name" : "test",
      "product_feature" : "test"
    },
    "verdict" : "BLACK",
    "confidence" : 4,
    "status" : "OPEN",
    "labels" : "OPEN",
    "value" : "123",
    "granular_marking" : "1",
    "environment" : {
      "vendor_type" : "MyXXX",
      "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "defanged" : false,
    "first_report_time" : "2021-01-30T23:00:00Z+0800",
    "last_report_time" : "2021-01-30T23:00:00Z+0800",
    "indicator_type" : {
      "id" : "909494e3-558e-xxxxxx-07a8e18ca6xxx",
      "indicator_type" : "ipv6"
    },
    "name" : "Threat indicator name.",
    "dataclass_id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "dataclass" : {
      "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
      "name" : "Name."
    },
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800"
  }
}
```

Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
    "name" : "Threat indicator name.",
    "data_object" : {
      "indicator_type" : {
        "indicator_type" : "ipv6",
        "id" : "ac794b2dfab9fe8c0676587301a636d3"
      },
      "value" : "ip",
      "data_source" : {
        "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
        "project_id" : "5b8bb3c888db498f9eeaf1023f7ba597",
```



```
      "region_id" : "xxx",
      "source_type" : 1
    },
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "granular_marking" : 1,
    "first_report_time" : "2023-07-04T16:47:01Z+0800",
    "status" : "Open"
  },
  "dataclass_ref" : {
    "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
    "name" : "Name."
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800"
 }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Create a threat indicator. Set its name to Threat Indicator Name, version to 1, type to DATA_SOURCE, and trigger flag to No.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class CreateIndicatorSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateIndicatorRequest request = new CreateIndicatorRequest();
        request.withWorkspaceId("{workspace_id}");
        IndicatorCreateRequest body = new IndicatorCreateRequest();
        DataClassRefPojo dataclassDataObject = new DataClassRefPojo();
        dataclassDataObject.withId("28f61af50fc9452aa0ed5ea25c3cc3d3")
            .withName("Name.");
        CreateIndicatorDetailIndicatorType indicatorTypeDataObject = new
```

```
CreateIndicatorDetailIndicatorType();
        indicatorTypeDataObject.withIndicatorType("ipv6")
            .withId("909494e3-558e-xxxxxx-07a8e18ca6xxx");
        CreateIndicatorDetailEnvironment environmentDataObject = new CreateIndicatorDetailEnvironment();
        environmentDataObject.withVendorType("MyXXX")
            .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        CreateIndicatorDetailDataSource dataSourceDataObject = new CreateIndicatorDetailDataSource();
        dataSourceDataObject.withSourceType(3)
            .withDomainId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withRegionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withProductName("test")
            .withProductFeature("test");
        CreateIndicatorDetail dataObjectbody = new CreateIndicatorDetail();
        dataObjectbody.withDataSource(dataSourceDataObject)
            .withVerdict("BLACK")
            .withConfidence(4)
            .withStatus("OPEN")
            .withLabels("OPEN")
            .withValue("123")
            .withGranularMarking("1")
            .withEnvironment(environmentDataObject)
            .withDefanged(false)
            .withFirstReportTime("2021-01-30T23:00:00Z+0800")
            .withLastReportTime("2021-01-30T23:00:00Z+0800")
            .withIndicatorType(indicatorTypeDataObject)
            .withName("Threat indicator name.")
            .withDataclassId("28f61af50fc9452aa0ed5ea25c3cc3d3")
            .withWorkspaceId("909494e3-558e-46b6-a9eb-07a8e18ca620")
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withDataclass(dataclassDataObject)
            .withCreateTime("2021-01-30T23:00:00Z+0800")
            .withUpdateTime("2021-01-30T23:00:00Z+0800");
        body.withDataObject(dataObjectbody);
        request.withBody(body);
        try {
            CreateIndicatorResponse response = client.createIndicator(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 threat indicator. Set its name to Threat Indicator Name, version to 1, type to DATA_SOURCE, and trigger flag to No.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateIndicatorRequest()
        request.workspace_id = "{workspace_id}"
        dataclassDataObject = DataClassRefPojo(
            id="28f61af50fc9452aa0ed5ea25c3cc3d3",
            name="Name."
        )
        indicatorTypeDataObject = CreateIndicatorDetailIndicatorType(
            indicator_type="ipv6",
            id="909494e3-558e-xxxxxx-07a8e18ca6xxx"
        )
        environmentDataObject = CreateIndicatorDetailEnvironment(
            vendor_type="MyXXX",
            domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f"
        )
        dataSourceDataObject = CreateIndicatorDetailDataSource(
            source_type=3,
            domain_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            region_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            product_name="test",
            product_feature="test"
        )
        dataObjectbody = CreateIndicatorDetail(
            data_source=dataSourceDataObject,
            verdict="BLACK",
            confidence=4,
            status="OPEN",
            labels="OPEN",
            value="123",
            granular_marking="1",
            environment=environmentDataObject,
            defanged=False,
            first_report_time="2021-01-30T23:00:00Z+0800",
            last_report_time="2021-01-30T23:00:00Z+0800",
            indicator_type=indicatorTypeDataObject,
            name="Threat indicator name.",
            dataclass_id="28f61af50fc9452aa0ed5ea25c3cc3d3",
            workspace_id="909494e3-558e-46b6-a9eb-07a8e18ca620",
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            dataclass=dataclassDataObject,
            create_time="2021-01-30T23:00:00Z+0800",
            update_time="2021-01-30T23:00:00Z+0800"
        )
        request.body = IndicatorCreateRequest(
            data_object=dataObjectbody
        )
        response = client.create_indicator(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 threat indicator. Set its name to Threat Indicator Name, version to 1, type to DATA_SOURCE, and trigger flag to No.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateIndicatorRequest{}
    request.WorkspaceId = "{workspace_id}"
    nameDataclass:= "Name."
    dataclassDataObject := &model.DataClassRefPojo{
        Id: "28f61af50fc9452aa0ed5ea25c3cc3d3",
        Name: &nameDataclass,
    }
    indicatorTypeDataObject := &model.CreateIndicatorDetailIndicatorType{
        IndicatorType: "ipv6",
        Id: "909494e3-558e-xxxxxx-07a8e18ca6xxx",
    }
    environmentDataObject := &model.CreateIndicatorDetailEnvironment{
        VendorType: "MyXXX",
        DomainId: "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        RegionId: "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        ProjectId: "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    }
    dataSourceDataObject := &model.CreateIndicatorDetailDataSource{
        SourceType: int32(3),
        DomainId: "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        ProjectId: "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        RegionId: "909494e3-558e-46b6-a9eb-07a8e18ca62f",
        ProductName: "test",
        ProductFeature: "test",
    }
    confidenceDataObject:= int32(4)
    statusDataObject:= "OPEN"
    labelsDataObject:= "OPEN"
    lastReportTimeDataObject:= "2021-01-30T23:00:00Z+0800"
```



```
    dataclassIdDataObject:= "28f61af50fc9452aa0ed5ea25c3cc3d3"
    projectIdDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    createTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    updateTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    dataObjectbody := &model.CreateIndicatorDetail{
        DataSource: dataSourceDataObject,
        Verdict: "BLACK",
        Confidence: &confidenceDataObject,
        Status: &statusDataObject,
        Labels: &labelsDataObject,
        Value: "123",
        GranularMarking: "1",
        Environment: environmentDataObject,
        Defanged: false,
        FirstReportTime: "2021-01-30T23:00:00Z+0800",
        LastReportTime: &lastReportTimeDataObject,
        IndicatorType: indicatorTypeDataObject,
        Name: "Threat indicator name.",
        DataclassId: &dataclassIdDataObject,
        WorkspaceId: "909494e3-558e-46b6-a9eb-07a8e18ca620",
        ProjectId: &projectIdDataObject,
        Dataclass: dataclassDataObject,
        CreateTime: &createTimeDataObject,
        UpdateTime: &updateTimeDataObject,
    }
    request.Body = &model.IndicatorCreateRequest{
        DataObject: dataObjectbody,
    }
    response, err := client.CreateIndicator(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.3.3 Deleting a Threat Indicator

Function

Deleting a Threat Indicator

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/indicators

Table 4-288 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-289 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-290 Request body parameters

Parameter	Mandatory	Type	Description
batch_ids	No	Array of strings	Threat indicator list.

Response Parameters

Status code: 200

Table 4-291 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-292 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**IndicatorBatchOperateResponse** object	Indicator response parameters.

Table 4-293 IndicatorBatchOperateResponse

Parameter	Type	Description
success_ids	Array of strings	Succeeded IDs.
error_ids	Array of strings	Failed IDs.

Status code: 400

Table 4-294 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-295 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Delete a threat indicator. Batch ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f

```
{
  "batch_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
}
```

Example Responses

Status code: 200

Response to a successful request.


```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "success_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
    "error_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Delete a threat indicator. Batch ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class DeleteIndicatorSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteIndicatorRequest request = new DeleteIndicatorRequest();
        request.withWorkspaceId("{workspace_id}");
        DeleteIndicatorRequestBody body = new DeleteIndicatorRequestBody();
        List<String> listbodyBatchIds = new ArrayList<>();
        listbodyBatchIds.add("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withBatchIds(listbodyBatchIds);
        request.withBody(body);
        try {
            DeleteIndicatorResponse response = client.deleteIndicator(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 a threat indicator. Batch ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteIndicatorRequest()
        request.workspace_id = "{workspace_id}"
        listBatchIdsbody = [
            "909494e3-558e-46b6-a9eb-07a8e18ca62f"
        ]
        request.body = DeleteIndicatorRequestBody(
            batch_ids=listBatchIdsbody
        )
        response = client.delete_indicator(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 a threat indicator. Batch ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteIndicatorRequest{}
    request.WorkspaceId = "{workspace_id}"
    var listBatchIdsbody = []string{
        "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    }
    request.Body = &model.DeleteIndicatorRequestBody{
        BatchIds: &listBatchIdsbody,
    }
    response, err := client.DeleteIndicator(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	Response to a successful request.
400	Response to a failed request.

Error Codes

See **Error Codes**.

4.3.4 Querying Details About a Threat Indicator

Function

This API is used to query the details about a threat indicator.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/{indicator_id}

Table 4-296 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
indicator_id	Yes	String	Threat indicator ID.

Request Parameters

Table 4-297 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-298 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-299 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**IndicatorDetail** object	Indicator details.

Table 4-300 IndicatorDetail

Parameter	Type	Description
id	String	Threat indicator ID.
name	String	Threat indicator name.
data_object	**IndicatorDataObjectDetail** object	Indicator details.
workspace_id	String	Workspace ID.
project_id	String	Project ID.
dataclass_ref	**DataClassRefPojo** object	Data class object information.
create_time	String	Creation time.
update_time	String	Update time.

Table 4-301 IndicatorDataObjectDetail

Parameter	Type	Description
indicator_type	**indicator_type** object	Indicator type object.
value	String	Value, for example, **ip**, **url**, and **domain**.
update_time	String	Update time.
create_time	String	Creation time.
environment	**environment** object	Environment information.
data_source	**data_source** object	Data source information.
first_report_time	String	First occurrence time.

Parameter	Type	Description
is_deleted	Boolean	Whether to delete.
last_report_time	String	Last occurrence time.
granular_marking	Integer	Granularity (confidentiality level). **1**: First discovery; **2**: Self-produced data; **3**: Purchase required; and **4**: Direct query from the external network.
name	String	Name.
id	String	Threat indicator ID.
project_id	String	Project ID.
revoked	Boolean	Whether to discard.
status	String	Status. The options are **Open**, **Closed**, and **Revoked**.
verdict	String	Threat degree. The options are **Black**, **White**, and **Gray**.
workspace_id	String	Workspace ID.
confidence	Integer	Confidence. Value range: 80 to 100.

Table 4-302 indicator_type

Parameter	Type	Description
indicator_type	String	Indicator type.
id	String	Indicator type ID.

Table 4-303 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Account ID.
region_id	String	Region ID.
project_id	String	Project ID.

Table 4-304 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The value can be **1**, **2**, or **3**. **1**: Huawei Cloud product; **2**: Third-party products, and **3**: Your in-house products.
domain_id	String	Account ID.
project_id	String	Project ID.
region_id	String	Region ID.

Table 4-305 DataClassRefPojo

Parameter	Type	Description
id	String	Data class ID.
name	String	Data class name.

Status code: 400

Table 4-306 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-307 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response to a successful request.


```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
    "name" : "Indicator name.",
    "data_object" : {
      "indicator_type" : {
        "indicator_type" : "ipv6",
        "id" : "ac794b2dfab9fe8c0676587301a636d3"
      },
      "value" : "ip",
      "data_source" : {
        "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
        "project_id" : "5b8bb3c888db498f9eeaf1023f7ba597",
        "region_id" : "xxx",
        "source_type" : 1
      },
      "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "granular_marking" : 1,
      "first_report_time" : "2023-07-04T16:47:01Z+0800",
      "status" : "Open"
    },
    "dataclass_ref" : {
      "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
      "name" : "Name."
    },
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800"
  }
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowIndicatorDetailSolution {

    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);
```



```
        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowIndicatorDetailRequest request = new ShowIndicatorDetailRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withIndicatorId("{indicator_id}");
        try {
            ShowIndicatorDetailResponse response = client.showIndicatorDetail(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowIndicatorDetailRequest()
        request.workspace_id = "{workspace_id}"
        request.indicator_id = "{indicator_id}"
        response = client.show_indicator_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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowIndicatorDetailRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.IndicatorId = "{indicator_id}"
    response, err := client.ShowIndicatorDetail(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.3.5 Updating a Threat Indicator

Function

This API is used to update a threat indicator.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/{indicator_id}

Table 4-308 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
indicator_id	Yes	String	Threat indicator ID.

Request Parameters

Table 4-309 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-310 Request body parameters

Parameter	Mandatory	Type	Description
data_object	No	**IndicatorDataObjectDetail** object	Indicator details.

Table 4-311 IndicatorDataObjectDetail

Parameter	Mandatory	Type	Description
indicator_type	No	**indicator_type** object	Indicator type object.
value	No	String	Value, for example, **ip**, **url**, and **domain**.
update_time	No	String	Update time.
create_time	No	String	Creation time.
environment	No	**environment** object	Environment information.
data_source	No	**data_source** object	Data source information.
first_report_time	No	String	First occurrence time.
is_deleted	No	Boolean	Whether to delete.
last_report_time	No	String	Last occurrence time.
granular_marking	No	Integer	Granularity (confidentiality level). **1**: First discovery; **2**: Self-produced data; **3**: Purchase required; and **4**: Direct query from the external network.
name	No	String	Name.
id	No	String	Threat indicator ID.
project_id	No	String	Project ID.
revoked	No	Boolean	Whether to discard.
status	No	String	Status. The options are **Open**, **Closed**, and **Revoked**.
verdict	No	String	Threat degree. The options are **Black**, **White**, and **Gray**.
workspace_id	No	String	Workspace ID.
confidence	No	Integer	Confidence. Value range: 80 to 100.

Table 4-312 indicator_type

Parameter	Mandatory	Type	Description
indicator_type	No	String	Indicator type.
id	No	String	Indicator type ID.

Table 4-313 environment

Parameter	Mandatory	Type	Description
vendor_type	No	String	Environment provider.
domain_id	No	String	Account ID.
region_id	No	String	Region ID.
project_id	No	String	Project ID.

Table 4-314 data_source

Parameter	Mandatory	Type	Description
source_type	No	Integer	Data source type. The value can be **1**, **2**, or **3**. **1**: Huawei Cloud product; **2**: Third-party products, and **3**: Your in-house products.
domain_id	No	String	Account ID.
project_id	No	String	Project ID.
region_id	No	String	Region ID.

Response Parameters

Status code: 200

Table 4-315 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-316 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**IndicatorDetail** object	Indicator details.

Table 4-317 IndicatorDetail

Parameter	Type	Description
id	String	Threat indicator ID.
name	String	Threat indicator name.
data_object	**IndicatorDataObjectDetail** object	Indicator details.
workspace_id	String	Workspace ID.
project_id	String	Project ID.
dataclass_ref	**DataClassRefPojo** object	Data class object information.
create_time	String	Creation time.
update_time	String	Update time.

Table 4-318 IndicatorDataObjectDetail

Parameter	Type	Description
indicator_type	**indicator_type** object	Indicator type object.
value	String	Value, for example, **ip**, **url**, and **domain**.
update_time	String	Update time.
create_time	String	Creation time.
environment	**environment** object	Environment information.
data_source	**data_source** object	Data source information.
first_report_time	String	First occurrence time.

Parameter	Type	Description
is_deleted	Boolean	Whether to delete.
last_report_time	String	Last occurrence time.
granular_marking	Integer	Granularity (confidentiality level). **1**: First discovery; **2**: Self-produced data; **3**: Purchase required; and **4**: Direct query from the external network.
name	String	Name.
id	String	Threat indicator ID.
project_id	String	Project ID.
revoked	Boolean	Whether to discard.
status	String	Status. The options are **Open**, **Closed**, and **Revoked**.
verdict	String	Threat degree. The options are **Black**, **White**, and **Gray**.
workspace_id	String	Workspace ID.
confidence	Integer	Confidence. Value range: 80 to 100.

Table 4-319 indicator_type

Parameter	Type	Description
indicator_type	String	Indicator type.
id	String	Indicator type ID.

Table 4-320 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Account ID.
region_id	String	Region ID.
project_id	String	Project ID.

Table 4-321 data_source

Parameter	Type	Description
source_type	Integer	Data source type. The value can be **1**, **2**, or **3**. **1**: Huawei Cloud product; **2**: Third-party products, and **3**: Your in-house products.
domain_id	String	Account ID.
project_id	String	Project ID.
region_id	String	Region ID.

Table 4-322 DataClassRefPojo

Parameter	Type	Description
id	String	Data class ID.
name	String	Data class name.

Status code: 400

Table 4-323 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-324 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Update a threat indicator. The threat indicator trigger flag is no, and the value is ip.

```
{
  "data_object" : {
    "indicator_type" : {
      "indicator_type" : "ipv6",
      "id" : "ac794b2dfab9fe8c0676587301a636d3"
```



```
  },
  "value" : "ip",
  "data_source" : {
    "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
    "project_id" : "5b8bb3c888db498f9eeaf1023f7ba597",
    "region_id" : "xxx",
    "source_type" : 1
  },
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "granular_marking" : 1,
  "first_report_time" : "2023-07-04T16:47:01Z+0800",
  "status" : "Open"
 }
}
```

Example Responses

Status code: 200

Response to a successful request.

```
{
 "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
 "message" : "Error message",
 "data" : {
  "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
  "name" : "Threat indicator name.",
  "data_object" : {
   "indicator_type" : {
    "indicator_type" : "ipv6",
    "id" : "ac794b2dfab9fe8c0676587301a636d3"
   },
   "value" : "ip",
   "data_source" : {
    "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
    "project_id" : "5b8bb3c888db498f9eeaf1023f7ba597",
    "region_id" : "xxx",
    "source_type" : 1
   },
   "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620",
   "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
   "granular_marking" : 1,
   "first_report_time" : "2023-07-04T16:47:01Z+0800",
   "status" : "Open"
  },
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "dataclass_ref" : {
   "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
   "name" : "Name."
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800"
 }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Update a threat indicator. The threat indicator trigger flag is no, and the value is ip.


```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class UpdateIndicatorSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateIndicatorRequest request = new UpdateIndicatorRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withIndicatorId("{indicator_id}");
        UpdateIndicatorRequestBody body = new UpdateIndicatorRequestBody();
        IndicatorDataObjectDetailDataSource dataSourceDataObject = new IndicatorDataObjectDetailDataSource();
        dataSourceDataObject.withSourceType(1)
            .withDomainId("ac7438b990ef4a37b741004eb45e8bf4")
            .withProjectId("5b8bb3c888db498f9eeaf1023f7ba597")
            .withRegionId("xxx");
        IndicatorDataObjectDetailIndicatorType indicatorTypeDataObject = new IndicatorDataObjectDetailIndicatorType();
        indicatorTypeDataObject.withIndicatorType("ipv6")
            .withId("ac794b2dfab9fe8c0676587301a636d3");
        IndicatorDataObjectDetail dataObjectbody = new IndicatorDataObjectDetail();
        dataObjectbody.withIndicatorType(indicatorTypeDataObject)
            .withValue("ip")
            .withDataSource(dataSourceDataObject)
            .withFirstReportTime("2023-07-04T16:47:01Z+0800")
            .withGranularMarking(1)
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withStatus("Open")
            .withWorkspaceId("909494e3-558e-46b6-a9eb-07a8e18ca620");
        body.withDataObject(dataObjectbody);
        request.withBody(body);
        try {
            UpdateIndicatorResponse response = client.updateIndicator(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 threat indicator. The threat indicator trigger flag is no, and the value is ip.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateIndicatorRequest()
        request.workspace_id = "{workspace_id}"
        request.indicator_id = "{indicator_id}"
        dataSourceDataObject = IndicatorDataObjectDetailDataSource(
            source_type=1,
            domain_id="ac7438b990ef4a37b741004eb45e8bf4",
            project_id="5b8bb3c888db498f9eeaf1023f7ba597",
            region_id="xxx"
        )
        indicatorTypeDataObject = IndicatorDataObjectDetailIndicatorType(
            indicator_type="ipv6",
            id="ac794b2dfab9fe8c0676587301a636d3"
        )
        dataObjectbody = IndicatorDataObjectDetail(
            indicator_type=indicatorTypeDataObject,
            value="ip",
            data_source=dataSourceDataObject,
            first_report_time="2023-07-04T16:47:01Z+0800",
            granular_marking=1,
            project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            status="Open",
            workspace_id="909494e3-558e-46b6-a9eb-07a8e18ca620"
        )
        request.body = UpdateIndicatorRequestBody(
            data_object=dataObjectbody
        )
        response = client.update_indicator(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 threat indicator. The threat indicator trigger flag is no, and the value is ip.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateIndicatorRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.IndicatorId = "{indicator_id}"
    sourceTypeDataSource:= int32(1)
    domainIdDataSource:= "ac7438b990ef4a37b741004eb45e8bf4"
    projectIdDataSource:= "5b8bb3c888db498f9eeaf1023f7ba597"
    regionIdDataSource:= "xxx"
    dataSourceDataObject := &model.IndicatorDataObjectDetailDataSource{
        SourceType: &sourceTypeDataSource,
        DomainId: &domainIdDataSource,
        ProjectId: &projectIdDataSource,
        RegionId: &regionIdDataSource,
    }
    indicatorTypeIndicatorType:= "ipv6"
    idIndicatorType:= "ac794b2dfab9fe8c0676587301a636d3"
    indicatorTypeDataObject := &model.IndicatorDataObjectDetailIndicatorType{
        IndicatorType: &indicatorTypeIndicatorType,
        Id: &idIndicatorType,
    }
    valueDataObject:= "ip"
    firstReportTimeDataObject:= "2023-07-04T16:47:01Z+0800"
    granularMarkingDataObject:= int32(1)
    projectIdDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    statusDataObject:= "Open"
    workspaceIdDataObject:= "909494e3-558e-46b6-a9eb-07a8e18ca620"
    dataObjectbody := &model.IndicatorDataObjectDetail{
        IndicatorType: indicatorTypeDataObject,
        Value: &valueDataObject,
        DataSource: dataSourceDataObject,
```



```
        FirstReportTime: &firstReportTimeDataObject,
        GranularMarking: &granularMarkingDataObject,
        ProjectId: &projectIdDataObject,
        Status: &statusDataObject,
        WorkspaceId: &workspaceIdDataObject,
    }
    request.Body = &model.UpdateIndicatorRequestBody{
        DataObject: dataObjectbody,
    }
    response, err := client.UpdateIndicator(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	Response to a successful request.
400	Response to a failed request.

Error Codes

See **Error Codes**.

4.4 Playbook Management

4.4.1 Monitoring Playbook Running

Function

This API is used to monitor the running status of a playbook.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}/monitor

Table 4-325 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
playbook_id	Yes	String	Playbook ID.

Table 4-326 Query Parameters

Parameter	Mandatory	Type	Description
start_time	Yes	String	Start time. ISO 8601 format: YYYY-MM-DDTHH:mm:ss.ms +timezone. Example: 2021-01-30T23:00:00Z+0800. The time zone is the one where the playbook instance was generated. If this parameter cannot be parsed, the default time zone GMT+8 is used.
version_query_type	Yes	String	Playbook version type. The options are: **ALL**: All versions; **VALID**: Valid versions; **DELETED**: Deleted versions.
end_time	Yes	String	End time. ISO 8601 format: YYYY-MM-DDTHH:mm:ss.ms +timezone. Example: 2021-01-30T23:00:00Z+0800. The time zone is the one where the playbook instance was generated. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Request Parameters

Table 4-327 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-328 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-329 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**PlaybookInstanceMonitorDetail** object	Playbook monitoring details.

Table 4-330 PlaybookInstanceMonitorDetail

Parameter	Type	Description
total_instance_run_num	Integer	Total execution times.
schedule_instance_run_num	Integer	Number of scheduled executions.

Parameter	Type	Description
event_instance_run_num	Integer	Number of time-triggered executions.
average_run_time	Number	Average running duration.
min_run_time_instance	PlaybookInstanceRunStatistics object	Workflow with the shortest running duration.
max_run_time_instance	PlaybookInstanceRunStatistics object	Workflow with the longest running duration.
total_instance_num	Integer	Total number of playbook instances.
success_instance_num	Integer	Number of instances that have been executed successfully.
fail_instance_num	Integer	Number of instances that failed to be executed.
terminate_instance_num	Integer	Number of terminated instances.
running_instance_num	Integer	Number of running instances.

Table 4-331 PlaybookInstanceRunStatistics

Parameter	Type	Description
playbook_instance_id	String	Playbook instance ID.
playbook_instance_name	String	Playbook instance name.
playbook_instance_run_time	Number	Playbook instance running time.

Status code: 400

Table 4-332 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-333 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : "00000000",
  "message" : "",
  "data" : {
    "total_instance_run_num" : "Unknown Type: in",
    "schedule_instance_run_num" : 99999999,
    "event_instance_run_num" : 99999999,
    "average_run_time" : 9999999999,
    "min_run_time_instance" : {
      "playbook_instance_id" : "string",
      "playbook_instance_name" : "string",
      "playbook_instance_run_time" : 9999999999
    },
    "max_run_time_instance" : {
      "playbook_instance_id" : "string",
      "playbook_instance_name" : "string",
      "playbook_instance_run_time" : 9999999999
    },
    "total_instance_num" : 99999999,
    "success_instance_num" : 99999999,
    "fail_instance_num" : 99999999,
    "terminate_instance_num" : 99999999,
    "running_instance_num" : 99999999
  }
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;
```



```
public class ShowPlaybookMonitorsSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookMonitorsRequest request = new ShowPlaybookMonitorsRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withPlaybookId("{playbook_id}");
        try {
            ShowPlaybookMonitorsResponse response = client.showPlaybookMonitors(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
```



```
        request = ShowPlaybookMonitorsRequest()
        request.workspace_id = "{workspace_id}"
        request.playbook_id = "{playbook_id}"
        response = client.show_playbook_monitors(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowPlaybookMonitorsRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.PlaybookId = "{playbook_id}"
    response, err := client.ShowPlaybookMonitors(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.4.2 Querying Playbook Statistics Data

Function

This API is used to obtain playbook statistics.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/statistics

Table 4-334 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-335 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.

Parameter	Mandatory	Type	Description
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-336 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-337 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**PlaybookStatisticDetail** object	Playbook status statistics.

Table 4-338 PlaybookStatisticDetail

Parameter	Type	Description
unapproved_num	Integer	Number of unapproved playbooks.
disabled_num	Integer	Number of playbooks that are not enabled.
enabled_num	Integer	Number of enabled playbooks.

Status code: 400

Table 4-339 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-340 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "unapproved_num" : 99999999,
    "disabled_num" : 99999999,
    "enabled_num" : 99999999
  }
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowPlaybookStatisticsSolution {

    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);
```



```
        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookStatisticsRequest request = new ShowPlaybookStatisticsRequest();
        request.withWorkspaceId("{workspace_id}");
        try {
            ShowPlaybookStatisticsResponse response = client.showPlaybookStatistics(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowPlaybookStatisticsRequest()
        request.workspace_id = "{workspace_id}"
        response = client.show_playbook_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"
```

```
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowPlaybookStatisticsRequest{}
    request.WorkspaceId = "{workspace_id}"
    response, err := client.ShowPlaybookStatistics(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.4.3 Querying the Playbook List

Function

This API is used to query the playbook list.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks

Table 4-341 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Table 4-342 Query Parameters

Parameter	Mandatory	Type	Description
search_txt	No	String	Search keyword.
enabled	No	Boolean	Whether to enable this feature.
offset	Yes	Integer	Pagination query parameter. This parameter specifies the start position of the query result. The value starts from **0**.
limit	Yes	Integer	The maximum number of records can be returned on each page for a pagination query. The value starts from 1.
description	No	String	Playbook description.
dataclass_name	No	String	Data class name.
name	No	String	Playbook name.

Request Parameters

Table 4-343 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 the user token.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-344 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-345 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Response message information.
total	Integer	Total records.
size	Integer	Records on each page.
page	Integer	Current page number.
data	Array of **PlaybookInfo** objects	Playbook list information.

Table 4-346 PlaybookInfo

Parameter	Type	Description
id	String	Playbook ID.
name	String	Playbook name.
description	String	Description.
create_time	String	Time the playbook was created.
update_time	String	Time the playbook was updated.
project_id	String	Project ID.
version_id	String	Playbook version ID.
enabled	Boolean	Whether to enable this feature.
workspace_id	String	Workspace ID.
approve_role	String	Reviewer role.
user_role	String	User role.
edit_role	String	Role of the editor.
owner_id	String	Owner ID.
version	String	Version No.
dataclass_name	String	Data class name.
dataclass_id	String	Data class ID.
unaudited_version_id	String	ID of the playbook version to be reviewed.
reject_version_id	String	ID of the rejected playbook version.

Status code: 400

Table 4-347 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-348 Response body parameters

Parameter	Type	Description
code	String	Error code.

Parameter	Type	Description
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response parameters for a successful playbook list query.


```
{
  "code" : 0,
  "message" : null,
  "total" : 41,
  "page" : 10,
  "data" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "enabled" : true,
    "workspace_id" : "string",
    "approve_role" : "approve",
    "user_role" : "string",
    "edit_role" : "editor",
    "owner_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "dataclass_name" : "string",
    "dataclass_id" : "string",
    "unaudited_version_id" : "string",
    "reject_version_id" : "string"
  } ]
}
```


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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListPlaybooksSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybooksRequest request = new ListPlaybooksRequest();
        request.withWorkspaceId("{workspace_id}");
        try {
            ListPlaybooksResponse response = client.listPlaybooks(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListPlaybooksRequest()
        request.workspace_id = "{workspace_id}"
        response = client.list_playbooks(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPlaybooksRequest{}
    request.WorkspaceId = "{workspace_id}"
    response, err := client.ListPlaybooks(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	Response parameters for a successful playbook list query.
400	Response parameters for failed requests.

Error Codes

See **Error Codes**.

4.4.4 Creating a Playbook

Function

This API is used to create a playbook.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks

Table 4-349 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-350 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of **X-Subject-Token** in the response header is the user token.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-351 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Playbook name.
description	No	String	Description.

Parameter	Mandatory	Type	Description
workspace_id	Yes	String	Workspace ID.

Response Parameters

Status code: 200

Table 4-352 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-353 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	PlaybookInfo object	Playbook details.

Table 4-354 PlaybookInfo

Parameter	Type	Description
id	String	Playbook ID.
name	String	Playbook name.
description	String	Description.
create_time	String	Time the playbook was created.
update_time	String	Time the playbook was updated.
project_id	String	Project ID.
version_id	String	Playbook version ID.
enabled	Boolean	Whether to enable this feature.
workspace_id	String	Workspace ID.
approve_role	String	Reviewer role.
user_role	String	User role.

Parameter	Type	Description
edit_role	String	Role of the editor.
owner_id	String	Owner ID.
version	String	Version No.
dataclass_name	String	Data class name.
dataclass_id	String	Data class ID.
unaudited_version_id	String	ID of the playbook version to be reviewed.
reject_version_id	String	ID of the rejected playbook version.

Status code: 400

Table 4-355 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-356 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Create a playbook. Name: MyXXX; workspace ID: string; approver: approve; and status: enabled.

```
{
  "name" : "MyXXX",
  "description" : "This my XXXX",
  "workspace_id" : "string"
}
```

Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : 0,
```



```
 "message" : "Error message",
 "data" : {
  "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "name" : "MyXXX",
  "description" : "This my XXXX",
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "enabled" : true,
  "workspace_id" : "string",
  "approve_role" : "approve",
  "user_role" : "string",
  "edit_role" : "editor",
  "owner_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "version" : "v1.1.1",
  "dataclass_name" : "string",
  "dataclass_id" : "string",
  "unaudited_version_id" : "string",
  "reject_version_id" : "string"
 }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Create a playbook. Name: MyXXX; workspace ID: string; approver: approve; and status: 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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class CreatePlaybookSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePlaybookRequest request = new CreatePlaybookRequest();
        request.withWorkspaceId("{workspace_id}");
```



```
        CreatePlaybookInfo body = new CreatePlaybookInfo();
        body.withWorkspaceId("string");
        body.withDescription("This my XXXX");
        body.withName("MyXXX");
        request.withBody(body);
        try {
            CreatePlaybookResponse response = client.createPlaybook(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 playbook. Name: MyXXX; workspace ID: string; approver: approve; and status: enabled.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreatePlaybookRequest()
        request.workspace_id = "{workspace_id}"
        request.body = CreatePlaybookInfo(
            workspace_id="string",
            description="This my XXXX",
            name="MyXXX"
        )
        response = client.create_playbook(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 playbook. Name: MyXXX; workspace ID: string; approver: approve; and status: enabled.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePlaybookRequest{}
    request.WorkspaceId = "{workspace_id}"
    descriptionCreatePlaybookInfo:= "This my XXXX"
    request.Body = &model.CreatePlaybookInfo{
        WorkspaceId: "string",
        Description: &descriptionCreatePlaybookInfo,
        Name: "MyXXX",
    }
    response, err := client.CreatePlaybook(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	Response to a successful request.

Status Code	Description
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.4.5 Querying Playbook Details

Function

This API is used to query details about a playbook.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}

Table 4-357 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
playbook_id	Yes	String	ID of playbook

Request Parameters

Table 4-358 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-359 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-360 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	PlaybookInfo object	Playbook details.

Table 4-361 PlaybookInfo

Parameter	Type	Description
id	String	Playbook ID.
name	String	Playbook name.
description	String	Description.
create_time	String	Time the playbook was created.
update_time	String	Time the playbook was updated.
project_id	String	Project ID.
version_id	String	Playbook version ID.
enabled	Boolean	Whether to enable this feature.
workspace_id	String	Workspace ID.
approve_role	String	Reviewer role.
user_role	String	User role.
edit_role	String	Role of the editor.
owner_id	String	Owner ID.
version	String	Version No.
dataclass_name	String	Data class name.

Parameter	Type	Description
dataclass_id	String	Data class ID.
unaudited_version_id	String	ID of the playbook version to be reviewed.
reject_version_id	String	ID of the rejected playbook version.

Status code: 400

Table 4-362 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-363 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "enabled" : true,
    "workspace_id" : "string",
    "approve_role" : "approve",
    "user_role" : "string",
    "edit_role" : "editor",
    "owner_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
```



```
    "dataclass_name" : "string",
    "dataclass_id" : "string",
    "unaudited_version_id" : "string",
    "reject_version_id" : "string"
  }
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowPlaybookSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookRequest request = new ShowPlaybookRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withPlaybookId("{playbook_id}");
        try {
            ShowPlaybookResponse response = client.showPlaybook(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowPlaybookRequest()
        request.workspace_id = "{workspace_id}"
        request.playbook_id = "{playbook_id}"
        response = client.show_playbook(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
```



```
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

    request := &model.ShowPlaybookRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.PlaybookId = "{playbook_id}"
    response, err := client.ShowPlaybook(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.4.6 Deleting a Playbook

Function

This API is used to delete a playbook.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}

Table 4-364 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Parameter	Mandatory	Type	Description
playbook_id	Yes	String	ID of playbook

Request Parameters

Table 4-365 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-366 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-367 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**PlaybookInfo** object	Playbook details.

Table 4-368 PlaybookInfo

Parameter	Type	Description
id	String	Playbook ID.
name	String	Playbook name.
description	String	Description.
create_time	String	Time the playbook was created.
update_time	String	Time the playbook was updated.
project_id	String	Project ID.
version_id	String	Playbook version ID.
enabled	Boolean	Whether to enable this feature.
workspace_id	String	Workspace ID.
approve_role	String	Reviewer role.
user_role	String	User role.
edit_role	String	Role of the editor.
owner_id	String	Owner ID.
version	String	Version No.
dataclass_name	String	Data class name.
dataclass_id	String	Data class ID.
unaudited_version_id	String	ID of the playbook version to be reviewed.
reject_version_id	String	ID of the rejected playbook version.

Status code: 400

Table 4-369 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-370 Response body parameters

Parameter	Type	Description
code	String	Error code.

Parameter	Type	Description
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "enabled" : true,
    "workspace_id" : "string",
    "approve_role" : "approve",
    "user_role" : "string",
    "edit_role" : "editor",
    "owner_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "dataclass_name" : "string",
    "dataclass_id" : "string",
    "unaudited_version_id" : "string",
    "reject_version_id" : "string"
  }
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class DeletePlaybookSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeletePlaybookRequest request = new DeletePlaybookRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withPlaybookId("{playbook_id}");
        try {
            DeletePlaybookResponse response = client.deletePlaybook(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeletePlaybookRequest()
        request.workspace_id = "{workspace_id}"
        request.playbook_id = "{playbook_id}"
        response = client.delete_playbook(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeletePlaybookRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.PlaybookId = "{playbook_id}"
    response, err := client.DeletePlaybook(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.4.7 Modifying a Playbook

Function

This API is used to modify a playbook.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}

Table 4-371 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
playbook_id	Yes	String	Playbook ID.

Request Parameters

Table 4-372 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-373 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Playbook name.

Parameter	Mandatory	Type	Description
description	No	String	Description.
enabled	No	Boolean	Whether to enable this feature.
active_version_id	No	String	ID of the enabled playbook version.

Response Parameters

Status code: 200

Table 4-374 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-375 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	PlaybookInfo object	Playbook details.

Table 4-376 PlaybookInfo

Parameter	Type	Description
id	String	Playbook ID.
name	String	Playbook name.
description	String	Description.
create_time	String	Time the playbook was created.
update_time	String	Time the playbook was updated.
project_id	String	Project ID.
version_id	String	Playbook version ID.
enabled	Boolean	Whether to enable this feature.

Parameter	Type	Description
workspace_id	String	Workspace ID.
approve_role	String	Reviewer role.
user_role	String	User role.
edit_role	String	Role of the editor.
owner_id	String	Owner ID.
version	String	Version No.
dataclass_name	String	Data class name.
dataclass_id	String	Data class ID.
unaudited_version_id	String	ID of the playbook version to be reviewed.
reject_version_id	String	ID of the rejected playbook version.

Status code: 400

Table 4-377 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-378 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Modify a playbook. Name: MyXXX; Description: This my XXXX; Status: Enabled, and playbook ID: active_version_id.

```
{
  "name" : "MyXXX",
  "description" : "This my XXXX",
  "enabled" : true,
  "active_version_id" : "active_version_id"
}
```


Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "enabled" : true,
    "workspace_id" : "string",
    "approve_role" : "approve",
    "user_role" : "string",
    "edit_role" : "editor",
    "owner_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "dataclass_name" : "string",
    "dataclass_id" : "string",
    "unaudited_version_id" : "string",
    "reject_version_id" : "string"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Modify a playbook. Name: MyXXX; Description: This my XXXX; Status: Enabled, and playbook ID: active_version_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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class UpdatePlaybookSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
            .withCredential(auth)
            .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
            .build();
        UpdatePlaybookRequest request = new UpdatePlaybookRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withPlaybookId("{playbook_id}");
        ModifyPlaybookInfo body = new ModifyPlaybookInfo();
        body.withActiveVersionId("active_version_id");
        body.withEnabled(true);
        body.withDescription("This my XXXX");
        body.withName("MyXXX");
        request.withBody(body);
        try {
            UpdatePlaybookResponse response = client.updatePlaybook(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 a playbook. Name: MyXXX; Description: This my XXXX; Status: Enabled, and playbook ID: active_version_id.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdatePlaybookRequest()
        request.workspace_id = "{workspace_id}"
        request.playbook_id = "{playbook_id}"
        request.body = ModifyPlaybookInfo(
            active_version_id="active_version_id",
```



```
            enabled=True,
            description="This my XXXX",
            name="MyXXX"
        )
        response = client.update_playbook(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 playbook. Name: MyXXX; Description: This my XXXX; Status: Enabled, and playbook ID: active_version_id.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdatePlaybookRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.PlaybookId = "{playbook_id}"
    activeVersionIdModifyPlaybookInfo:= "active_version_id"
    enabledModifyPlaybookInfo:= true
    descriptionModifyPlaybookInfo:= "This my XXXX"
    nameModifyPlaybookInfo:= "MyXXX"
    request.Body = &model.ModifyPlaybookInfo{
        ActiveVersionId: &activeVersionIdModifyPlaybookInfo,
        Enabled: &enabledModifyPlaybookInfo,
        Description: &descriptionModifyPlaybookInfo,
        Name: &nameModifyPlaybookInfo,
    }
    response, err := client.UpdatePlaybook(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.5 Alert Rule Management

4.5.1 Listing Alert Rules

Function

List alert rules

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules

Table 4-379 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Table 4-380 Query Parameters

Parameter	Mandatory	Type	Description
offset	Yes	Long	Offset.

Parameter	Mandatory	Type	Description
limit	Yes	Long	Number of items.
sort_key	No	String	Sorting field.
sort_dir	No	String	Sorting order. You can sort fields in ascending or descending order.
pipe_id	No	String	Data pipeline ID.
rule_name	No	String	Alert rule name.
rule_id	No	String	Alert rule ID.
status	No	Array of strings	Status. **enabled**: The rule is enabled. **disabled**: The rule is disabled.
severity	No	Array of strings	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)

Request Parameters

Table 4-381 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. You can obtain the token by calling the IAM API used to obtain a user token.

Response Parameters

Status code: 200

Table 4-382 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 4-383 Response body parameters

Parameter	Type	Description
count	Long	Total number.
records	Array of **AlertRule** objects	Alert model.

Table 4-384 AlertRule

Parameter	Type	Description
rule_id	String	Alert rule ID.
pipe_id	String	Data pipeline ID.
pipe_name	String	Data pipeline name.
create_by	String	Creator.
create_time	Long	Creation time.
update_by	String	Updater.
update_time	Long	Update time.
delete_time	Long	Deletion time.
rule_name	String	Alert rule name.
query	String	Query statement.
query_type	String	Query syntax: SQL.
status	String	Status. **enabled**: The rule is enabled. **disabled**: The rule is disabled.
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
custom_properties	Map<String,String>	Custom extension information.
event_grouping	Boolean	Alert group.
schedule	**Schedule** object	Schedule rule.
triggers	Array of **AlertRuleTrigger** objects	Alert triggering rules.

Table 4-385 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval.
frequency_unit	String	Scheduling interval unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY)
period_interval	Integer	Time window interval.
period_unit	String	Time window unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY.)
delay_interval	Integer	Delay interval.
overtime_interval	Integer	Timeout interval.

Table 4-386 AlertRuleTrigger

Parameter	Type	Description
mode	String	Mode and quantity. **COUNT**.
operator	String	Operator. The value can be: **EQ**: Equal to **NE**: Not equal to **GT**: Greater than **LT**: Less than
expression	String	expression
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
accumulated_times	Integer	accumulated_times

Status code: 400

Table 4-387 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.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.


```
{
  "count" : 9223372036854776000,
  "records" : [ {
    "rule_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
    "pipe_id" : "772fb35b-83bc-46c9-a0b1-ebe31070a889",
    "create_by" : "582dd19dd99d4505a1d7929dc943b169",
    "create_time" : 1665221214,
    "update_by" : "582dd19dd99d4505a1d7929dc943b169",
    "update_time" : 1665221214,
    "delete_time" : 0,
    "rule_name" : "Alert rule",
    "query" : "* | select status, count(*) as count group by status",
    "query_type" : "SQL",
    "status" : "ENABLED",
    "severity" : "TIPS",
    "custom_properties" : {
      "references" : "https://localhost/references",
      "maintainer" : "isap"
    },
    "event_grouping" : true,
    "schedule" : {
      "frequency_interval" : 5,
      "frequency_unit" : "MINUTE",
      "period_interval" : 5,
      "period_unit" : "MINUTE",
      "delay_interval" : 2,
      "overtime_interval" : 10
    },
    "triggers" : [ {
      "mode" : "COUNT",
      "operator" : "GT",
      "expression" : 10,
      "severity" : "TIPS"
    } ]
  } ]
}
```


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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListAlertRulesSolution {
```

```
    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListAlertRulesRequest request = new ListAlertRulesRequest();
        request.withWorkspaceId("{workspace_id}");
        try {
            ListAlertRulesResponse response = client.listAlertRules(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAlertRulesRequest()
        request.workspace_id = "{workspace_id}"
```



```
        response = client.list_alert_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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAlertRulesRequest{}
    request.WorkspaceId = "{workspace_id}"
    response, err := client.ListAlertRules(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	Request failed.

Error Codes

See **Error Codes**.

4.5.2 Creating an Alert Rule

Function

Create alert rule

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules

Table 4-388 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-389 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. You can obtain the token by calling the IAM API used to obtain a user token.

Table 4-390 Request body parameters

Parameter	Mandatory	Type	Description
pipe_id	Yes	String	Data pipeline ID.
rule_name	Yes	String	Alert rule name.
description	No	String	Description.
query	Yes	String	Query statement.

Parameter	Mandatory	Type	Description
query_type	No	String	Query syntax: SQL.
status	No	String	Status. **enabled**: The rule is enabled. **disabled**: The rule is disabled.
severity	No	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
custom_properties	No	Map<String,String>	Custom extension information.
alert_type	No	Map<String,String>	Alert type.
event_grouping	No	Boolean	Alert group.
suspression	No	Boolean	Alert suppression.
simulation	No	Boolean	Simulated alerts.
schedule	Yes	**Schedule** object	Schedule of an alarm rule.
triggers	Yes	Array of **AlertRuleTrigger** objects	Alert triggering rules.
pipe_name	Yes	String	Pipeline name.
alert_name	Yes	String	Alert name.
alert_description	No	String	Alert description.
alert_remediation	No	String	Handling suggestions.
accumulated_times	No	Integer	Executions.

Table 4-391 Schedule

Parameter	Mandatory	Type	Description
frequency_interval	Yes	Integer	Scheduling interval.

Parameter	Mandatory	Type	Description
frequency_unit	Yes	String	Scheduling interval unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY)
period_interval	Yes	Integer	Time window interval.
period_unit	Yes	String	Time window unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY.)
delay_interval	No	Integer	Delay interval.
overtime_interval	No	Integer	Timeout interval.

Table 4-392 AlertRuleTrigger

Parameter	Mandatory	Type	Description
mode	No	String	Mode and quantity. **COUNT**.
operator	No	String	Operator. The value can be: **EQ**: Equal to **NE**: Not equal to **GT**: Greater than **LT**: Less than
expression	Yes	String	expression
severity	No	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
accumulated_times	No	Integer	accumulated_times

Response Parameters

Status code: 200

Table 4-393 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 4-394 Response body parameters

Parameter	Type	Description
rule_id	String	Alert rule ID.
pipe_id	String	Data pipeline ID.
pipe_name	String	Data pipeline name.
create_by	String	Creator.
create_time	Long	Creation time.
update_by	String	Updater.
update_time	Long	Update time.
delete_time	Long	Deletion time.
rule_name	String	Alert rule name.
query	String	Query statement.
query_type	String	Query syntax: SQL.
status	String	Status. **enabled**: The rule is enabled. **disabled**: The rule is disabled.
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
custom_properties	Map<String,String>	Custom extension information.
event_grouping	Boolean	Alert group.
schedule	**Schedule** object	Schedule rule.
triggers	Array of **AlertRuleTrigger** objects	Alert triggering rules.

Table 4-395 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval.
frequency_unit	String	Scheduling interval unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY)
period_interval	Integer	Time window interval.
period_unit	String	Time window unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY.)
delay_interval	Integer	Delay interval.
overtime_interval	Integer	Timeout interval.

Table 4-396 AlertRuleTrigger

Parameter	Type	Description
mode	String	Mode and quantity. **COUNT**.
operator	String	Operator. The value can be: **EQ**: Equal to **NE**: Not equal to **GT**: Greater than **LT**: Less than
expression	String	expression
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
accumulated_times	Integer	accumulated_times

Status code: 400

Table 4-397 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.

Example Requests

Create an alert rule whose ID is 772fb35b-83bc-46c9-a0b1-ebe31070a889, Name is Alert rule, Query type is SQL, and Status is Enabled.

```
{
  "pipe_id" : "772fb35b-83bc-46c9-a0b1-ebe31070a889",
  "pipe_name" : "sec-hss-alarm",
  "rule_name" : "Alert rule",
  "description" : "An alert rule",
  "query" : "* | select status, count(*) as count group by status",
  "query_type" : "SQL",
  "status" : "ENABLED",
  "severity" : "TIPS",
  "alert_name" : "test",
  "custom_properties" : {
    "references" : "https://localhost/references",
    "maintainer" : "isap"
  },
  "event_grouping" : false,
  "suspression" : false,
  "simulation" : false,
  "accumulated_times" : 1,
  "schedule" : {
    "frequency_interval" : 5,
    "frequency_unit" : "MINUTE",
    "period_interval" : 5,
    "period_unit" : "MINUTE",
    "delay_interval" : 2,
    "overtime_interval" : 10
  },
  "triggers" : [ {
    "mode" : "COUNT",
    "operator" : "GT",
    "expression" : 10,
    "severity" : "TIPS",
    "accumulated_times" : 1
  } ]
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "rule_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
  "pipe_id" : "772fb35b-83bc-46c9-a0b1-ebe31070a889",
  "create_by" : "582dd19dd99d4505a1d7929dc943b169",
  "create_time" : 1665221214,
  "update_by" : "582dd19dd99d4505a1d7929dc943b169",
  "update_time" : 1665221214,
  "delete_time" : 0,
  "rule_name" : "Alert rule",
  "query" : "* | select status, count(*) as count group by status",
  "query_type" : "SQL",
  "status" : "ENABLED",
  "severity" : "TIPS",
  "custom_properties" : {
    "references" : "https://localhost/references",
    "maintainer" : "isap"
  },
  "event_grouping" : true,
  "schedule" : {
    "frequency_interval" : 5,
    "frequency_unit" : "MINUTE",
    "period_interval" : 5,
```



```
    "period_unit" : "MINUTE",
    "delay_interval" : 2,
    "overtime_interval" : 10
  },
  "triggers" : [ {
    "mode" : "COUNT",
    "operator" : "GT",
    "expression" : 10,
    "severity" : "TIPS"
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Create an alert rule whose ID is 772fb35b-83bc-46c9-a0b1-ebe31070a889, Name is Alert rule, Query type is SQL, and 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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;
import java.util.Map;
import java.util.HashMap;

public class CreateAlertRuleSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateAlertRuleRequest request = new CreateAlertRuleRequest();
        request.withWorkspaceId("{workspace_id}");
        CreateAlertRuleRequestBody body = new CreateAlertRuleRequestBody();
        List<AlertRuleTrigger> listbodyTriggers = new ArrayList<>();
        listbodyTriggers.add(
            new AlertRuleTrigger()
                .withMode(AlertRuleTrigger.ModeEnum.fromValue("COUNT"))
                .withOperator(AlertRuleTrigger.OperatorEnum.fromValue("GT"))
                .withExpression("10")
```



```
                .withSeverity(AlertRuleTrigger.SeverityEnum.fromValue("TIPS"))
                .withAccumulatedTimes(1)
        );
        Schedule schedulebody = new Schedule();
        schedulebody.withFrequencyInterval(5)
            .withFrequencyUnit(Schedule.FrequencyUnitEnum.fromValue("MINUTE"))
            .withPeriodInterval(5)
            .withPeriodUnit(Schedule.PeriodUnitEnum.fromValue("MINUTE"))
            .withDelayInterval(2)
            .withOvertimeInterval(10);
        Map<String, String> listbodyCustomProperties = new HashMap<>();
        listbodyCustomProperties.put("references", "https://localhost/references");
        listbodyCustomProperties.put("maintainer", "isap");
        body.withAccumulatedTimes(1);
        body.withAlertName("test");
        body.withPipeName("sec-hss-alarm");
        body.withTriggers(listbodyTriggers);
        body.withSchedule(schedulebody);
        body.withSimulation(false);
        body.withSuspression(false);
        body.withEventGrouping(false);
        body.withCustomProperties(listbodyCustomProperties);
        body.withSeverity(CreateAlertRuleRequestBody.SeverityEnum.fromValue("TIPS"));
        body.withStatus(CreateAlertRuleRequestBody.StatusEnum.fromValue("ENABLED"));
        body.withQueryType(CreateAlertRuleRequestBody.QueryTypeEnum.fromValue("SQL"));
        body.withQuery("* | select status, count(*) as count group by status");
        body.withDescription("An alert rule");
        body.withRuleName("Alert rule");
        body.withPipeId("772fb35b-83bc-46c9-a0b1-ebe31070a889");
        request.withBody(body);
        try {
            CreateAlertRuleResponse response = client.createAlertRule(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 an alert rule whose ID is 772fb35b-83bc-46c9-a0b1-ebe31070a889, Name is Alert rule, Query type is SQL, and Status is Enabled.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = CreateAlertRuleRequest()
    request.workspace_id = "{workspace_id}"
    listTriggersbody = [
        AlertRuleTrigger(
            mode="COUNT",
            operator="GT",
            expression="10",
            severity="TIPS",
            accumulated_times=1
        )
    ]
    schedulebody = Schedule(
        frequency_interval=5,
        frequency_unit="MINUTE",
        period_interval=5,
        period_unit="MINUTE",
        delay_interval=2,
        overtime_interval=10
    )
    listCustomPropertiesbody = {
        "references": "https://localhost/references",
        "maintainer": "isap"
    }
    request.body = CreateAlertRuleRequestBody(
        accumulated_times=1,
        alert_name="test",
        pipe_name="sec-hss-alarm",
        triggers=listTriggersbody,
        schedule=schedulebody,
        simulation=False,
        suspression=False,
        event_grouping=False,
        custom_properties=listCustomPropertiesbody,
        severity="TIPS",
        status="ENABLED",
        query_type="SQL",
        query="* | select status, count(*) as count group by status",
        description="An alert rule",
        rule_name="Alert rule",
        pipe_id="772fb35b-83bc-46c9-a0b1-ebe31070a889"
    )
    response = client.create_alert_rule(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 alert rule whose ID is 772fb35b-83bc-46c9-a0b1-ebe31070a889, Name is Alert rule, Query type is SQL, and Status is Enabled.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
```



```
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateAlertRuleRequest{}
    request.WorkspaceId = "{workspace_id}"
    modeTriggers:= model.GetAlertRuleTriggerModeEnum().COUNT
    operatorTriggers:= model.GetAlertRuleTriggerOperatorEnum().GT
    severityTriggers:= model.GetAlertRuleTriggerSeverityEnum().TIPS
    accumulatedTimesTriggers:= int32(1)
    var listTriggersbody = []model.AlertRuleTrigger{
        {
            Mode: &modeTriggers,
            Operator: &operatorTriggers,
            Expression: "10",
            Severity: &severityTriggers,
            AccumulatedTimes: &accumulatedTimesTriggers,
        },
    }
    delayIntervalSchedule:= int32(2)
    overtimeIntervalSchedule:= int32(10)
    schedulebody := &model.Schedule{
        FrequencyInterval: int32(5),
        FrequencyUnit: model.GetScheduleFrequencyUnitEnum().MINUTE,
        PeriodInterval: int32(5),
        PeriodUnit: model.GetSchedulePeriodUnitEnum().MINUTE,
        DelayInterval: &delayIntervalSchedule,
        OvertimeInterval: &overtimeIntervalSchedule,
    }
    var listCustomPropertiesbody = map[string]string{
        "references": "https://localhost/references",
        "maintainer": "isap",
    }
    accumulatedTimesCreateAlertRuleRequestBody:= int32(1)
    simulationCreateAlertRuleRequestBody:= false
    suspressionCreateAlertRuleRequestBody:= false
    eventGroupingCreateAlertRuleRequestBody:= false
    severityCreateAlertRuleRequestBody:= model.GetCreateAlertRuleRequestBodySeverityEnum().TIPS
    statusCreateAlertRuleRequestBody:= model.GetCreateAlertRuleRequestBodyStatusEnum().ENABLED
    queryTypeCreateAlertRuleRequestBody:= model.GetCreateAlertRuleRequestBodyQueryTypeEnum().SQL
    descriptionCreateAlertRuleRequestBody:= "An alert rule"
    request.Body = &model.CreateAlertRuleRequestBody{
        AccumulatedTimes: &accumulatedTimesCreateAlertRuleRequestBody,
        AlertName: "test",
        PipeName: "sec-hss-alarm",
        Triggers: listTriggersbody,
        Schedule: schedulebody,
```



```
        Simulation: &simulationCreateAlertRuleRequestBody,
        Suspression: &suspressionCreateAlertRuleRequestBody,
        EventGrouping: &eventGroupingCreateAlertRuleRequestBody,
        CustomProperties: listCustomPropertiesbody,
        Severity: &severityCreateAlertRuleRequestBody,
        Status: &statusCreateAlertRuleRequestBody,
        QueryType: &queryTypeCreateAlertRuleRequestBody,
        Query: "* | select status, count(*) as count group by status",
        Description: &descriptionCreateAlertRuleRequestBody,
        RuleName: "Alert rule",
        PipeId: "772fb35b-83bc-46c9-a0b1-ebe31070a889",
    }
    response, err := client.CreateAlertRule(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	Request failed.

Error Codes

See **Error Codes**.

4.5.3 Deleting an Alert Rule

Function

Delete alert rule

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules

Table 4-398 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-399 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. You can obtain the token by calling the IAM API used to obtain a user token.

Table 4-400 Request body parameters

Parameter	Mandatory	Type	Description
[items]	Yes	Array of strings	An array of alert rule IDs.

Response Parameters

Status code: 200

Table 4-401 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 4-402 Response body parameters

Parameter	Type	Description
deleted	Boolean	Whether to delete.
fail_list	Array of **AlertRule** objects	Alert rule ID.

Parameter	Type	Description
success_list	Array of **AlertRule** objects	Alert rule ID.

Table 4-403 AlertRule

Parameter	Type	Description
rule_id	String	Alert rule ID.
pipe_id	String	Data pipeline ID.
pipe_name	String	Data pipeline name.
create_by	String	Creator.
create_time	Long	Creation time.
update_by	String	Updater.
update_time	Long	Update time.
delete_time	Long	Deletion time.
rule_name	String	Alert rule name.
query	String	Query statement.
query_type	String	Query syntax: SQL.
status	String	Status. **enabled**: The rule is enabled. **disabled**: The rule is disabled.
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
custom_properties	Map<String,String>	Custom extension information.
event_grouping	Boolean	Alert group.
schedule	**Schedule** object	Schedule rule.
triggers	Array of **AlertRuleTrigger** objects	Alert triggering rules.

Table 4-404 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval.
frequency_unit	String	Scheduling interval unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY)
period_interval	Integer	Time window interval.
period_unit	String	Time window unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY.)
delay_interval	Integer	Delay interval.
overtime_interval	Integer	Timeout interval.

Table 4-405 AlertRuleTrigger

Parameter	Type	Description
mode	String	Mode and quantity. **COUNT**.
operator	String	Operator. The value can be: **EQ**: Equal to **NE**: Not equal to **GT**: Greater than **LT**: Less than
expression	String	expression
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
accumulated_times	Integer	accumulated_times

Status code: 400

Table 4-406 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.

Example Requests

This API is used to delete an alert rule. The request body is an array of alert rule IDs.

```
[ "612b7f41-da89-495b-a6a1-fdf14e4cc794" ]
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "deleted" : true,
  "fail_list" : [ ],
  "success_list" : [ ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

This API is used to delete an alert rule. The request body is an array of alert rule IDs.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class DeleteAlertRuleSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteAlertRuleRequest request = new DeleteAlertRuleRequest();
        request.withWorkspaceId("{workspace_id}");
```



```
        List<String> listbodyBody = new ArrayList<>();
        listbodyBody.add("612b7f41-da89-495b-a6a1-fdf14e4cc794");
        request.withBody(listbodyBody);
        try {
            DeleteAlertRuleResponse response = client.deleteAlertRule(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 delete an alert rule. The request body is an array of alert rule IDs.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteAlertRuleRequest()
        request.workspace_id = "{workspace_id}"
        listBodybody = [
            "612b7f41-da89-495b-a6a1-fdf14e4cc794"
        ]
        request.body = listBodybody
        response = client.delete_alert_rule(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 delete an alert rule. The request body is an array of alert rule IDs.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteAlertRuleRequest{}
    request.WorkspaceId = "{workspace_id}"
    var listBodybody = []string{
        "612b7f41-da89-495b-a6a1-fdf14e4cc794",
    }
    request.Body = &listBodybody
    response, err := client.DeleteAlertRule(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	Request failed.

Error Codes

See **Error Codes**.

4.5.4 Querying an Alert Rule

Function

This API is used to query an alert rule.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/{rule_id}

Table 4-407 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
rule_id	Yes	String	Alert rule ID.

Request Parameters

Table 4-408 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. You can obtain the token by calling the IAM API used to obtain a user token.

Response Parameters

Status code: 200

Table 4-409 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 4-410 Response body parameters

Parameter	Type	Description
rule_id	String	Alert rule ID.
pipe_id	String	Data pipeline ID.
pipe_name	String	Data pipeline name.
create_by	String	Creator.
create_time	Long	Creation time.
update_by	String	Updater.
update_time	Long	Update time.
delete_time	Long	Deletion time.
rule_name	String	Alert rule name.
query	String	Query statement.
query_type	String	Query syntax: SQL.
status	String	Status. **enabled**: The rule is enabled. **disabled**: The rule is disabled.
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
custom_properties	Map<String,String>	Custom extension information.
event_grouping	Boolean	Alert group.
schedule	**Schedule** object	Schedule rule.
triggers	Array of **AlertRuleTrigger** objects	Alert triggering rules.

Table 4-411 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval.
frequency_unit	String	Scheduling interval unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY)
period_interval	Integer	Time window interval.
period_unit	String	Time window unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY.)
delay_interval	Integer	Delay interval.
overtime_interval	Integer	Timeout interval.

Table 4-412 AlertRuleTrigger

Parameter	Type	Description
mode	String	Mode and quantity. **COUNT**.
operator	String	Operator. The value can be: **EQ**: Equal to **NE**: Not equal to **GT**: Greater than **LT**: Less than
expression	String	expression
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
accumulated_times	Integer	accumulated_times

Status code: 400

Table 4-413 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.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.


```
{
  "rule_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
  "pipe_id" : "772fb35b-83bc-46c9-a0b1-ebe31070a889",
  "create_by" : "582dd19dd99d4505a1d7929dc943b169",
  "create_time" : 1665221214,
  "update_by" : "582dd19dd99d4505a1d7929dc943b169",
  "update_time" : 1665221214,
  "delete_time" : 0,
  "rule_name" : "Alert rule",
  "query" : "* | select status, count(*) as count group by status",
  "query_type" : "SQL",
  "status" : "ENABLED",
  "severity" : "TIPS",
  "custom_properties" : {
    "references" : "https://localhost/references",
    "maintainer" : "isap"
  },
  "event_grouping" : true,
  "schedule" : {
    "frequency_interval" : 5,
    "frequency_unit" : "MINUTE",
    "period_interval" : 5,
    "period_unit" : "MINUTE",
    "delay_interval" : 2,
    "overtime_interval" : 10
  },
  "triggers" : [ {
    "mode" : "COUNT",
    "operator" : "GT",
    "expression" : 10,
    "severity" : "TIPS"
  } ]
}
```


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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowAlertRuleSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowAlertRuleRequest request = new ShowAlertRuleRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withRuleId("{rule_id}");
        try {
            ShowAlertRuleResponse response = client.showAlertRule(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowAlertRuleRequest()
        request.workspace_id = "{workspace_id}"
        request.rule_id = "{rule_id}"
        response = client.show_alert_rule(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowAlertRuleRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.RuleId = "{rule_id}"
    response, err := client.ShowAlertRule(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	Request failed.

Error Codes

See **Error Codes**.

4.5.5 Updating an Alert Rule

Function

Update alert rule

Calling Method

For details, see **Calling APIs**.

URI

PUT /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/{rule_id}

Table 4-414 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
rule_id	Yes	String	Alert rule ID.

Request Parameters

Table 4-415 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. You can obtain the token by calling the IAM API used to obtain a user token.

Table 4-416 Request body parameters

Parameter	Mandatory	Type	Description
rule_name	No	String	Alert rule name.
description	No	String	Description.
query	No	String	Query statement.

Parameter	Mandatory	Type	Description
query_type	No	String	Query syntax: SQL.
status	No	String	Status. **enabled**: The rule is enabled. **disabled**: The rule is disabled.
severity	No	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. TIPS, LOW, MEDIUM, HIGH, FATAL
custom_properties	No	Map<String,String>	Custom extension information.
alert_type	No	Map<String,String>	Alert type.
event_grouping	No	Boolean	Alert group.
suppression	No	Boolean	Alert suppression.
simulation	No	Boolean	Simulated alerts.
schedule	No	**Schedule** object	Schedule rule.
triggers	No	Array of **AlertRuleTrigger** objects	Alert triggering rules.

Table 4-417 Schedule

Parameter	Mandatory	Type	Description
frequency_interval	Yes	Integer	Scheduling interval.
frequency_unit	Yes	String	Scheduling interval unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY)
period_interval	Yes	Integer	Time window interval.
period_unit	Yes	String	Time window unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY.)
delay_interval	No	Integer	Delay interval.

Parameter	Mandatory	Type	Description
overtime_interval	No	Integer	Timeout interval.

Table 4-418 AlertRuleTrigger

Parameter	Mandatory	Type	Description
mode	No	String	Mode and quantity. **COUNT**.
operator	No	String	Operator. The value can be: **EQ**: Equal to **NE**: Not equal to **GT**: Greater than **LT**: Less than
expression	Yes	String	expression
severity	No	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
accumulated_times	No	Integer	accumulated_times

Response Parameters

Status code: 200

Table 4-419 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 4-420 Response body parameters

Parameter	Type	Description
rule_id	String	Alert rule ID.
pipe_id	String	Data pipeline ID.
pipe_name	String	Data pipeline name.

Parameter	Type	Description
create_by	String	Creator.
create_time	Long	Creation time.
update_by	String	Updater.
update_time	Long	Update time.
delete_time	Long	Deletion time.
rule_name	String	Alert rule name.
query	String	Query statement.
query_type	String	Query syntax: SQL.
status	String	Status. **enabled**: The rule is enabled. **disabled**: The rule is disabled.
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
custom_properties	Map<String,String>	Custom extension information.
event_grouping	Boolean	Alert group.
schedule	**Schedule** object	Schedule rule.
triggers	Array of **AlertRuleTrigger** objects	Alert triggering rules.

Table 4-421 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval.
frequency_unit	String	Scheduling interval unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY)
period_interval	Integer	Time window interval.
period_unit	String	Time window unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY.)
delay_interval	Integer	Delay interval.

Parameter	Type	Description
overtime_interval	Integer	Timeout interval.

Table 4-422 AlertRuleTrigger

Parameter	Type	Description
mode	String	Mode and quantity. **COUNT**.
operator	String	Operator. The value can be: **EQ**: Equal to **NE**: Not equal to **GT**: Greater than **LT**: Less than
expression	String	expression
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
accumulated_times	Integer	accumulated_times

Status code: 400

Table 4-423 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.

Example Requests

Update an alert rule whose name is Alert rule, query type is SQL, status is Enabled, and Severity is Warning.

```
{
  "rule_name" : "Alert rule",
  "query" : "* | select status, count(*) as count group by status",
  "query_type" : "SQL",
  "status" : "ENABLED",
  "severity" : "TIPS",
  "custom_properties" : {
    "references" : "https://localhost/references",
    "maintainer" : "isap"
  },
```



```
  "event_grouping" : true,
  "schedule" : {
    "frequency_interval" : 5,
    "frequency_unit" : "MINUTE",
    "period_interval" : 5,
    "period_unit" : "MINUTE",
    "delay_interval" : 2,
    "overtime_interval" : 10
  },
  "triggers" : [ {
    "mode" : "COUNT",
    "operator" : "GT",
    "expression" : 10,
    "severity" : "TIPS"
  } ]
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "rule_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
  "pipe_id" : "772fb35b-83bc-46c9-a0b1-ebe31070a889",
  "create_by" : "582dd19dd99d4505a1d7929dc943b169",
  "create_time" : 1665221214,
  "update_by" : "582dd19dd99d4505a1d7929dc943b169",
  "update_time" : 1665221214,
  "delete_time" : 0,
  "rule_name" : "Alert rule",
  "query" : "* | select status, count(*) as count group by status",
  "query_type" : "SQL",
  "status" : "ENABLED",
  "severity" : "TIPS",
  "custom_properties" : {
    "references" : "https://localhost/references",
    "maintainer" : "isap"
  },
  "event_grouping" : true,
  "schedule" : {
    "frequency_interval" : 5,
    "frequency_unit" : "MINUTE",
    "period_interval" : 5,
    "period_unit" : "MINUTE",
    "delay_interval" : 2,
    "overtime_interval" : 10
  },
  "triggers" : [ {
    "mode" : "COUNT",
    "operator" : "GT",
    "expression" : 10,
    "severity" : "TIPS"
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Update an alert rule whose name is Alert rule, query type is SQL, status is Enabled, and Severity is Warning.


```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;
import java.util.Map;
import java.util.HashMap;

public class UpdateAlertRuleSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateAlertRuleRequest request = new UpdateAlertRuleRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withRuleId("{rule_id}");
        UpdateAlertRuleRequestBody body = new UpdateAlertRuleRequestBody();
        List<AlertRuleTrigger> listbodyTriggers = new ArrayList<>();
        listbodyTriggers.add(
            new AlertRuleTrigger()
                .withMode(AlertRuleTrigger.ModeEnum.fromValue("COUNT"))
                .withOperator(AlertRuleTrigger.OperatorEnum.fromValue("GT"))
                .withExpression("10")
                .withSeverity(AlertRuleTrigger.SeverityEnum.fromValue("TIPS"))
        );
        Schedule schedulebody = new Schedule();
        schedulebody.withFrequencyInterval(5)
            .withFrequencyUnit(Schedule.FrequencyUnitEnum.fromValue("MINUTE"))
            .withPeriodInterval(5)
            .withPeriodUnit(Schedule.PeriodUnitEnum.fromValue("MINUTE"))
            .withDelayInterval(2)
            .withOvertimeInterval(10);
        Map<String, String> listbodyCustomProperties = new HashMap<>();
        listbodyCustomProperties.put("references", "https://localhost/references");
        listbodyCustomProperties.put("maintainer", "isap");
        body.withTriggers(listbodyTriggers);
        body.withSchedule(schedulebody);
        body.withEventGrouping(true);
        body.withCustomProperties(listbodyCustomProperties);
        body.withSeverity(UpdateAlertRuleRequestBody.SeverityEnum.fromValue("TIPS"));
        body.withStatus(UpdateAlertRuleRequestBody.StatusEnum.fromValue("ENABLED"));
        body.withQueryType(UpdateAlertRuleRequestBody.QueryTypeEnum.fromValue("SQL"));
        body.withQuery("* | select status, count(*) as count group by status");
        body.withRuleName("Alert rule");
        request.withBody(body);
```



```
        try {
            UpdateAlertRuleResponse response = client.updateAlertRule(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 an alert rule whose name is Alert rule, query type is SQL, status is Enabled, and Severity is Warning.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateAlertRuleRequest()
        request.workspace_id = "{workspace_id}"
        request.rule_id = "{rule_id}"
        listTriggersbody = [
            AlertRuleTrigger(
                mode="COUNT",
                operator="GT",
                expression="10",
                severity="TIPS"
            )
        ]
        schedulebody = Schedule(
            frequency_interval=5,
            frequency_unit="MINUTE",
            period_interval=5,
            period_unit="MINUTE",
            delay_interval=2,
            overtime_interval=10
        )
        listCustomPropertiesbody = {
            "references": "https://localhost/references",
```



```
            "maintainer": "isap"
        }
        request.body = UpdateAlertRuleRequestBody(
            triggers=listTriggersbody,
            schedule=schedulebody,
            event_grouping=True,
            custom_properties=listCustomPropertiesbody,
            severity="TIPS",
            status="ENABLED",
            query_type="SQL",
            query="* | select status, count(*) as count group by status",
            rule_name="Alert rule"
        )
        response = client.update_alert_rule(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 an alert rule whose name is Alert rule, query type is SQL, status is Enabled, and Severity is Warning.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateAlertRuleRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.RuleId = "{rule_id}"
    modeTriggers:= model.GetAlertRuleTriggerModeEnum().COUNT
    operatorTriggers:= model.GetAlertRuleTriggerOperatorEnum().GT
    severityTriggers:= model.GetAlertRuleTriggerSeverityEnum().TIPS
    var listTriggersbody = []model.AlertRuleTrigger{
        {
            Mode: &modeTriggers,
            Operator: &operatorTriggers,
            Expression: "10",
```



```
            Severity: &severityTriggers,
        },
    }
    delayIntervalSchedule:= int32(2)
    overtimeIntervalSchedule:= int32(10)
    schedulebody := &model.Schedule{
        FrequencyInterval: int32(5),
        FrequencyUnit: model.GetScheduleFrequencyUnitEnum().MINUTE,
        PeriodInterval: int32(5),
        PeriodUnit: model.GetSchedulePeriodUnitEnum().MINUTE,
        DelayInterval: &delayIntervalSchedule,
        OvertimeInterval: &overtimeIntervalSchedule,
    }
    var listCustomPropertiesbody = map[string]string{
        "references": "https://localhost/references",
        "maintainer": "isap",
    }
    eventGroupingUpdateAlertRuleRequestBody:= true
    severityUpdateAlertRuleRequestBody:= model.GetUpdateAlertRuleRequestBodySeverityEnum().TIPS
    statusUpdateAlertRuleRequestBody:= model.GetUpdateAlertRuleRequestBodyStatusEnum().ENABLED
    queryTypeUpdateAlertRuleRequestBody:= model.GetUpdateAlertRuleRequestBodyQueryTypeEnum().SQL
    queryUpdateAlertRuleRequestBody:= "* | select status, count(*) as count group by status"
    ruleNameUpdateAlertRuleRequestBody:= "Alert rule"
    request.Body = &model.UpdateAlertRuleRequestBody{
        Triggers: &listTriggersbody,
        Schedule: schedulebody,
        EventGrouping: &eventGroupingUpdateAlertRuleRequestBody,
        CustomProperties: listCustomPropertiesbody,
        Severity: &severityUpdateAlertRuleRequestBody,
        Status: &statusUpdateAlertRuleRequestBody,
        QueryType: &queryTypeUpdateAlertRuleRequestBody,
        Query: &queryUpdateAlertRuleRequestBody,
        RuleName: &ruleNameUpdateAlertRuleRequestBody,
    }
    response, err := client.UpdateAlertRule(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	Request failed.

Error Codes

See **Error Codes**.

4.5.6 Simulating an Alert Rule

Function

Simulate alert rule

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/simulation

Table 4-424 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-425 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. You can obtain the token by calling the IAM API used to obtain a user token.

Table 4-426 Request body parameters

Parameter	Mandatory	Type	Description
pipe_id	Yes	String	Data pipeline ID.
query	Yes	String	Query statement.
query_type	No	String	Query syntax: SQL.
from	Yes	Long	Start time.
to	Yes	Long	End time.
event_grouping	No	Boolean	Alert group.

Parameter	Mandatory	Type	Description
triggers	Yes	Array of **AlertRuleTrigger** objects	Alert triggering rules.

Table 4-427 AlertRuleTrigger

Parameter	Mandatory	Type	Description
mode	No	String	Mode and quantity. **COUNT**.
operator	No	String	Operator. The value can be: **EQ**: Equal to **NE**: Not equal to **GT**: Greater than **LT**: Less than
expression	Yes	String	expression
severity	No	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
accumulated_times	No	Integer	accumulated_times

Response Parameters

Status code: 200

Table 4-428 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 4-429 Response body parameters

Parameter	Type	Description
alert_count	Integer	Number of alerts.

Parameter	Type	Description
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)

Status code: 400

Table 4-430 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.

Example Requests

Simulate an alert rule. The ID of the pipe to which the alarm rule belongs is ead2769b-afb0-45dd-b9fa-a2953e6ac82f, the query type is SQL, and the severity is Warning.

```
{
  "pipe_id" : "ead2769b-afb0-45dd-b9fa-a2953e6ac82f",
  "query" : "* | select status, count(*) as count group by status",
  "query_type" : "SQL",
  "event_grouping" : true,
  "from" : 1665221214000,
  "to" : 1665546370000,
  "triggers" : [ {
    "mode" : "COUNT",
    "operator" : "GT",
    "expression" : 10,
    "severity" : "TIPS"
  } ]
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "alert_count" : 100,
  "severity" : "TIPS"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Simulate an alert rule. The ID of the pipe to which the alarm rule belongs is ead2769b-afb0-45dd-b9fa-a2953e6ac82f, the query type is SQL, and the severity is Warning.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class CreateAlertRuleSimulationSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateAlertRuleSimulationRequest request = new CreateAlertRuleSimulationRequest();
        request.withWorkspaceId("{workspace_id}");
        CreateAlertRuleSimulationRequestBody body = new CreateAlertRuleSimulationRequestBody();
        List<AlertRuleTrigger> listbodyTriggers = new ArrayList<>();
        listbodyTriggers.add(
            new AlertRuleTrigger()
                .withMode(AlertRuleTrigger.ModeEnum.fromValue("COUNT"))
                .withOperator(AlertRuleTrigger.OperatorEnum.fromValue("GT"))
                .withExpression("10")
                .withSeverity(AlertRuleTrigger.SeverityEnum.fromValue("TIPS"))
        );
        body.withTriggers(listbodyTriggers);
        body.withEventGrouping(true);
        body.withTo(1665546370000L);
        body.withFrom(1665221214000L);
        body.withQueryType(CreateAlertRuleSimulationRequestBody.QueryTypeEnum.fromValue("SQL"));
        body.withQuery("* | select status, count(*) as count group by status");
        body.withPipeId("ead2769b-afb0-45dd-b9fa-a2953e6ac82f");
        request.withBody(body);
        try {
            CreateAlertRuleSimulationResponse response = client.createAlertRuleSimulation(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

Simulate an alert rule. The ID of the pipe to which the alarm rule belongs is ead2769b-afb0-45dd-b9fa-a2953e6ac82f, the query type is SQL, and the severity is Warning.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateAlertRuleSimulationRequest()
        request.workspace_id = "{workspace_id}"
        listTriggersbody = [
            AlertRuleTrigger(
                mode="COUNT",
                operator="GT",
                expression="10",
                severity="TIPS"
            )
        ]
        request.body = CreateAlertRuleSimulationRequestBody(
            triggers=listTriggersbody,
            event_grouping=True,
            to=1665546370000,
            _from=1665221214000,
            query_type="SQL",
            query="* | select status, count(*) as count group by status",
            pipe_id="ead2769b-afb0-45dd-b9fa-a2953e6ac82f"
        )
        response = client.create_alert_rule_simulation(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

Simulate an alert rule. The ID of the pipe to which the alarm rule belongs is ead2769b-afb0-45dd-b9fa-a2953e6ac82f, the query type is SQL, and the severity is Warning.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateAlertRuleSimulationRequest{}
    request.WorkspaceId = "{workspace_id}"
    modeTriggers:= model.GetAlertRuleTriggerModeEnum().COUNT
    operatorTriggers:= model.GetAlertRuleTriggerOperatorEnum().GT
    severityTriggers:= model.GetAlertRuleTriggerSeverityEnum().TIPS
    var listTriggersbody = []model.AlertRuleTrigger{
        {
            Mode: &modeTriggers,
            Operator: &operatorTriggers,
            Expression: "10",
            Severity: &severityTriggers,
        },
    }
    eventGroupingCreateAlertRuleSimulationRequestBody:= true
    queryTypeCreateAlertRuleSimulationRequestBody:= model.GetCreateAlertRuleSimulationRequestBodyQueryTypeEnum().SQL
    request.Body = &model.CreateAlertRuleSimulationRequestBody{
        Triggers: listTriggersbody,
        EventGrouping: &eventGroupingCreateAlertRuleSimulationRequestBody,
        To: int64(1665546370000),
        From: int64(1665221214000),
        QueryType: &queryTypeCreateAlertRuleSimulationRequestBody,
        Query: "* | select status, count(*) as count group by status",
        PipeId: "ead2769b-afb0-45dd-b9fa-a2953e6ac82f",
    }
    response, err := client.CreateAlertRuleSimulation(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	Request failed.

Error Codes

See **Error Codes**.

4.5.7 Total number of alert rules.

Function

List alert rule metrics

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/metrics

Table 4-431 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-432 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. You can obtain the token by calling the IAM API used to obtain a user token.

Response Parameters

Status code: 200

Table 4-433 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 4-434 Response body parameters

Parameter	Type	Description
category	String	Metric category and number of groups. **GROUP_COUNT**.
metric	Map<String,Number>	Metric value.

Status code: 400

Table 4-435 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.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

- Example 1

```
{
  "category" : {
    "GROUP_COUNT" : null
  },
  "metric" : null
}
```

- Example 2

```
{
  "category" : "GROUP_COUNT",
  "metric" : {
    "ENABLED" : 8,
    "DISABLED" : 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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListAlertRuleMetricsSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListAlertRuleMetricsRequest request = new ListAlertRuleMetricsRequest();
        request.withWorkspaceId("{workspace_id}");
        try {
            ListAlertRuleMetricsResponse response = client.listAlertRuleMetrics(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAlertRuleMetricsRequest()
        request.workspace_id = "{workspace_id}"
        response = client.list_alert_rule_metrics(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAlertRuleMetricsRequest{}
    request.WorkspaceId = "{workspace_id}"
    response, err := client.ListAlertRuleMetrics(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	Request failed.

Error Codes

See **Error Codes**.

4.5.8 Enabling an Alert Rule

Function

Enable alert rule

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/enable

Table 4-436 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-437 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. You can obtain the token by calling the IAM API used to obtain a user token.

Table 4-438 Request body parameters

Parameter	Mandatory	Type	Description
[items]	Yes	Array of strings	Request for enabling an alert rule.

Response Parameters

Status code: 200

Table 4-439 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 4-440 Response body parameters

Parameter	Type	Description
fail_list	Array of **AlertRule** objects	Alert rule ID.
success_list	Array of **AlertRule** objects	Alert rule ID.

Table 4-441 AlertRule

Parameter	Type	Description
rule_id	String	Alert rule ID.
pipe_id	String	Data pipeline ID.
pipe_name	String	Data pipeline name.
create_by	String	Creator.
create_time	Long	Creation time.
update_by	String	Updater.
update_time	Long	Update time.
delete_time	Long	Deletion time.
rule_name	String	Alert rule name.
query	String	Query statement.
query_type	String	Query syntax: SQL.
status	String	Status. **enabled**: The rule is enabled. **disabled**: The rule is disabled.
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
custom_properties	Map<String,String>	Custom extension information.
event_grouping	Boolean	Alert group.
schedule	**Schedule** object	Schedule rule.
triggers	Array of **AlertRuleTrigger** objects	Alert triggering rules.

Table 4-442 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval.
frequency_unit	String	Scheduling interval unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY)
period_interval	Integer	Time window interval.
period_unit	String	Time window unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY.)
delay_interval	Integer	Delay interval.
overtime_interval	Integer	Timeout interval.

Table 4-443 AlertRuleTrigger

Parameter	Type	Description
mode	String	Mode and quantity. **COUNT**.
operator	String	Operator. The value can be: **EQ**: Equal to **NE**: Not equal to **GT**: Greater than **LT**: Less than
expression	String	expression
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
accumulated_times	Integer	accumulated_times

Status code: 400

Table 4-444 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.

Example Requests

Enable an alert rule. Rule ID: 123123.

```
[ "123123" ]
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "fail_list" : [ ],
  "success_list" : [ ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Enable an alert rule. Rule ID: 123123.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class EnableAlertRuleSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        EnableAlertRuleRequest request = new EnableAlertRuleRequest();
        request.withWorkspaceId("{workspace_id}");
        List<String> listbodyBody = new ArrayList<>();
        listbodyBody.add("123123");
        request.withBody(listbodyBody);
        try {
```



```
            EnableAlertRuleResponse response = client.enableAlertRule(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 an alert rule. Rule ID: 123123.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = EnableAlertRuleRequest()
        request.workspace_id = "{workspace_id}"
        listBodybody = [
            "123123"
        ]
        request.body = listBodybody
        response = client.enable_alert_rule(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 an alert rule. Rule ID: 123123.

```
package main

import (
    "fmt"
```



```
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.EnableAlertRuleRequest{}
    request.WorkspaceId = "{workspace_id}"
    var listBodybody = []string{
        "123123",
    }
    request.Body = &listBodybody
    response, err := client.EnableAlertRule(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	Request failed.

Error Codes

See **Error Codes**.

4.5.9 Disabling an Alert Rule

Function

Disable alert rule

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/disable

Table 4-445 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-446 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. You can obtain the token by calling the IAM API used to obtain a user token.

Table 4-447 Request body parameters

Parameter	Mandatory	Type	Description
[items]	Yes	Array of strings	Request for disabling an alert rule.

Response Parameters

Status code: 200

Table 4-448 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 4-449 Response body parameters

Parameter	Type	Description
fail_list	Array of **AlertRule** objects	Alert rule ID.
success_list	Array of **AlertRule** objects	Alert rule ID.

Table 4-450 AlertRule

Parameter	Type	Description
rule_id	String	Alert rule ID.
pipe_id	String	Data pipeline ID.
pipe_name	String	Data pipeline name.
create_by	String	Creator.
create_time	Long	Creation time.
update_by	String	Updater.
update_time	Long	Update time.
delete_time	Long	Deletion time.
rule_name	String	Alert rule name.
query	String	Query statement.
query_type	String	Query syntax: SQL.
status	String	Status. **enabled**: The rule is enabled. **disabled**: The rule is disabled.
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)

Parameter	Type	Description
custom_properties	Map<String,String>	Custom extension information.
event_grouping	Boolean	Alert group.
schedule	**Schedule** object	Schedule rule.
triggers	Array of **AlertRuleTrigger** objects	Alert triggering rules.

Table 4-451 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval.
frequency_unit	String	Scheduling interval unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY)
period_interval	Integer	Time window interval.
period_unit	String	Time window unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY.)
delay_interval	Integer	Delay interval.
overtime_interval	Integer	Timeout interval.

Table 4-452 AlertRuleTrigger

Parameter	Type	Description
mode	String	Mode and quantity. **COUNT**.
operator	String	Operator. The value can be: **EQ**: Equal to **NE**: Not equal to **GT**: Greater than **LT**: Less than
expression	String	expression
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)

Parameter	Type	Description
accumulated_times	Integer	accumulated_times

Status code: 400

Table 4-453 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.

Example Requests

Disable an alert rule. Rule ID: 123123.

```
[ "123123" ]
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "fail_list" : [ ],
  "success_list" : [ ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Disable an alert rule. Rule ID: 123123.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class DisableAlertRuleSolution {
```



```
    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DisableAlertRuleRequest request = new DisableAlertRuleRequest();
        request.withWorkspaceId("{workspace_id}");
        List<String> listbodyBody = new ArrayList<>();
        listbodyBody.add("123123");
        request.withBody(listbodyBody);
        try {
            DisableAlertRuleResponse response = client.disableAlertRule(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 an alert rule. Rule ID: 123123.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()
```



```
    try:
        request = DisableAlertRuleRequest()
        request.workspace_id = "{workspace_id}"
        listBodybody = [
            "123123"
        ]
        request.body = listBodybody
        response = client.disable_alert_rule(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 an alert rule. Rule ID: 123123.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DisableAlertRuleRequest{}
    request.WorkspaceId = "{workspace_id}"
    var listBodybody = []string{
        "123123",
    }
    request.Body = &listBodybody
    response, err := client.DisableAlertRule(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	Request failed.

Error Codes

See **Error Codes**.

4.5.10 Querying the Alert Rule Template List

Function

List alert rule templates

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/templates

Table 4-454 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Table 4-455 Query Parameters

Parameter	Mandatory	Type	Description
offset	Yes	Long	Offset.
limit	Yes	Long	Number of items.
sort_key	No	String	Sorting field.

Parameter	Mandatory	Type	Description
sort_dir	No	String	Sorting order. You can sort fields in ascending or descending order.
severity	No	Array of strings	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. TIPS, LOW, MEDIUM, HIGH, FATAL

Request Parameters

Table 4-456 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. You can obtain the token by calling the IAM API used to obtain a user token.

Response Parameters

Status code: 200

Table 4-457 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 4-458 Response body parameters

Parameter	Type	Description
count	Long	Total number.
records	Array of **AlertRuleTemplate** objects	Alert rule template.

Table 4-459 AlertRuleTemplate

Parameter	Type	Description
template_id	String	Alert rule template ID.
update_time	Long	Update time.
template_name	String	Name of the alert rule template.
data_source	String	Data source.
version	String	Version.
query	String	Query statement.
query_type	String	Query syntax: SQL.
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
custom_properties	Map<String,String>	Custom extension information.
event_grouping	Boolean	Alert group.
schedule	**Schedule** object	Schedule rule.
triggers	Array of **AlertRuleTrigger** objects	Alert triggering rules.

Table 4-460 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval.
frequency_unit	String	Scheduling interval unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY)
period_interval	Integer	Time window interval.
period_unit	String	Time window unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY.)
delay_interval	Integer	Delay interval.
overtime_interval	Integer	Timeout interval.

Table 4-461 AlertRuleTrigger

Parameter	Type	Description
mode	String	Mode and quantity. **COUNT**.
operator	String	Operator. The value can be: **EQ**: Equal to **NE**: Not equal to **GT**: Greater than **LT**: Less than
expression	String	expression
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
accumulated_times	Integer	accumulated_times

Status code: 400

Table 4-462 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.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.


```
{
  "count" : 9223372036854776000,
  "records" : [ {
    "template_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
    "update_time" : 1665221214,
    "template_name" : "Alert rule template",
    "data_source" : "sec_hss_vul",
    "version" : "1.0.0",
    "query" : "* | select status, count(*) as count group by status",
    "query_type" : "SQL",
    "severity" : "TIPS",
    "custom_properties" : {
```



```
    "references" : "https://localhost/references",
    "maintainer" : "isap"
   },
   "event_grouping" : true,
   "schedule" : {
    "frequency_interval" : 5,
    "frequency_unit" : "MINUTE",
    "period_interval" : 5,
    "period_unit" : "MINUTE",
    "delay_interval" : 2,
    "overtime_interval" : 10
   },
   "triggers" : [ {
    "mode" : "COUNT",
    "operator" : "GT",
    "expression" : 10,
    "severity" : "TIPS"
   } ]
  } ]
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListAlertRuleTemplatesSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListAlertRuleTemplatesRequest request = new ListAlertRuleTemplatesRequest();
        request.withWorkspaceId("{workspace_id}");
        try {
            ListAlertRuleTemplatesResponse response = client.listAlertRuleTemplates(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAlertRuleTemplatesRequest()
        request.workspace_id = "{workspace_id}"
        response = client.list_alert_rule_templates(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAlertRuleTemplatesRequest{}
    request.WorkspaceId = "{workspace_id}"
    response, err := client.ListAlertRuleTemplates(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	Request failed.

Error Codes

See **Error Codes**.

4.5.11 Viewing Alert Rule Templates

Function

List alert rule templates

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/templates/{template_id}

Table 4-463 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
template_id	Yes	String	Alert rule template ID.

Request Parameters

Table 4-464 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. You can obtain the token by calling the IAM API used to obtain a user token.

Response Parameters

Status code: 200

Table 4-465 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 4-466 Response body parameters

Parameter	Type	Description
template_id	String	Alert rule template ID.
update_time	Long	Update time.
template_name	String	Name of the alert rule template.
data_source	String	Data source.
version	String	Version.
query	String	Query statement.
query_type	String	Query syntax: SQL.

Parameter	Type	Description
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
custom_properties	Map<String,String>	Custom extension information.
event_grouping	Boolean	Alert group.
schedule	**Schedule** object	Schedule rule.
triggers	Array of **AlertRuleTrigger** objects	Alert triggering rules.

Table 4-467 Schedule

Parameter	Type	Description
frequency_interval	Integer	Scheduling interval.
frequency_unit	String	Scheduling interval unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY)
period_interval	Integer	Time window interval.
period_unit	String	Time window unit, which can be minute, hour, or day. (MINUTE, HOUR, DAY.)
delay_interval	Integer	Delay interval.
overtime_interval	Integer	Timeout interval.

Table 4-468 AlertRuleTrigger

Parameter	Type	Description
mode	String	Mode and quantity. **COUNT**.
operator	String	Operator. The value can be: **EQ**: Equal to **NE**: Not equal to **GT**: Greater than **LT**: Less than
expression	String	expression

Parameter	Type	Description
severity	String	Severity. The options are **Informational**, **Low**, **Medium**, **High**, and **Critical**. (TIPS, LOW, MEDIUM, HIGH, FATAL)
accumulated_times	Integer	accumulated_times

Status code: 400

Table 4-469 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.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.


```
{
  "template_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
  "update_time" : 1665221214,
  "template_name" : "Alert rule template",
  "data_source" : "sec_hss_vul",
  "version" : "1.0.0",
  "query" : "* | select status, count(*) as count group by status",
  "query_type" : "SQL",
  "severity" : "TIPS",
  "custom_properties" : {
    "references" : "https://localhost/references",
    "maintainer" : "isap"
  },
  "event_grouping" : true,
  "schedule" : {
    "frequency_interval" : 5,
    "frequency_unit" : "MINUTE",
    "period_interval" : 5,
    "period_unit" : "MINUTE",
    "delay_interval" : 2,
    "overtime_interval" : 10
  },
  "triggers" : [ {
    "mode" : "COUNT",
    "operator" : "GT",
    "expression" : 10,
    "severity" : "TIPS"
```



```
 } ]
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowAlertRuleTemplateSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowAlertRuleTemplateRequest request = new ShowAlertRuleTemplateRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withTemplateId("{template_id}");
        try {
            ShowAlertRuleTemplateResponse response = client.showAlertRuleTemplate(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowAlertRuleTemplateRequest()
        request.workspace_id = "{workspace_id}"
        request.template_id = "{template_id}"
        response = client.show_alert_rule_template(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowAlertRuleTemplateRequest{}
```



```
    request.WorkspaceId = "{workspace_id}"
    request.TemplateId = "{template_id}"
    response, err := client.ShowAlertRuleTemplate(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	Request failed.

Error Codes

See **Error Codes**.

4.6 Playbook Version Management

4.6.1 Cloning a Playbook and Its Version

Function

Cloning a Playbook and Its Version

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/clone

Table 4-470 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Parameter	Mandatory	Type	Description
workspace_id	Yes	String	Workspace ID.
version_id	Yes	String	Playbook version ID.

Request Parameters

Table 4-471 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-472 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Name.

Response Parameters

Status code: 200

Table 4-473 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-474 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message

Parameter	Type	Description
data	**PlaybookVersionInfo** object	Playbook version details.

Table 4-475 PlaybookVersionInfo

Parameter	Type	Description
id	String	Playbook version ID.
description	String	Description.
create_time	String	Creation time.
update_time	String	Update time.
project_id	String	Project ID.
creator_id	String	Creator ID.
modifier_id	String	ID of the editor.
playbook_id	String	Playbook ID.
version	String	Version No.
enabled	Boolean	Enable or not. **true**: Enabled **false**: Disabled
status	String	Playbook version status. Options: **Editing**, **APPROVING**, **UNPASSED**, and **PUBLISHED**
action_strategy	String	Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is **ASYNC**.
actions	Array of **ActionInfo** objects	The list of workflows associated with the playbook.
rule_enable	Boolean	Whether to enable the trigger condition filter.
rules	**RuleInfo** object	Playbook trigger information.
dataclass_id	String	Data class ID.
trigger_type	String	How the playbook is triggered. Options: **EVENT** and **TIMER**

Parameter	Type	Description
dataobject_create	Boolean	Whether to trigger a playbook when a data object is created.
dataobject_update	Boolean	Whether to trigger a playbook when a data object is updated.
dataobject_delete	Boolean	Whether to trigger a playbook when a data object is deleted.
version_type	Integer	Version type (**0**: Draft; **1**: Released).
rule_id	String	Filter rule ID.
dataclass_name	String	Data class name.
approve_name	String	Reviewer.

Table 4-476 ActionInfo

Parameter	Type	Description
id	String	Playbook workflow ID.
name	String	Workflow name.
description	String	Description.
action_type	String	Workflow type.
action_id	String	Workflow ID.
playbook_id	String	Playbook ID.
playbook_version_id	String	Playbook version ID.
project_id	String	Project ID.

Table 4-477 RuleInfo

Parameter	Type	Description
id	String	Rule ID.
project_id	String	Project ID.
rule	String	Trigger rules.

Status code: 400

Table 4-478 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-479 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Clone a playbook and its version. The playbook name is **name**.

```
{
  "name" : "name"
}
```

Example Responses

Status code: 200

Response parameters for a successful request.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "modifier_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "enabled" : true,
    "status" : "editing",
    "action_strategy" : "sync",
    "actions" : [ {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "description" : "This my XXXX",
      "action_type" : "Workflow",
      "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "playbook_id" : "string",
      "playbook_version_id" : "string",
      "project_id" : "string"
    } ],
    "rule_enable" : true,
    "rules" : {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "rule" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
```



```
  },
  "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "trigger_type" : "event",
  "dataobject_create" : true,
  "dataobject_update" : true,
  "dataobject_delete" : true,
  "version_type" : 1,
  "rule_id" : "string",
  "dataclass_name" : "string",
  "approve_name" : "string"
 }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Clone a playbook and its version. The playbook name is **name**.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class CopyPlaybookVersionSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CopyPlaybookVersionRequest request = new CopyPlaybookVersionRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withVersionId("{version_id}");
        CopyPlaybookInfo body = new CopyPlaybookInfo();
        body.withName("name");
        request.withBody(body);
        try {
            CopyPlaybookVersionResponse response = client.copyPlaybookVersion(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

Clone a playbook and its version. The playbook name is **name**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CopyPlaybookVersionRequest()
        request.workspace_id = "{workspace_id}"
        request.version_id = "{version_id}"
        request.body = CopyPlaybookInfo(
            name="name"
        )
        response = client.copy_playbook_version(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

Clone a playbook and its version. The playbook name is **name**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CopyPlaybookVersionRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.VersionId = "{version_id}"
    nameCopyPlaybookInfo:= "name"
    request.Body = &model.CopyPlaybookInfo{
        Name: &nameCopyPlaybookInfo,
    }
    response, err := client.CopyPlaybookVersion(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	Response parameters for a successful request.
400	Response parameters for failed requests.

Error Codes

See **Error Codes**.

4.6.2 Querying the Playbook Version List

Function

This API is used to query the version list of a playbook.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}/versions

Table 4-480 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
playbook_id	Yes	String	Playbook ID.

Table 4-481 Query Parameters

Parameter	Mandatory	Type	Description
status	No	String	Playbook version status. Options: **Editing**, **APPROVING**, **UNPASSED**, and **PUBLISHED**
enabled	No	Integer	Enable/Disable
version_type	No	Integer	Version type. The options are as follows: **0**: Draft version. **1**: Formal version.
offset	No	Integer	Pagination query parameter. This parameter specifies the start position of the query result. The value starts from **0**.
limit	No	Integer	The maximum number of records can be returned on each page for a pagination query. The value starts from 1.

Request Parameters

Table 4-482 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-483 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-484 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
size	Integer	Records on each page.
page	Integer	Current page number.
total	Integer	Total number.
data	Array of **PlaybookVersionListEntity** objects	Playbook version list.

Table 4-485 PlaybookVersionListEntity

Parameter	Type	Description
id	String	Playbook version ID.
description	String	Description.
create_time	String	Creation time.
update_time	String	Update time.
project_id	String	Project ID.
creator_id	String	Creator ID.
modifier_id	String	ID of the editor.
playbook_id	String	Playbook ID.
version	String	Version No.
enabled	Boolean	Whether to activate.
status	String	Status. (**EDITING**: Being edited; **APPROVING**: Being reviewed; **UNPASSED**: Rejected; **PUBLISHED**: Approved)
action_strategy	String	Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is **ASYNC**.
rule_enable	Boolean	Whether the filtering rule is enabled.
dataclass_id	String	Data class ID.
trigger_type	String	Trigger mode. **EVENT**: Triggered by incidents; **TIMER**: Triggered as scheduled.
dataobject_create	Boolean	Whether to trigger a playbook when a data object is created.
dataobject_update	Boolean	Whether to trigger a playbook when a data object is updated.
dataobject_delete	Boolean	Whether to trigger a playbook when a data object is deleted.
version_type	Integer	Version type.
rule_id	String	Filter rule ID.
dataclass_name	String	Data class name.
approve_name	String	Reviewer.

Status code: 400

Table 4-486 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-487 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : 0,
  "message" : "Error message",
  "size" : 3,
  "page" : 10,
  "total" : 41,
  "data" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "modifier_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "enabled" : true,
    "status" : "editing",
    "action_strategy" : "sync",
    "rule_enable" : true,
    "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "trigger_type" : "event",
    "dataobject_create" : true,
    "dataobject_update" : true,
    "dataobject_delete" : true,
    "version_type" : 1,
    "rule_id" : "string",
    "dataclass_name" : "string",
    "approve_name" : "string"
  } ]
}
```


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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListPlaybookVersionsSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybookVersionsRequest request = new ListPlaybookVersionsRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withPlaybookId("{playbook_id}");
        try {
            ListPlaybookVersionsResponse response = client.listPlaybookVersions(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListPlaybookVersionsRequest()
        request.workspace_id = "{workspace_id}"
        request.playbook_id = "{playbook_id}"
        response = client.list_playbook_versions(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPlaybookVersionsRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.PlaybookId = "{playbook_id}"
    response, err := client.ListPlaybookVersions(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.6.3 Creating a Playbook Version

Function

This API is used to create a playbook version.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}/versions

Table 4-488 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
playbook_id	Yes	String	Playbook ID.

Request Parameters

Table 4-489 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-490 Request body parameters

Parameter	Mandatory	Type	Description
description	No	String	Description.
workspace_id	No	String	Workspace ID.
playbook_id	No	String	Playbook ID.
actions	No	Array of **ActionInfo** objects	The list of the associated workflows.
dataclass_id	No	String	Data class ID.
rule_enable	No	Boolean	Whether the filter rule is enabled.
rule_id	No	String	Filter rule ID.
trigger_type	No	String	Trigger method. **EVENT**: Triggered by incidents; **TIMER**: Triggered as scheduled.
dataobject_create	No	Boolean	Whether to trigger a playbook when a data object is created.
dataobject_update	No	Boolean	Whether to trigger a playbook when a data object is updated.
dataobject_delete	No	Boolean	Whether to trigger a playbook when a data object is deleted.
action_strategy	No	String	Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is **ASYNC**.

Table 4-491 ActionInfo

Parameter	Mandatory	Type	Description
id	No	String	Playbook workflow ID.
name	No	String	Workflow name.
description	No	String	Description.
action_type	No	String	Workflow type.
action_id	No	String	Workflow ID.
playbook_id	No	String	Playbook ID.
playbook_version_id	No	String	Playbook version ID.
project_id	No	String	Project ID.

Response Parameters

Status code: 200

Table 4-492 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-493 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message
data	**PlaybookVersionInfo** object	Playbook version details.

Table 4-494 PlaybookVersionInfo

Parameter	Type	Description
id	String	Playbook version ID.
description	String	Description.

Parameter	Type	Description
create_time	String	Creation time.
update_time	String	Update time.
project_id	String	Project ID.
creator_id	String	Creator ID.
modifier_id	String	ID of the editor.
playbook_id	String	Playbook ID.
version	String	Version No.
enabled	Boolean	Enable or not. **true**: Enabled **false**: Disabled
status	String	Playbook version status. Options: **Editing**, **APPROVING**, **UNPASSED**, and **PUBLISHED**
action_strategy	String	Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is **ASYNC**.
actions	Array of **ActionInfo** objects	The list of workflows associated with the playbook.
rule_enable	Boolean	Whether to enable the trigger condition filter.
rules	**RuleInfo** object	Playbook trigger information.
dataclass_id	String	Data class ID.
trigger_type	String	How the playbook is triggered. Options: **EVENT** and **TIMER**
dataobject_create	Boolean	Whether to trigger a playbook when a data object is created.
dataobject_update	Boolean	Whether to trigger a playbook when a data object is updated.
dataobject_delete	Boolean	Whether to trigger a playbook when a data object is deleted.
version_type	Integer	Version type (**0**: Draft; **1**: Released).
rule_id	String	Filter rule ID.
dataclass_name	String	Data class name.

Parameter	Type	Description
approve_name	String	Reviewer.

Table 4-495 ActionInfo

Parameter	Type	Description
id	String	Playbook workflow ID.
name	String	Workflow name.
description	String	Description.
action_type	String	Workflow type.
action_id	String	Workflow ID.
playbook_id	String	Playbook ID.
playbook_version_id	String	Playbook version ID.
project_id	String	Project ID.

Table 4-496 RuleInfo

Parameter	Type	Description
id	String	Rule ID.
project_id	String	Project ID.
rule	String	Trigger rules.

Status code: 400

Table 4-497 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-498 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Create a playbook version. Set the workspace ID to string, playbook ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, data class ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, and rule to Enabled.

```
{
  "description" : "This my XXXX",
  "workspace_id" : "string",
  "playbook_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "actions" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "description" : "This my XXXX",
    "action_type" : "Workflow",
    "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "string",
    "playbook_version_id" : "string",
    "project_id" : "string"
  } ],
  "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "rule_enable" : true,
  "rule_id" : "4185bbd2-9d18-4362-92cb-46df0b24fe4e",
  "trigger_type" : "event",
  "dataobject_create" : true,
  "dataobject_update" : true,
  "dataobject_delete" : true,
  "action_strategy" : "sync"
}
```

Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "modifier_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "enabled" : true,
    "status" : "editing",
    "action_strategy" : "sync",
    "actions" : [ {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
```



```
    "description" : "This my XXXX",
    "action_type" : "Workflow",
    "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "string",
    "playbook_version_id" : "string",
    "project_id" : "string"
  } ],
  "rule_enable" : true,
  "rules" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "rule" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  },
  "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "trigger_type" : "event",
  "dataobject_create" : true,
  "dataobject_update" : true,
  "dataobject_delete" : true,
  "version_type" : 1,
  "rule_id" : "string",
  "dataclass_name" : "string",
  "approve_name" : "string"
 }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Create a playbook version. Set the workspace ID to string, playbook ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, data class ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, and rule to 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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class CreatePlaybookVersionSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
```



```
            .withCredential(auth)
            .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
            .build();
        CreatePlaybookVersionRequest request = new CreatePlaybookVersionRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withPlaybookId("{playbook_id}");
        CreatePlaybookVersionInfo body = new CreatePlaybookVersionInfo();
        List<ActionInfo> listbodyActions = new ArrayList<>();
        listbodyActions.add(
            new ActionInfo()
                .withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withName("MyXXX")
                .withDescription("This my XXXX")
                .withActionType("Workflow")
                .withActionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withPlaybookId("string")
                .withPlaybookVersionId("string")
                .withProjectId("string")
        );
        body.withActionStrategy("sync");
        body.withDataobjectDelete(true);
        body.withDataobjectUpdate(true);
        body.withDataobjectCreate(true);
        body.withTriggerType("event");
        body.withRuleId("4185bbd2-9d18-4362-92cb-46df0b24fe4e");
        body.withRuleEnable(true);
        body.withDataclassId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withActions(listbodyActions);
        body.withPlaybookId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withWorkspaceId("string");
        body.withDescription("This my XXXX");
        request.withBody(body);
        try {
            CreatePlaybookVersionResponse response = client.createPlaybookVersion(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 playbook version. Set the workspace ID to string, playbook ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, data class ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, and rule to Enabled.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreatePlaybookVersionRequest()
        request.workspace_id = "{workspace_id}"
        request.playbook_id = "{playbook_id}"
        listActionsbody = [
            ActionInfo(
                id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
                name="MyXXX",
                description="This my XXXX",
                action_type="Workflow",
                action_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
                playbook_id="string",
                playbook_version_id="string",
                project_id="string"
            )
        ]
        request.body = CreatePlaybookVersionInfo(
            action_strategy="sync",
            dataobject_delete=True,
            dataobject_update=True,
            dataobject_create=True,
            trigger_type="event",
            rule_id="4185bbd2-9d18-4362-92cb-46df0b24fe4e",
            rule_enable=True,
            dataclass_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            actions=listActionsbody,
            playbook_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            workspace_id="string",
            description="This my XXXX"
        )
        response = client.create_playbook_version(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 playbook version. Set the workspace ID to string, playbook ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, data class ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, and rule to Enabled.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePlaybookVersionRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.PlaybookId = "{playbook_id}"
    idActions:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    nameActions:= "MyXXX"
    descriptionActions:= "This my XXXX"
    actionTypeActions:= "Workflow"
    actionIdActions:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    playbookIdActions:= "string"
    playbookVersionIdActions:= "string"
    projectIdActions:= "string"
    var listActionsbody = []model.ActionInfo{
        {
            Id: &idActions,
            Name: &nameActions,
            Description: &descriptionActions,
            ActionType: &actionTypeActions,
            ActionId: &actionIdActions,
            PlaybookId: &playbookIdActions,
            PlaybookVersionId: &playbookVersionIdActions,
            ProjectId: &projectIdActions,
        },
    }
    actionStrategyCreatePlaybookVersionInfo:= "sync"
    dataobjectDeleteCreatePlaybookVersionInfo:= true
    dataobjectUpdateCreatePlaybookVersionInfo:= true
    dataobjectCreateCreatePlaybookVersionInfo:= true
    triggerTypeCreatePlaybookVersionInfo:= "event"
    ruleIdCreatePlaybookVersionInfo:= "4185bbd2-9d18-4362-92cb-46df0b24fe4e"
    ruleEnableCreatePlaybookVersionInfo:= true
    dataclassIdCreatePlaybookVersionInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    playbookIdCreatePlaybookVersionInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    workspaceIdCreatePlaybookVersionInfo:= "string"
    descriptionCreatePlaybookVersionInfo:= "This my XXXX"
    request.Body = &model.CreatePlaybookVersionInfo{
        ActionStrategy: &actionStrategyCreatePlaybookVersionInfo,
        DataobjectDelete: &dataobjectDeleteCreatePlaybookVersionInfo,
        DataobjectUpdate: &dataobjectUpdateCreatePlaybookVersionInfo,
        DataobjectCreate: &dataobjectCreateCreatePlaybookVersionInfo,
        TriggerType: &triggerTypeCreatePlaybookVersionInfo,
        RuleId: &ruleIdCreatePlaybookVersionInfo,
        RuleEnable: &ruleEnableCreatePlaybookVersionInfo,
        DataclassId: &dataclassIdCreatePlaybookVersionInfo,
        Actions: &listActionsbody,
        PlaybookId: &playbookIdCreatePlaybookVersionInfo,
        WorkspaceId: &workspaceIdCreatePlaybookVersionInfo,
        Description: &descriptionCreatePlaybookVersionInfo,
    }
    response, err := client.CreatePlaybookVersion(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.6.4 Querying Playbook Version Details

Function

Show playbook version version

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}

Table 4-499 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
version_id	Yes	String	Playbook version ID.

Request Parameters

Table 4-500 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-501 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-502 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message
data	**PlaybookVersionInfo** object	Playbook version details.

Table 4-503 PlaybookVersionInfo

Parameter	Type	Description
id	String	Playbook version ID.
description	String	Description.
create_time	String	Creation time.
update_time	String	Update time.

Parameter	Type	Description
project_id	String	Project ID.
creator_id	String	Creator ID.
modifier_id	String	ID of the editor.
playbook_id	String	Playbook ID.
version	String	Version No.
enabled	Boolean	Enable or not. **true**: Enabled **false**: Disabled
status	String	Playbook version status. Options: **Editing**, **APPROVING**, **UNPASSED**, and **PUBLISHED**
action_strategy	String	Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is **ASYNC**.
actions	Array of **ActionInfo** objects	The list of workflows associated with the playbook.
rule_enable	Boolean	Whether to enable the trigger condition filter.
rules	**RuleInfo** object	Playbook trigger information.
dataclass_id	String	Data class ID.
trigger_type	String	How the playbook is triggered. Options: **EVENT** and **TIMER**
dataobject_create	Boolean	Whether to trigger a playbook when a data object is created.
dataobject_update	Boolean	Whether to trigger a playbook when a data object is updated.
dataobject_delete	Boolean	Whether to trigger a playbook when a data object is deleted.
version_type	Integer	Version type (**0**: Draft; **1**: Released).
rule_id	String	Filter rule ID.
dataclass_name	String	Data class name.
approve_name	String	Reviewer.

Table 4-504 ActionInfo

Parameter	Type	Description
id	String	Playbook workflow ID.
name	String	Workflow name.
description	String	Description.
action_type	String	Workflow type.
action_id	String	Workflow ID.
playbook_id	String	Playbook ID.
playbook_version_id	String	Playbook version ID.
project_id	String	Project ID.

Table 4-505 RuleInfo

Parameter	Type	Description
id	String	Rule ID.
project_id	String	Project ID.
rule	String	Trigger rules.

Status code: 400

Table 4-506 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-507 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response to a successful request.


```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "modifier_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "enabled" : true,
    "status" : "editing",
    "action_strategy" : "sync",
    "actions" : [ {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "description" : "This my XXXX",
      "action_type" : "Workflow",
      "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "playbook_id" : "string",
      "playbook_version_id" : "string",
      "project_id" : "string"
    } ],
    "rule_enable" : true,
    "rules" : {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "rule" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "trigger_type" : "event",
    "dataobject_create" : true,
    "dataobject_update" : true,
    "dataobject_delete" : true,
    "version_type" : 1,
    "rule_id" : "string",
    "dataclass_name" : "string",
    "approve_name" : "string"
  }
}
```


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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowPlaybookVersionSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookVersionRequest request = new ShowPlaybookVersionRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withVersionId("{version_id}");
        try {
            ShowPlaybookVersionResponse response = client.showPlaybookVersion(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowPlaybookVersionRequest()
        request.workspace_id = "{workspace_id}"
        request.version_id = "{version_id}"
        response = client.show_playbook_version(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowPlaybookVersionRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.VersionId = "{version_id}"
    response, err := client.ShowPlaybookVersion(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.6.5 Deleting a Playbook Version

Function

This API is used to delete a playbook version.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}

Table 4-508 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
version_id	Yes	String	Playbook version ID.

Request Parameters

Table 4-509 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-510 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-511 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Response message.

Status code: 400

Table 4-512 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-513 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : 0,
  "message" : "Error message"
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class DeletePlaybookVersionSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
```



```
        DeletePlaybookVersionRequest request = new DeletePlaybookVersionRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withVersionId("{version_id}");
        try {
            DeletePlaybookVersionResponse response = client.deletePlaybookVersion(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeletePlaybookVersionRequest()
        request.workspace_id = "{workspace_id}"
        request.version_id = "{version_id}"
        response = client.delete_playbook_version(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeletePlaybookVersionRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.VersionId = "{version_id}"
    response, err := client.DeletePlaybookVersion(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.6.6 Updating a Playbook Version

Function

This API is used to update a playbook version.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}

Table 4-514 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
version_id	Yes	String	Playbook version ID.

Request Parameters

Table 4-515 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-516 Request body parameters

Parameter	Mandatory	Type	Description
description	No	String	Description.
workspace_id	No	String	Workspace ID.
playbook_id	No	String	Playbook ID.
dataclass_id	No	String	Data class ID.
rule_enable	No	Boolean	Whether to enable the trigger condition filter.

Parameter	Mandatory	Type	Description
enabled	No	Boolean	Whether to activate. (**false**: Not activated; **true**: Activated)
status	No	String	Status (**APPROVING**: Being reviewed; **EDITING**: Being edited; **UNPASSED**: Rejected; **Published**: Released)
rule_id	No	String	Rule ID.
trigger_type	No	String	Trigger method. **EVENT**: Triggered by incidents; **TIMER**: Triggered as scheduled.
dataobject_create	No	Boolean	Whether to trigger a playbook when a data object is created.
dataobject_update	No	Boolean	Whether to trigger a playbook when a data object is updated.
dataobject_delete	No	Boolean	Whether to trigger a playbook when a data object is deleted.
action_strategy	No	String	Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is **ASYNC**.

Response Parameters

Status code: 200

Table 4-517 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-518 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message
data	**PlaybookVersionInfo** object	Playbook version details.

Table 4-519 PlaybookVersionInfo

Parameter	Type	Description
id	String	Playbook version ID.
description	String	Description.
create_time	String	Creation time.
update_time	String	Update time.
project_id	String	Project ID.
creator_id	String	Creator ID.
modifier_id	String	ID of the editor.
playbook_id	String	Playbook ID.
version	String	Version No.
enabled	Boolean	Enable or not. **true**: Enabled **false**: Disabled
status	String	Playbook version status. Options: **Editing**, **APPROVING**, **UNPASSED**, and **PUBLISHED**
action_strategy	String	Execution policy. Currently, only asynchronous concurrent execution is supported. The corresponding value is **ASYNC**.
actions	Array of **ActionInfo** objects	The list of workflows associated with the playbook.
rule_enable	Boolean	Whether to enable the trigger condition filter.
rules	**RuleInfo** object	Playbook trigger information.
dataclass_id	String	Data class ID.
trigger_type	String	How the playbook is triggered. Options: **EVENT** and **TIMER**
dataobject_create	Boolean	Whether to trigger a playbook when a data object is created.
dataobject_update	Boolean	Whether to trigger a playbook when a data object is updated.
dataobject_delete	Boolean	Whether to trigger a playbook when a data object is deleted.
version_type	Integer	Version type (**0**: Draft; **1**: Released).

Parameter	Type	Description
rule_id	String	Filter rule ID.
dataclass_name	String	Data class name.
approve_name	String	Reviewer.

Table 4-520 ActionInfo

Parameter	Type	Description
id	String	Playbook workflow ID.
name	String	Workflow name.
description	String	Description.
action_type	String	Workflow type.
action_id	String	Workflow ID.
playbook_id	String	Playbook ID.
playbook_version_id	String	Playbook version ID.
project_id	String	Project ID.

Table 4-521 RuleInfo

Parameter	Type	Description
id	String	Rule ID.
project_id	String	Project ID.
rule	String	Trigger rules.

Status code: 400

Table 4-522 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-523 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Update a playbook version. Set the workspace ID to string, playbook ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, data class ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, and playbook rule to Enabled.

```
{
  "description" : "This my XXXX",
  "workspace_id" : "string",
  "playbook_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "rule_enable" : true,
  "enabled" : true,
  "status" : "UNPASSED",
  "rule_id" : "4185bbd2-9d18-4362-92cb-46df0b24fe4e",
  "trigger_type" : "event",
  "dataobject_create" : true,
  "dataobject_update" : true,
  "dataobject_delete" : true,
  "action_strategy" : "sync"
}
```

Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "description" : "This my XXXX",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "modifier_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1",
    "enabled" : true,
    "status" : "editing",
    "action_strategy" : "sync",
    "actions" : [ {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "description" : "This my XXXX",
      "action_type" : "Workflow",
      "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "playbook_id" : "string",
      "playbook_version_id" : "string",
      "project_id" : "string"
    } ],
    "rule_enable" : true,
```



```
  "rules" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "rule" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  },
  "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "trigger_type" : "event",
  "dataobject_create" : true,
  "dataobject_update" : true,
  "dataobject_delete" : true,
  "version_type" : 1,
  "rule_id" : "string",
  "dataclass_name" : "string",
  "approve_name" : "string"
 }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Update a playbook version. Set the workspace ID to string, playbook ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, data class ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, and playbook rule to 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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class UpdatePlaybookVersionSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdatePlaybookVersionRequest request = new UpdatePlaybookVersionRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withVersionId("{version_id}");
        ModifyPlaybookVersionInfo body = new ModifyPlaybookVersionInfo();
        body.withActionStrategy("sync");
        body.withDataobjectDelete(true);
        body.withDataobjectUpdate(true);
```



```
        body.withDataobjectCreate(true);
        body.withTriggerType("event");
        body.withRuleId("4185bbd2-9d18-4362-92cb-46df0b24fe4e");
        body.withStatus("UNPASSED");
        body.withEnabled(true);
        body.withRuleEnable(true);
        body.withDataclassId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withPlaybookId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withWorkspaceId("string");
        body.withDescription("This my XXXX");
        request.withBody(body);
        try {
            UpdatePlaybookVersionResponse response = client.updatePlaybookVersion(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 playbook version. Set the workspace ID to string, playbook ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, data class ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, and playbook rule to Enabled.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdatePlaybookVersionRequest()
        request.workspace_id = "{workspace_id}"
        request.version_id = "{version_id}"
        request.body = ModifyPlaybookVersionInfo(
            action_strategy="sync",
            dataobject_delete=True,
            dataobject_update=True,
            dataobject_create=True,
```



```
            trigger_type="event",
            rule_id="4185bbd2-9d18-4362-92cb-46df0b24fe4e",
            status="UNPASSED",
            enabled=True,
            rule_enable=True,
            dataclass_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            playbook_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            workspace_id="string",
            description="This my XXXX"
        )
        response = client.update_playbook_version(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 playbook version. Set the workspace ID to string, playbook ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, data class ID to 909494e3-558e-46b6-a9eb-07a8e18ca62f, and playbook rule to Enabled.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdatePlaybookVersionRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.VersionId = "{version_id}"
    actionStrategyModifyPlaybookVersionInfo:= "sync"
    dataobjectDeleteModifyPlaybookVersionInfo:= true
    dataobjectUpdateModifyPlaybookVersionInfo:= true
    dataobjectCreateModifyPlaybookVersionInfo:= true
    triggerTypeModifyPlaybookVersionInfo:= "event"
    ruleIdModifyPlaybookVersionInfo:= "4185bbd2-9d18-4362-92cb-46df0b24fe4e"
    statusModifyPlaybookVersionInfo:= "UNPASSED"
    enabledModifyPlaybookVersionInfo:= true
    ruleEnableModifyPlaybookVersionInfo:= true
```



```
    dataclassIdModifyPlaybookVersionInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    playbookIdModifyPlaybookVersionInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    workspaceIdModifyPlaybookVersionInfo:= "string"
    descriptionModifyPlaybookVersionInfo:= "This my XXXX"
    request.Body = &model.ModifyPlaybookVersionInfo{
        ActionStrategy: &actionStrategyModifyPlaybookVersionInfo,
        DataobjectDelete: &dataobjectDeleteModifyPlaybookVersionInfo,
        DataobjectUpdate: &dataobjectUpdateModifyPlaybookVersionInfo,
        DataobjectCreate: &dataobjectCreateModifyPlaybookVersionInfo,
        TriggerType: &triggerTypeModifyPlaybookVersionInfo,
        RuleId: &ruleIdModifyPlaybookVersionInfo,
        Status: &statusModifyPlaybookVersionInfo,
        Enabled: &enabledModifyPlaybookVersionInfo,
        RuleEnable: &ruleEnableModifyPlaybookVersionInfo,
        DataclassId: &dataclassIdModifyPlaybookVersionInfo,
        PlaybookId: &playbookIdModifyPlaybookVersionInfo,
        WorkspaceId: &workspaceIdModifyPlaybookVersionInfo,
        Description: &descriptionModifyPlaybookVersionInfo,
    }
    response, err := client.UpdatePlaybookVersion(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.7 Playbook Rule Management

4.7.1 Querying Playbook Rule Details

Function

This API is used to query details about a playbook rule.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/rules/{rule_id}

Table 4-524 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
version_id	Yes	String	version Id value
rule_id	Yes	String	version Id value

Request Parameters

Table 4-525 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-526 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-527 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**RuleInfo** object	Playbook trigger information.

Table 4-528 RuleInfo

Parameter	Type	Description
id	String	Rule ID.
project_id	String	Project ID.
rule	String	Trigger rules.

Status code: 400

Table 4-529 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-530 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : 0,
  "message" : "Error message",
```



```
 "data" : {
   "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
   "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
   "rule" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
 }
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowPlaybookRuleSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookRuleRequest request = new ShowPlaybookRuleRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withVersionId("{version_id}");
        request.withRuleId("{rule_id}");
        try {
            ShowPlaybookRuleResponse response = client.showPlaybookRule(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowPlaybookRuleRequest()
        request.workspace_id = "{workspace_id}"
        request.version_id = "{version_id}"
        request.rule_id = "{rule_id}"
        response = client.show_playbook_rule(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
```



```
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowPlaybookRuleRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.VersionId = "{version_id}"
    request.RuleId = "{rule_id}"
    response, err := client.ShowPlaybookRule(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.7.2 Deleting a Playbook Rule

Function

This API is used to delete a playbook rule.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/rules/{rule_id}

Table 4-531 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
version_id	Yes	String	Playbook version ID.
rule_id	Yes	String	Rule ID.

Request Parameters

Table 4-532 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-533 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-534 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Response message.

Status code: 400

Table 4-535 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-536 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : 0,
  "message" : "Error message"
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class DeletePlaybookRuleSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeletePlaybookRuleRequest request = new DeletePlaybookRuleRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withVersionId("{version_id}");
        request.withRuleId("{rule_id}");
        try {
            DeletePlaybookRuleResponse response = client.deletePlaybookRule(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeletePlaybookRuleRequest()
        request.workspace_id = "{workspace_id}"
        request.version_id = "{version_id}"
        request.rule_id = "{rule_id}"
        response = client.delete_playbook_rule(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeletePlaybookRuleRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.VersionId = "{version_id}"
    request.RuleId = "{rule_id}"
    response, err := client.DeletePlaybookRule(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.7.3 Creating a Playbook Rule

Function

This API is used to create a playbook rule.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/rules

Table 4-537 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
version_id	Yes	String	Playbook version ID.

Request Parameters

Table 4-538 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-539 Request body parameters

Parameter	Mandatory	Type	Description
rule	Yes	**ConditionInfo** object	Details about playbook triggering rules.

Table 4-540 ConditionInfo

Parameter	Mandatory	Type	Description
expression_type	No	String	Expression type. The default value is **common**. This parameter is mandatory for event-triggered playbooks.
conditions	No	Array of **ConditionItem** objects	Trigger condition. This parameter is mandatory for event-triggered playbooks.
logics	No	Array of strings	Condition logic combination. This parameter is mandatory for event-triggered playbooks.
cron	No	String	Cron expression (scheduled task). This parameter is mandatory for timer-triggered playbooks.
schedule_type	No	String	Scheduled repetition type (second; hour; day; week). This parameter is mandatory for timer-triggered playbooks.
start_type	No	String	Playbook execution start type. **IMMEDIATELY**: The playbook is executed immediately after being created. **CUSTOM**: The playbook is executed at the time you specify for it. This parameter is mandatory for timer-triggered playbooks.
end_type	No	String	Playbook execution end type. **FOREVER**: The playbook will be executed permanently. **CUSTOM**: The playbook will end at the time you specify for it. This parameter is mandatory for timer-triggered playbooks.

Parameter	Mandatory	Type	Description
end_time	No	String	End time of a scheduled task. This parameter is mandatory for timer-triggered playbooks.
repeat_range	No	String	Execution time: 2021-01-30T23:00:00Z+0800. This parameter is mandatory for timer-triggered playbooks.
only_once	No	Boolean	Whether to execute it only once. This parameter is mandatory for timer-triggered playbooks.
execution_type	No	String	Execution queue type. **PARALLEL**: The new task is executed concurrently with the previous task. This parameter is mandatory for timer-triggered playbooks.

Table 4-541 ConditionItem

Parameter	Mandatory	Type	Description
name	No	String	Condition name.
detail	No	String	Condition details.
data	No	Array of strings	Condition expression data.

Response Parameters

Status code: 200

Table 4-542 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-543 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**RuleInfo** object	Playbook trigger information.

Table 4-544 RuleInfo

Parameter	Type	Description
id	String	Rule ID.
project_id	String	Project ID.
rule	String	Trigger rules.

Status code: 400

Table 4-545 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-546 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Create a playbook rule named **condition_0** and set the expression type to all.

```
{
  "rule" : {
    "expression_type" : "common",
    "conditions" : [ {
      "name" : "condition_0",
      "detail" : "123",
      "data" : [ "handle_status, ==, Open" ]
    } ],
    "logics" : [ "condition_0" ]
  }
}
```


Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : 0,
  "message" : "",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "rule" : "{\"expression_type\":\"common\",\"conditions\":[{\"name\":\"condition_0\",\"data\":
[\"ref_order_id\",\"==\",\"123\"],\"detail\":\"123\"}],\"logics\":[\"condition_0\"]}"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Create a playbook rule named **condition_0** and set the expression type to all.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class CreatePlaybookRuleSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePlaybookRuleRequest request = new CreatePlaybookRuleRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withVersionId("{version_id}");
        CreateRuleInfo body = new CreateRuleInfo();
        List<String> listRuleLogics = new ArrayList<>();
        listRuleLogics.add("condition_0");
        List<String> listConditionsData = new ArrayList<>();
```



```
        listConditionsData.add("handle_status, ==, Open");
        List<ConditionItem> listRuleConditions = new ArrayList<>();
        listRuleConditions.add(
            new ConditionItem()
                .withName("condition_0")
                .withDetail("123")
                .withData(listConditionsData)
        );
        ConditionInfo rulebody = new ConditionInfo();
        rulebody.withExpressionType("common")
            .withConditions(listRuleConditions)
            .withLogics(listRuleLogics);
        body.withRule(rulebody);
        request.withBody(body);
        try {
            CreatePlaybookRuleResponse response = client.createPlaybookRule(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 playbook rule named **condition_0** and set the expression type to all.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreatePlaybookRuleRequest()
        request.workspace_id = "{workspace_id}"
        request.version_id = "{version_id}"
        listLogicsRule = [
            "condition_0"
        ]
        listDataConditions = [
            "handle_status, ==, Open"
```



```
        ]
        listConditionsRule = [
            ConditionItem(
                name="condition_0",
                detail="123",
                data=listDataConditions
            )
        ]
        rulebody = ConditionInfo(
            expression_type="common",
            conditions=listConditionsRule,
            logics=listLogicsRule
        )
        request.body = CreateRuleInfo(
            rule=rulebody
        )
        response = client.create_playbook_rule(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 playbook rule named **condition_0** and set the expression type to all.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePlaybookRuleRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.VersionId = "{version_id}"
    var listLogicsRule = []string{
        "condition_0",
    }
    var listDataConditions = []string{
        "handle_status, ==, Open",
    }
```



```
    nameConditions:= "condition_0"
    detailConditions:= "123"
    var listConditionsRule = []model.ConditionItem{
        {
            Name: &nameConditions,
            Detail: &detailConditions,
            Data: &listDataConditions,
        },
    }
    expressionTypeRule:= "common"
    rulebody := &model.ConditionInfo{
        ExpressionType: &expressionTypeRule,
        Conditions: &listConditionsRule,
        Logics: &listLogicsRule,
    }
    request.Body = &model.CreateRuleInfo{
        Rule: rulebody,
    }
    response, err := client.CreatePlaybookRule(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.7.4 Updating a Playbook Rule

Function

This API is used to update a playbook rule.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/rules/{rule_id}

Table 4-547 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
version_id	Yes	String	Playbook version ID.
rule_id	Yes	String	Playbook rule ID.

Request Parameters

Table 4-548 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-549 Request body parameters

Parameter	Mandatory	Type	Description
rule	No	**ConditionInfo** object	Details about playbook triggering rules.

Table 4-550 ConditionInfo

Parameter	Mandatory	Type	Description
expression_type	No	String	Expression type. The default value is **common**. This parameter is mandatory for event-triggered playbooks.
conditions	No	Array of **ConditionItem** objects	Trigger condition. This parameter is mandatory for event-triggered playbooks.

Parameter	Mandatory	Type	Description
logics	No	Array of strings	Condition logic combination. This parameter is mandatory for event-triggered playbooks.
cron	No	String	Cron expression (scheduled task). This parameter is mandatory for timer-triggered playbooks.
schedule_type	No	String	Scheduled repetition type (second; hour; day; week). This parameter is mandatory for timer-triggered playbooks.
start_type	No	String	Playbook execution start type. **IMMEDIATELY**: The playbook is executed immediately after being created. **CUSTOM**: The playbook is executed at the time you specify for it. This parameter is mandatory for timer-triggered playbooks.
end_type	No	String	Playbook execution end type. **FOREVER**: The playbook will be executed permanently. **CUSTOM**: The playbook will end at the time you specify for it. This parameter is mandatory for timer-triggered playbooks.
end_time	No	String	End time of a scheduled task. This parameter is mandatory for timer-triggered playbooks.
repeat_range	No	String	Execution time: 2021-01-30T23:00:00Z+0800. This parameter is mandatory for timer-triggered playbooks.
only_once	No	Boolean	Whether to execute it only once. This parameter is mandatory for timer-triggered playbooks.
execution_type	No	String	Execution queue type. **PARALLEL**: The new task is executed concurrently with the previous task. This parameter is mandatory for timer-triggered playbooks.

Table 4-551 ConditionItem

Parameter	Mandatory	Type	Description
name	No	String	Condition name.
detail	No	String	Condition details.
data	No	Array of strings	Condition expression data.

Response Parameters

Status code: 200

Table 4-552 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-553 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**RuleInfo** object	Playbook trigger information.

Table 4-554 RuleInfo

Parameter	Type	Description
id	String	Rule ID.
project_id	String	Project ID.
rule	String	Trigger rules.

Status code: 400

Table 4-555 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-556 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Update a playbook rule named **condition_0** and set the expression type to all.

```
{
  "rule" : {
    "expression_type" : "common",
    "conditions" : [ {
      "name" : "condition_0",
      "detail" : "123",
      "data" : [ "handle_status, ==, Open" ]
    } ],
    "logics" : [ "condition_0" ]
  }
}
```

Example Responses

Status code: 200

Response parameters for a successful request.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "rule" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Update a playbook rule named **condition_0** and set the expression type to all.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class UpdatePlaybookRuleSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdatePlaybookRuleRequest request = new UpdatePlaybookRuleRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withVersionId("{version_id}");
        request.withRuleId("{rule_id}");
        ModifyRuleInfo body = new ModifyRuleInfo();
        List<String> listRuleLogics = new ArrayList<>();
        listRuleLogics.add("condition_0");
        List<String> listConditionsData = new ArrayList<>();
        listConditionsData.add("handle_status, ==, Open");
        List<ConditionItem> listRuleConditions = new ArrayList<>();
        listRuleConditions.add(
            new ConditionItem()
                .withName("condition_0")
                .withDetail("123")
                .withData(listConditionsData)
        );
        ConditionInfo rulebody = new ConditionInfo();
        rulebody.withExpressionType("common")
            .withConditions(listRuleConditions)
            .withLogics(listRuleLogics);
        body.withRule(rulebody);
        request.withBody(body);
        try {
            UpdatePlaybookRuleResponse response = client.updatePlaybookRule(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 playbook rule named **condition_0** and set the expression type to all.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdatePlaybookRuleRequest()
        request.workspace_id = "{workspace_id}"
        request.version_id = "{version_id}"
        request.rule_id = "{rule_id}"
        listLogicsRule = [
            "condition_0"
        ]
        listDataConditions = [
            "handle_status, ==, Open"
        ]
        listConditionsRule = [
            ConditionItem(
                name="condition_0",
                detail="123",
                data=listDataConditions
            )
        ]
        rulebody = ConditionInfo(
            expression_type="common",
            conditions=listConditionsRule,
            logics=listLogicsRule
        )
        request.body = ModifyRuleInfo(
            rule=rulebody
        )
        response = client.update_playbook_rule(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 playbook rule named **condition_0** and set the expression type to all.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdatePlaybookRuleRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.VersionId = "{version_id}"
    request.RuleId = "{rule_id}"
    var listLogicsRule = []string{
        "condition_0",
    }
    var listDataConditions = []string{
        "handle_status, ==, Open",
    }
    nameConditions:= "condition_0"
    detailConditions:= "123"
    var listConditionsRule = []model.ConditionItem{
        {
            Name: &nameConditions,
            Detail: &detailConditions,
            Data: &listDataConditions,
        },
    }
    expressionTypeRule:= "common"
    rulebody := &model.ConditionInfo{
        ExpressionType: &expressionTypeRule,
        Conditions: &listConditionsRule,
        Logics: &listLogicsRule,
    }
    request.Body = &model.ModifyRuleInfo{
        Rule: rulebody,
    }
    response, err := client.UpdatePlaybookRule(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	Response parameters for a successful request.
400	Response parameters for failed requests.

Error Codes

See **Error Codes**.

4.8 Playbook Instance Management

4.8.1 Querying the Playbook Instance List

Function

This API is used to query the playbook instance list.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances

Table 4-557 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Table 4-558 Query Parameters

Parameter	Mandatory	Type	Description
status	No	String	Playbook instance status. (**RUNNING**: Running; **FINISHED**: Successful; **FAILED**: Failed; **RETRYING**: Retrying; **TERMINATING**: Terminating; **TERMINATED**: Terminated)
name	No	String	Instance name.
playbook_name	No	String	Playbook name.
dataclass_name	No	String	Data class name.
dataobject_name	No	String	Data object name.
trigger_type	No	String	Trigger type. **TIMER**: The playbook is triggered at a scheduled time; **EVENT**: The playbook is triggered by an event.
from_date	No	String	Start time for the query.
to_date	No	String	End time for the query.
limit	Yes	Integer	The maximum number of records can be returned on each page for a pagination query. The value starts from 1.
offset	Yes	Integer	Pagination query parameter. This parameter specifies the start position of the query result. The value starts from **0**.

Request Parameters

Table 4-559 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-560 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-561 Response body parameters

Parameter	Type	Description
count	Integer	Total number.
instances	Array of **PlaybookInstanceInfo** objects	Playbook instance list information.

Table 4-562 PlaybookInstanceInfo

Parameter	Type	Description
id	String	Playbook instance ID.
name	String	Playbook instance name.
project_id	String	Project ID.
playbook	**PlaybookInfoRef** object	Playbook information.

Parameter	Type	Description
dataclass	DataclassInfoRef object	Data class information.
dataobject	DataobjectInfo object	Data object details.
status	String	Playbook instance status. (**RUNNING**: Running; **FINISHED**: Successful; **FAILED**: Failed; **RETRYING**: Retrying; **TERMINATING**: Terminating; **TERMINATED**: Terminated)
trigger_type	String	Trigger type. **TIMER**: The playbook is triggered at a scheduled time; **EVENT**: The playbook is triggered by an event.
start_time	String	Creation time.
end_time	String	Update time.

Table 4-563 PlaybookInfoRef

Parameter	Type	Description
id	String	Playbook ID.
version_id	String	Playbook version ID.
name	String	Name.
version	String	Version.

Table 4-564 DataclassInfoRef

Parameter	Type	Description
id	String	Data class ID.
name	String	Data class name.

Table 4-565 DataobjectInfo

Parameter	Type	Description
id	String	ID.
create_time	String	Creation time.
update_time	String	Update time.

Parameter	Type	Description
project_id	String	Project ID.
dataclass_id	String	Data class ID.
name	String	Name.
content	String	Data content.

Status code: 400

Table 4-566 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-567 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response to a successful request.


```
{
  "count" : 41,
  "instances" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook" : {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "version" : "v1.1.1"
    },
    "dataclass" : {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    },
    "dataobject" : {
```



```
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  },
  "status" : "TERMINATED",
  "trigger_type" : "string",
  "start_time" : "2021-01-30T23:00:00Z+0800",
  "end_time" : "2021-01-30T23:00:00Z+0800"
 } ]
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListPlaybookInstancesSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybookInstancesRequest request = new ListPlaybookInstancesRequest();
        request.withWorkspaceId("{workspace_id}");
        try {
            ListPlaybookInstancesResponse response = client.listPlaybookInstances(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListPlaybookInstancesRequest()
        request.workspace_id = "{workspace_id}"
        response = client.list_playbook_instances(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
```



```
        WithCredential(auth).
        Build())

    request := &model.ListPlaybookInstancesRequest{}
    request.WorkspaceId = "{workspace_id}"
    response, err := client.ListPlaybookInstances(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.8.2 Querying Details About a Playbook Instance

Function

Show playbook instance

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}

Table 4-568 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Parameter	Mandatory	Type	Description
instance_id	Yes	String	instance _id

Request Parameters

Table 4-569 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.
content-type	Yes	String	application/ json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-570 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-571 Response body parameters

Parameter	Type	Description
id	String	Playbook instance ID.
name	String	Playbook instance name.
project_id	String	Project ID.
playbook	**PlaybookInfoRef** object	Playbook information.
dataclass	**DataclassInfoRef** object	Data class information.

Parameter	Type	Description
dataobject	DataobjectInfo object	Data object details.
status	String	Playbook instance status. (**RUNNING**: Running; **FINISHED**: Successful; **FAILED**: Failed; **RETRYING**: Retrying; **TERMINATING**: Terminating; **TERMINATED**: Terminated)
trigger_type	String	Trigger type. **TIMER**: The playbook is triggered at a scheduled time; **EVENT**: The playbook is triggered by an event.
start_time	String	Creation time.
end_time	String	Update time.

Table 4-572 PlaybookInfoRef

Parameter	Type	Description
id	String	Playbook ID.
version_id	String	Playbook version ID.
name	String	Name.
version	String	Version.

Table 4-573 DataclassInfoRef

Parameter	Type	Description
id	String	Data class ID.
name	String	Data class name.

Table 4-574 DataobjectInfo

Parameter	Type	Description
id	String	ID.
create_time	String	Creation time.
update_time	String	Update time.
project_id	String	Project ID.

Parameter	Type	Description
dataclass_id	String	Data class ID.
name	String	Name.
content	String	Data content.

Status code: 400

Table 4-575 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-576 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Instance Informations

```
{
  "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "name" : "MyXXX",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "playbook" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1"
  },
  "dataclass" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  },
  "dataobject" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  },
  "status" : "TERMINATED",
```



```
  "trigger_type" : "string",
  "start_time" : "2021-01-30T23:00:00Z+0800",
  "end_time" : "2021-01-30T23:00:00Z+0800"
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowPlaybookInstanceSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookInstanceRequest request = new ShowPlaybookInstanceRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withInstanceId("{instance_id}");
        try {
            ShowPlaybookInstanceResponse response = client.showPlaybookInstance(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowPlaybookInstanceRequest()
        request.workspace_id = "{workspace_id}"
        request.instance_id = "{instance_id}"
        response = client.show_playbook_instance(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())
```



```
    request := &model.ShowPlaybookInstanceRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.InstanceId = "{instance_id}"
    response, err := client.ShowPlaybookInstance(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	Instance Informations
400	Error response

Error Codes

See **Error Codes**.

4.8.3 Operating a Playbook Instance

Function

Operating a Playbook Instance

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}/operation

Table 4-577 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
instance_id	Yes	String	Playbook instance ID.

Request Parameters

Table 4-578 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-579 Request body parameters

Parameter	Mandatory	Type	Description
operation	No	String	Operation type. **RETRY** or **TERMINATE**

Response Parameters

Status code: 200

Table 4-580 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-581 Response body parameters

Parameter	Type	Description
id	String	Playbook instance ID.
name	String	Playbook instance name.
project_id	String	Project ID.
playbook	**PlaybookInfoRef** object	Playbook information.
dataclass	**DataclassInfoRef** object	Data class information.

Parameter	Type	Description
dataobject	DataobjectInfo object	Data object details.
status	String	Playbook instance status. (**RUNNING**: Running; **FINISHED**: Successful; **FAILED**: Failed; **RETRYING**: Retrying; **TERMINATING**: Terminating; **TERMINATED**: Terminated)
trigger_type	String	Trigger type. **TIMER**: The playbook is triggered at a scheduled time; **EVENT**: The playbook is triggered by an event.
start_time	String	Creation time.
end_time	String	Update time.

Table 4-582 PlaybookInfoRef

Parameter	Type	Description
id	String	Playbook ID.
version_id	String	Playbook version ID.
name	String	Name.
version	String	Version.

Table 4-583 DataclassInfoRef

Parameter	Type	Description
id	String	Data class ID.
name	String	Data class name.

Table 4-584 DataobjectInfo

Parameter	Type	Description
id	String	ID.
create_time	String	Creation time.
update_time	String	Update time.
project_id	String	Project ID.

Parameter	Type	Description
dataclass_id	String	Data class ID.
name	String	Name.
content	String	Data content.

Status code: 400

Table 4-585 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-586 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Retrying Workflows of a Playbook Instance

```
{
  "operation" : "RETRY"
}
```

Example Responses

Status code: 200

Response to a successful request.

```
{
  "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "name" : "MyXXX",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "playbook" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "version" : "v1.1.1"
  },
  "dataclass" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  },
  "dataobject" : {
```



```
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  },
  "status" : "TERMINATED",
  "trigger_type" : "string",
  "start_time" : "2021-01-30T23:00:00Z+0800",
  "end_time" : "2021-01-30T23:00:00Z+0800"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Retrying Workflows of a Playbook Instance

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ChangePlaybookInstanceSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ChangePlaybookInstanceRequest request = new ChangePlaybookInstanceRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withInstanceId("{instance_id}");
        OperationPlaybookInfo body = new OperationPlaybookInfo();
        body.withOperation("RETRY");
        request.withBody(body);
        try {
            ChangePlaybookInstanceResponse response = client.changePlaybookInstance(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

Retrying Workflows of a Playbook Instance

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ChangePlaybookInstanceRequest()
        request.workspace_id = "{workspace_id}"
        request.instance_id = "{instance_id}"
        request.body = OperationPlaybookInfo(
            operation="RETRY"
        )
        response = client.change_playbook_instance(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

Retrying Workflows of a Playbook Instance

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ChangePlaybookInstanceRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.InstanceId = "{instance_id}"
    operationOperationPlaybookInfo:= "RETRY"
    request.Body = &model.OperationPlaybookInfo{
        Operation: &operationOperationPlaybookInfo,
    }
    response, err := client.ChangePlaybookInstance(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.8.4 Querying the Playbook Topology

Function

Querying the Playbook Topology

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}/topology

Table 4-587 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
instance_id	Yes	String	Playbook instance ID.

Request Parameters

Table 4-588 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-589 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-590 Response body parameters

Parameter	Type	Description
count	Integer	Total number.
action_instances	Array of **ActionInstanceInfo** objects	Workflow instance list.

Table 4-591 ActionInstanceInfo

Parameter	Type	Description
action	**ActionInfo** object	Playbook workflow information.
instance_log	**AuditLogInfo** object	Playbook instance review information.

Table 4-592 ActionInfo

Parameter	Type	Description
id	String	Playbook workflow ID.
name	String	Workflow name.
description	String	Description.
action_type	String	Workflow type.
action_id	String	Workflow ID.
playbook_id	String	Playbook ID.
playbook_version_id	String	Playbook version ID.
project_id	String	Project ID.

Table 4-593 AuditLogInfo

Parameter	Type	Description
instance_type	String	Instance type. **AOP_WORKFLOW** for workflows, **SCRIPT** for scripts, and **PLAYBOOK** for playbooks.
action_id	String	Workflow ID.
action_name	String	Workflow name.

Parameter	Type	Description
instance_id	String	Instance ID.
parent_instance_id	String	Instance ID of the parent node.
log_level	String	Log level.
input	String	Input.
output	String	Output.
error_msg	String	Error message.
start_time	String	Start time.
end_time	String	End time.
status	String	Status. (**RUNNING**: Running; **FINISHED**: Successful; **FAILED**: Failed; **RETRYING**: Retrying; **TERMINATING**: Terminating; **TERMINATED**: Terminated)
trigger_type	String	Trigger type. **TIMER**: The playbook is triggered at a scheduled time; **EVENT**: The playbook is triggered by an event.

Status code: 400

Table 4-594 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-595 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response to a successful request.

```
{
  "count" : 41,
  "action_instances" : [ {
    "action" : {
      "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "name" : "MyXXX",
      "description" : "This my XXXX",
      "action_type" : "Workflow",
      "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "playbook_id" : "string",
      "playbook_version_id" : "string",
      "project_id" : "string"
    },
    "instance_log" : {
      "instance_type" : "APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG",
      "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "action_name" : "DisabledIp",
      "instance_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "parent_instance_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
      "log_level" : "DEBUG INFO WARN",
      "input" : "input",
      "output" : "output",
      "error_msg" : "error_msg",
      "start_time" : "2021-01-30T23:00:00Z",
      "end_time" : "2021-01-31T23:00:00Z",
      "status" : "CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED",
      "trigger_type" : "DEBUG, TIMER, EVENT, MANUAL"
    }
  } ]
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowPlaybookTopologySolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookTopologyRequest request = new ShowPlaybookTopologyRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withInstanceId("{instance_id}");
        try {
            ShowPlaybookTopologyResponse response = client.showPlaybookTopology(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowPlaybookTopologyRequest()
        request.workspace_id = "{workspace_id}"
        request.instance_id = "{instance_id}"
        response = client.show_playbook_topology(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowPlaybookTopologyRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.InstanceId = "{instance_id}"
    response, err := client.ShowPlaybookTopology(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.8.5 Querying Review Logs of a Playbook Instance

Function

Querying Review Logs of a Playbook Instance

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/auditlogs

Table 4-596 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Table 4-597 Query Parameters

Parameter	Mandatory	Type	Description
offset	Yes	Long	offset
limit	Yes	Long	limit
sort_key	No	String	sort_key
sort_dir	No	String	sort_dir. asc, desc

Request Parameters

Table 4-598 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-599 Request body parameters

Parameter	Mandatory	Type	Description
instance_type	No	String	Instance type. **AOP_WORKFLOW** for workflows, **SCRIPT** for scripts, and **PLAYBOOK** for playbooks.
action_id	No	String	Workflow ID.
action_name	No	String	Workflow name.
instance_id	No	String	Instance ID.
parent_instance_id	No	String	Instance ID of the parent node.
log_level	No	String	Log level.
input	No	String	Input.
output	No	String	Output.
error_msg	No	String	Error message.
start_time	No	String	Start time.
end_time	No	String	End time.
status	No	String	Status. (**RUNNING**: Running; **FINISHED**: Successful; **FAILED**: Failed; **RETRYING**: Retrying; **TERMINATING**: Terminating; **TERMINATED**: Terminated)
trigger_type	No	String	Trigger type. **TIMER**: The playbook is triggered at a scheduled time; **EVENT**: The playbook is triggered by an event.

Response Parameters

Status code: 200

Table 4-600 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-601 Response body parameters

Parameter	Type	Description
count	Integer	Total records.
audit_logs	Array of **AuditLogInfo** objects	Audit log list.

Table 4-602 AuditLogInfo

Parameter	Type	Description
instance_type	String	Instance type. **AOP_WORKFLOW** for workflows, **SCRIPT** for scripts, and **PLAYBOOK** for playbooks.
action_id	String	Workflow ID.
action_name	String	Workflow name.
instance_id	String	Instance ID.
parent_instance_id	String	Instance ID of the parent node.
log_level	String	Log level.
input	String	Input.
output	String	Output.
error_msg	String	Error message.
start_time	String	Start time.
end_time	String	End time.
status	String	Status. (**RUNNING**: Running; **FINISHED**: Successful; **FAILED**: Failed; **RETRYING**: Retrying; **TERMINATING**: Terminating; **TERMINATED**: Terminated)
trigger_type	String	Trigger type. **TIMER**: The playbook is triggered at a scheduled time; **EVENT**: The playbook is triggered by an event.

Status code: 400

Table 4-603 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-604 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Query playbook instance review logs. Details: Instance type: APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG; Workflow ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Workflow name: DisabledIp; Instance ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Parent instance ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Log level: DEBUG, INFO WARN; Input: input; Output: output; Error message: error_msg. Start time: 2021-01-30 23:00:00 End time: 2021-01-31 23:00:00 Status: CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED Trigger type: DEBUG, TIMER, EVENT, or MANUAL.

```
{
  "instance_type" : "APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG",
  "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "action_name" : "DisabledIp",
  "instance_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "parent_instance_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "log_level" : "DEBUG INFO WARN",
  "input" : "input",
  "output" : "output",
  "error_msg" : "error_msg",
  "start_time" : "2021-01-30T23:00:00Z",
  "end_time" : "2021-01-31T23:00:00Z",
  "status" : "CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED",
  "trigger_type" : "DEBUG, TIMER, EVENT, MANUAL"
}
```

Example Responses

Status code: 200

Response to a successful request.

```
{
  "count" : 41,
  "audit_logs" : [ {
    "instance_type" : "APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG",
    "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "action_name" : "DisabledIp",
    "instance_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "parent_instance_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
```



```
    "log_level" : "DEBUG INFO WARN",
    "input" : "input",
    "output" : "output",
    "error_msg" : "error_msg",
    "start_time" : "2021-01-30T23:00:00Z",
    "end_time" : "2021-01-31T23:00:00Z",
    "status" : "CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED",
    "trigger_type" : "DEBUG, TIMER, EVENT, MANUAL"
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Query playbook instance review logs. Details: Instance type: APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG; Workflow ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Workflow name: DisabledIp; Instance ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Parent instance ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Log level: DEBUG, INFO WARN; Input: input; Output: output; Error message: error_msg. Start time: 2021-01-30 23:00:00 End time: 2021-01-31 23:00:00 Status: CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED Trigger type: DEBUG, TIMER, EVENT, or MANUAL.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListPlaybookAuditLogsSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybookAuditLogsRequest request = new ListPlaybookAuditLogsRequest();
        request.withWorkspaceId("{workspace_id}");
        AuditLogInfo body = new AuditLogInfo();
        body.withTriggerType("DEBUG, TIMER, EVENT, MANUAL");
        body.withStatus("CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED");
```



```
        body.withEndTime("2021-01-31T23:00:00Z");
        body.withStartTime("2021-01-30T23:00:00Z");
        body.withErrorMsg("error_msg");
        body.withOutput("output");
        body.withInput("input");
        body.withLogLevel("DEBUG INFO WARN");
        body.withParentInstanceId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withInstanceId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withActionName("DisabledIp");
        body.withActionId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withInstanceType("APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG");
        request.withBody(body);
        try {
            ListPlaybookAuditLogsResponse response = client.listPlaybookAuditLogs(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 playbook instance review logs. Details: Instance type: APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG; Workflow ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Workflow name: DisabledIp; Instance ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Parent instance ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Log level: DEBUG, INFO WARN; Input: input; Output: output; Error message: error_msg. Start time: 2021-01-30 23:00:00 End time: 2021-01-31 23:00:00 Status: CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED Trigger type: DEBUG, TIMER, EVENT, or MANUAL.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()
```



```
    try:
        request = ListPlaybookAuditLogsRequest()
        request.workspace_id = "{workspace_id}"
        request.body = AuditLogInfo(
            trigger_type="DEBUG, TIMER, EVENT, MANUAL",
            status="CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED",
            end_time="2021-01-31T23:00:00Z",
            start_time="2021-01-30T23:00:00Z",
            error_msg="error_msg",
            output="output",
            input="input",
            log_level="DEBUG INFO WARN",
            parent_instance_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            instance_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            action_name="DisabledIp",
            action_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            instance_type="APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG"
        )
        response = client.list_playbook_audit_logs(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 playbook instance review logs. Details: Instance type: APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG; Workflow ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Workflow name: DisabledIp; Instance ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Parent instance ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Log level: DEBUG, INFO WARN; Input: input; Output: output; Error message: error_msg. Start time: 2021-01-30 23:00:00 End time: 2021-01-31 23:00:00 Status: CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED Trigger type: DEBUG, TIMER, EVENT, or MANUAL.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
```



```
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

    request := &model.ListPlaybookAuditLogsRequest{}
    request.WorkspaceId = "{workspace_id}"
    triggerTypeAuditLogInfo:= "DEBUG, TIMER, EVENT, MANUAL"
    statusAuditLogInfo:= "CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED"
    endTimeAuditLogInfo:= "2021-01-31T23:00:00Z"
    startTimeAuditLogInfo:= "2021-01-30T23:00:00Z"
    errorMsgAuditLogInfo:= "error_msg"
    outputAuditLogInfo:= "output"
    inputAuditLogInfo:= "input"
    logLevelAuditLogInfo:= "DEBUG INFO WARN"
    parentInstanceIdAuditLogInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    instanceIdAuditLogInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    actionNameAuditLogInfo:= "DisabledIp"
    actionIdAuditLogInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    instanceTypeAuditLogInfo:= "APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG"
    request.Body = &model.AuditLogInfo{
        TriggerType: &triggerTypeAuditLogInfo,
        Status: &statusAuditLogInfo,
        EndTime: &endTimeAuditLogInfo,
        StartTime: &startTimeAuditLogInfo,
        ErrorMsg: &errorMsgAuditLogInfo,
        Output: &outputAuditLogInfo,
        Input: &inputAuditLogInfo,
        LogLevel: &logLevelAuditLogInfo,
        ParentInstanceId: &parentInstanceIdAuditLogInfo,
        InstanceId: &instanceIdAuditLogInfo,
        ActionName: &actionNameAuditLogInfo,
        ActionId: &actionIdAuditLogInfo,
        InstanceType: &instanceTypeAuditLogInfo,
    }
    response, err := client.ListPlaybookAuditLogs(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.9 Playbook Review Management

4.9.1 Reviewing a Playbook

Function

This API is used to review a playbook.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/approval

Table 4-605 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
version_id	Yes	String	Version ID.

Request Parameters

Table 4-606 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-607 Request body parameters

Parameter	Mandatory	Type	Description
result	No	String	**PASS** or **UN_PASS**
content	No	String	Review comments.

Response Parameters

Status code: 200

Table 4-608 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-609 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Response message.
data	**ApproveOpinionDetail** object	Review details.

Table 4-610 ApproveOpinionDetail

Parameter	Type	Description
result	String	Review result.
content	String	Review content.

Status code: 400

Table 4-611 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-612 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Review a playbook. The review result is "PASS" and the review comments are "xxxxx."

```
{
  "result" : "PASS",
  "content" : "xxxxx"
}
```

Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "result" : "PASS",
    "content" : "need modify"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Review a playbook. The review result is "PASS" and the review comments are "xxxxx."

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class CreatePlaybookApproveSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePlaybookApproveRequest request = new CreatePlaybookApproveRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withVersionId("{version_id}");
        ApprovePlaybookInfo body = new ApprovePlaybookInfo();
        body.withContent("xxxxx");
        body.withResult("PASS");
        request.withBody(body);
        try {
            CreatePlaybookApproveResponse response = client.createPlaybookApprove(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

Review a playbook. The review result is "PASS" and the review comments are "xxxxx."

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
```



```
        request = CreatePlaybookApproveRequest()
        request.workspace_id = "{workspace_id}"
        request.version_id = "{version_id}"
        request.body = ApprovePlaybookInfo(
            content="xxxxx",
            result="PASS"
        )
        response = client.create_playbook_approve(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

Review a playbook. The review result is "PASS" and the review comments are "xxxxx."

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePlaybookApproveRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.VersionId = "{version_id}"
    contentApprovePlaybookInfo:= "xxxxx"
    resultApprovePlaybookInfo:= "PASS"
    request.Body = &model.ApprovePlaybookInfo{
        Content: &contentApprovePlaybookInfo,
        Result: &resultApprovePlaybookInfo,
    }
    response, err := client.CreatePlaybookApprove(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.9.2 Querying the Playbook Review Result

Function

This API is used to query the playbook review result.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/approval

Table 4-613 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Table 4-614 Query Parameters

Parameter	Mandatory	Type	Description
resource_id	No	String	Resource ID.
approve_type	No	String	Review type. (**PLAYBOOK**: Playbooks. **AOP_WORKFLOW**: Workflows.)

Request Parameters

Table 4-615 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-616 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-617 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Response message.
data	Array of **ApproveOpinionDetail** objects	Playbook review details.

Table 4-618 ApproveOpinionDetail

Parameter	Type	Description
result	String	Review result.
content	String	Review content.

Status code: 400

Table 4-619 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-620 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : [ {
    "result" : "PASS",
    "content" : "need modify"
  } ]
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListPlaybookApprovesSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybookApprovesRequest request = new ListPlaybookApprovesRequest();
        request.withWorkspaceId("{workspace_id}");
        try {
            ListPlaybookApprovesResponse response = client.listPlaybookApproves(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListPlaybookApprovesRequest()
        request.workspace_id = "{workspace_id}"
        response = client.list_playbook_approves(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPlaybookApprovesRequest{}
    request.WorkspaceId = "{workspace_id}"
    response, err := client.ListPlaybookApproves(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.10 Playbook Workflow Management

4.10.1 Querying the Playbook Workflow

Function

Querying the Playbook Workflow List

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/actions

Table 4-621 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
version_id	Yes	String	Playbook version ID.

Table 4-622 Query Parameters

Parameter	Mandatory	Type	Description
limit	Yes	Integer	The maximum number of records can be returned on each page for a pagination query. The value starts from 1.
offset	Yes	Integer	Pagination query parameter. This parameter specifies the start position of the query result. The value starts from **0**.

Request Parameters

Table 4-623 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-624 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-625 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
total	Integer	Total number.
size	Integer	The number of records on each page.
page	Integer	Current page number.
data	Array of **ActionInfo** objects	Playbook workflow list.

Table 4-626 ActionInfo

Parameter	Type	Description
id	String	Playbook workflow ID.
name	String	Workflow name.
description	String	Description.
action_type	String	Workflow type.
action_id	String	Workflow ID.
playbook_id	String	Playbook ID.
playbook_version_id	String	Playbook version ID.
project_id	String	Project ID.

Status code: 400

Table 4-627 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-628 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response parameters for a successful request.

```
{
  "code" : 0,
  "message" : "Error message",
  "total" : 41,
  "size" : 3,
```



```
 "page" : 10,
 "data" : [ {
  "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "name" : "MyXXX",
  "description" : "This my XXXX",
  "action_type" : "Workflow",
  "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "playbook_id" : "string",
  "playbook_version_id" : "string",
  "project_id" : "string"
 } ]
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListPlaybookActionsSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybookActionsRequest request = new ListPlaybookActionsRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withVersionId("{version_id}");
        try {
            ListPlaybookActionsResponse response = client.listPlaybookActions(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListPlaybookActionsRequest()
        request.workspace_id = "{workspace_id}"
        request.version_id = "{version_id}"
        response = client.list_playbook_actions(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPlaybookActionsRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.VersionId = "{version_id}"
    response, err := client.ListPlaybookActions(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	Response parameters for a successful request.
400	Response parameters for failed requests.

Error Codes

See **Error Codes**.

4.10.2 Creating a Playbook Workflow

Function

This API is used to create a playbook workflow.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/actions

Table 4-629 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
version_id	Yes	String	Playbook version ID.

Request Parameters

Table 4-630 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-631 Request body parameters

Parameter	Mandatory	Type	Description
[items]	Yes	Array of **CreateAction** objects	Create actions

Table 4-632 CreateAction

Parameter	Mandatory	Type	Description
name	No	String	Name.
description	No	String	Description.
action_type	Yes	String	Type. The default value is **AOP_WORKFLOW**.
action_id	Yes	String	Playbook workflow ID.
sort_order	No	String	Sorting method.

Response Parameters

Status code: 200

Table 4-633 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-634 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error message
data	Array of **ActionInfo** objects	list of informations of playbook action

Table 4-635 ActionInfo

Parameter	Type	Description
id	String	Playbook workflow ID.
name	String	Workflow name.
description	String	Description.
action_type	String	Workflow type.
action_id	String	Workflow ID.
playbook_id	String	Playbook ID.
playbook_version_id	String	Playbook version ID.
project_id	String	Project ID.

Status code: 400

Table 4-636 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-637 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Create a playbook workflow. Workflow name: MyXXX; Description: This my XXXX; Workflow type: aopworkflow; Workflow ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Sorted by: string.

```
[ {
  "name" : "MyXXX",
  "description" : "This my XXXX",
  "action_type" : "aopworkflow",
  "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "sort_order" : "string"
} ]
```

Example Responses

Status code: 200

Response to a successful request.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "description" : "This my XXXX",
    "action_type" : "Workflow",
    "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "string",
    "playbook_version_id" : "string",
    "project_id" : "string"
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Create a playbook workflow. Workflow name: MyXXX; Description: This my XXXX; Workflow type: aopworkflow; Workflow ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Sorted by: string.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class CreatePlaybookActionSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePlaybookActionRequest request = new CreatePlaybookActionRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withVersionId("{version_id}");
        List<CreateAction> listbodyCreateActionInfo = new ArrayList<>();
        listbodyCreateActionInfo.add(
            new CreateAction()
                .withName("MyXXX")
                .withDescription("This my XXXX")
                .withActionType("aopworkflow")
                .withActionId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
                .withSortOrder("string")
        );
        request.withBody(listbodyCreateActionInfo);
        try {
            CreatePlaybookActionResponse response = client.createPlaybookAction(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 playbook workflow. Workflow name: MyXXX; Description: This my XXXX; Workflow type: aopworkflow; Workflow ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Sorted by: string.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreatePlaybookActionRequest()
        request.workspace_id = "{workspace_id}"
        request.version_id = "{version_id}"
        listCreateActionInfobody = [
            CreateAction(
                name="MyXXX",
                description="This my XXXX",
                action_type="aopworkflow",
                action_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
                sort_order="string"
            )
        ]
        request.body = listCreateActionInfobody
        response = client.create_playbook_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

Create a playbook workflow. Workflow name: MyXXX; Description: This my XXXX; Workflow type: aopworkflow; Workflow ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Sorted by: string.

```
package main

import (
    "fmt"
```



```
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePlaybookActionRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.VersionId = "{version_id}"
    nameCreateActionInfo:= "MyXXX"
    descriptionCreateActionInfo:= "This my XXXX"
    sortOrderCreateActionInfo:= "string"
    var listCreateActionInfobody = []model.CreateAction{
        {
            Name: &nameCreateActionInfo,
            Description: &descriptionCreateActionInfo,
            ActionType: "aopworkflow",
            ActionId: "909494e3-558e-46b6-a9eb-07a8e18ca62f",
            SortOrder: &sortOrderCreateActionInfo,
        },
    }
    request.Body = &listCreateActionInfobody
    response, err := client.CreatePlaybookAction(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	Response to a successful request.
400	Response message for failed requests.

Error Codes

See **Error Codes**.

4.10.3 Deleting a Playbook Workflow

Function

This API is used to delete a playbook workflow.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/actions/{action_id}

Table 4-638 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
version_id	Yes	String	Playbook version ID.
action_id	Yes	String	Playbook workflow ID.

Request Parameters

Table 4-639 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-640 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-641 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Response message.

Status code: 400

Table 4-642 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-643 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Response parameters for a successful request.

```
{
  "code" : 0,
```



```
 "message" : "Error message"
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class DeletePlaybookActionSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeletePlaybookActionRequest request = new DeletePlaybookActionRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withVersionId("{version_id}");
        request.withActionId("{action_id}");
        try {
            DeletePlaybookActionResponse response = client.deletePlaybookAction(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeletePlaybookActionRequest()
        request.workspace_id = "{workspace_id}"
        request.version_id = "{version_id}"
        request.action_id = "{action_id}"
        response = client.delete_playbook_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

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())
```



```
    request := &model.DeletePlaybookActionRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.VersionId = "{version_id}"
    request.ActionId = "{action_id}"
    response, err := client.DeletePlaybookAction(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	Response parameters for a successful request.
400	Response parameters for failed requests.

Error Codes

See **Error Codes**.

4.10.4 Updating a Playbook Workflow

Function

This API is used to update a playbook workflow.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/actions/{action_id}

Table 4-644 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Parameter	Mandatory	Type	Description
version_id	Yes	String	Playbook version ID.
action_id	Yes	String	Playbook workflow ID.

Request Parameters

Table 4-645 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-646 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Name.
description	No	String	Description.
action_type	No	String	Type. The default value is **AOP_WORKFLOW**.
action_id	No	String	Playbook workflow ID.
sort_order	No	String	Sorting method.

Response Parameters

Status code: 200

Table 4-647 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-648 Response body parameters

Parameter	Type	Description
code	String	Error code
message	String	Error message
data	**ActionInfo** object	Playbook workflow information.

Table 4-649 ActionInfo

Parameter	Type	Description
id	String	Playbook workflow ID.
name	String	Workflow name.
description	String	Description.
action_type	String	Workflow type.
action_id	String	Workflow ID.
playbook_id	String	Playbook ID.
playbook_version_id	String	Playbook version ID.
project_id	String	Project ID.

Status code: 400

Table 4-650 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-651 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Update a playbook workflow. Workflow name: MyXXX; Description: This my XXXX; Workflow type: aopworkflow; Workflow ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Sorted by: string.

```
{
  "name" : "MyXXX",
  "description" : "This my XXXX",
  "action_type" : "aopworkflow",
  "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "sort_order" : "string"
}
```

Example Responses

Status code: 200

Response parameters for a successful request.

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "MyXXX",
    "description" : "This my XXXX",
    "action_type" : "Workflow",
    "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "playbook_id" : "string",
    "playbook_version_id" : "string",
    "project_id" : "string"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Update a playbook workflow. Workflow name: MyXXX; Description: This my XXXX; Workflow type: aopworkflow; Workflow ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Sorted by: string.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class UpdatePlaybookActionSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdatePlaybookActionRequest request = new UpdatePlaybookActionRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withVersionId("{version_id}");
        request.withActionId("{action_id}");
        ModifyActionInfo body = new ModifyActionInfo();
        body.withSortOrder("string");
        body.withActionId("909494e3-558e-46b6-a9eb-07a8e18ca62f");
        body.withActionType("aopworkflow");
        body.withDescription("This my XXXX");
        body.withName("MyXXX");
        request.withBody(body);
        try {
            UpdatePlaybookActionResponse response = client.updatePlaybookAction(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 playbook workflow. Workflow name: MyXXX; Description: This my XXXX; Workflow type: aopworkflow; Workflow ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Sorted by: string.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdatePlaybookActionRequest()
        request.workspace_id = "{workspace_id}"
        request.version_id = "{version_id}"
        request.action_id = "{action_id}"
        request.body = ModifyActionInfo(
            sort_order="string",
            action_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            action_type="aopworkflow",
            description="This my XXXX",
            name="MyXXX"
        )
        response = client.update_playbook_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

Update a playbook workflow. Workflow name: MyXXX; Description: This my XXXX; Workflow type: aopworkflow; Workflow ID: 909494e3-558e-46b6-a9eb-07a8e18ca62f; Sorted by: string.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdatePlaybookActionRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.VersionId = "{version_id}"
    request.ActionId = "{action_id}"
    sortOrderModifyActionInfo:= "string"
```



```
    actionIdModifyActionInfo:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    actionTypeModifyActionInfo:= "aopworkflow"
    descriptionModifyActionInfo:= "This my XXXX"
    nameModifyActionInfo:= "MyXXX"
    request.Body = &model.ModifyActionInfo{
        SortOrder: &sortOrderModifyActionInfo,
        ActionId: &actionIdModifyActionInfo,
        ActionType: &actionTypeModifyActionInfo,
        Description: &descriptionModifyActionInfo,
        Name: &nameModifyActionInfo,
    }
    response, err := client.UpdatePlaybookAction(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	Response parameters for a successful request.
400	Response parameters for failed requests.

Error Codes

See **Error Codes**.

4.11 Incident Relationship Management

4.11.1 Querying the List of Associated Data Objects

Function

This API is used to query the list of associated data objects.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}/search

Table 4-652 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
dataclass_type	Yes	String	Data class the association subject data object belongs to. The value must be plural and written in lowercase, for example, "alerts" and "incidents".
data_object_id	Yes	String	ID of the associated data object.
related_dataclass_type	Yes	String	Data class the associated data object belongs to. The value must be plural and written in lowercase, for example, "alerts" and "incidents".

Request Parameters

Table 4-653 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.
content-type	Yes	String	Content type.

Table 4-654 Request body parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	The number of records on each page.
offset	No	Integer	Offset.
sort_by	No	String	Sorting field: create_time | update_time

Parameter	Mandatory	Type	Description
order	No	String	Sorting order. Options: **DESC** and **ASC**.
from_date	No	String	Search start time, for example, 2023-02-20T00:00:00.000Z.
to_date	No	String	Search end time, for example, 2023-02-27T23:59:59.999Z.
condition	No	**condition** object	Search condition expression.

Table 4-655 condition

Parameter	Mandatory	Type	Description
conditions	No	Array of **conditions** objects	Expression list.
logics	No	Array of strings	Expression name list.

Table 4-656 conditions

Parameter	Mandatory	Type	Description
name	No	String	Expression name.
data	No	Array of strings	Expression content list.

Response Parameters

Status code: 200

Table 4-657 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-658 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
total	Integer	Total number of alerts.
limit	Integer	The number of records on each page.
offset	Integer	Offset.
success	Boolean	Successful or not.
data	Array of **DataObjectDetail** objects	Alert list.

Table 4-659 DataObjectDetail

Parameter	Type	Description
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
data_object	**DataObject** object	Alert entity information.
dataclass_ref	**dataclass_ref** object	Data class object.
format_version	Integer	Format version.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
project_id	String	ID of the current project.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
version	Integer	Version.
workspace_id	String	ID of the current workspace.

Table 4-660 DataObject

Parameter	Type	Description
version	String	Version of the data source of an alert. The value must be one officially released by the SSA service.
id	String	Unique identifier of an incident. The value is in UUID format and can contain a maximum of 36 characters.
domain_id	String	ID of the account (domain_id) to whom the data is delivered and hosted.
region_id	String	ID of the region where the account to whom the data is delivered and hosted.
workspace_id	String	ID of the current workspace.
environment	**environment** object	Coordinates of the environment where the alert was generated.
datasource	**datasource** object	Data source reported for the first time.
first_observed_time	String	First discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
last_observed_time	String	Latest discovery time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
create_time	String	Recording time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Parameter	Type	Description
arrive_time	String	Receiving time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
title	String	Alert title.
description	String	Alert description.
source_url	String	Alert URL, which points to the page of the current incident description in the data source product.
count	Integer	Incident occurrences.
confidence	Integer	Incident confidence. Confidence is used to illustrate the accuracy of an identified behavior or problem. Value range: 0 to 100. **0** indicates that the confidence is 0%, and **100** indicates that the confidence is 100%.
severity	String	Severity level. Value range: Tips | Low | Medium | High | Fatal Note: **0**: Tips. No threats are found. **1**: Low. No actions are required for the threat. **2**: Medium. The threat needs to be handled but is not urgent. **3**: High. The threat must be handled preferentially. **4**: Fatal. The threat must be handled immediately to prevent further damage.
criticality	Integer	Criticality, which specifies the importance level of the resources involved in an incident. Value range: 0 to 100. **0** indicates that the resource is not critical, and **100** indicates that the resource is critical.
alert_type	**alert_type** object	Alert classification. For details, see the *Alert Type Definition*.
network_list	Array of **network_list** objects	Network information.

Parameter	Type	Description
resource_list	Array of **resource_list** objects	Affected resources.
remediation	**remediation** object	Remedy measure.
verification_state	String	Verification status, which identifies the accuracy of the incident. The options are as follows: **Unknown**: The incident is unknown. **True_Positive**: The incident is confirmed. **False_Positive**: The incident is a false positive. The default value is **Unknown**.
handle_status	String	Incident handling status. The options are as follows: **Open**: Default status. **Block** **Closed** The default value is **Open**.
sla	Integer	Closure time: The deadline by which the incident must be resolved. Unit: hour.
update_time	String	Update time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
close_time	String	Closure time, in the ISO 8601 format of "YYYY-MM-DDTHH:mm:ss.ms+Time zone". Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
ipdrr_phase	String	Period/Handling phase No. **Preparation**: Preparation stage. **Detection and Analysis**: Detection and analysis stage. **Contain, Eradication& Recovery**: Containment, eradication, and recovery stage. **Post-Incident-Activity**: Post-incident activity stage.

Parameter	Type	Description
simulation	String	Debugging field.
actor	String	Alert investigator.
owner	String	Owner and service owner.
creator	String	Creator.
close_reason	String	Closure reason. False detection Resolved Repeated Other
close_comment	String	Comment for the closure.
malware	**malware** object	Malware.
system_info	Object	System information.
process	Array of **process** objects	Process information.
user_info	Array of **user_info** objects	User information.
file_info	Array of **file_info** objects	File information.

Table 4-661 environment

Parameter	Type	Description
vendor_type	String	Environment provider.
domain_id	String	Account ID.
region_id	String	Region ID. **global** is returned for global services.
cross_workspace_id	String	Source workspace ID before data delivery. In the source workspace, the value is null. After data delivery, the value is the ID of the delegated user.
project_id	String	Project ID. The default value is null for global services.

Table 4-662 datasource

Parameter	Type	Description
source_type	Integer	Data source type. The options are as follows: **1**: Cloud service **2**: Third-party product **3**: Private product
domain_id	String	Account ID to which the data source product belongs.
project_id	String	ID of the project to which the data source product belongs.
region_id	String	Region where the data source product is located. For details about the value range, see "Regions and Endpoints".
company_name	String	Name of the company to which the data source product belongs.
product_name	String	Name of the data source product.
product_feature	String	Name of the feature of the product that detects the incident.
product_module	String	Threat detection model list.

Table 4-663 alert_type

Parameter	Type	Description
category	String	Category.
alert_type	String	Alert type.

Table 4-664 network_list

Parameter	Type	Description
direction	String	Direction. The value can be **IN** or **OUT**.
protocol	String	Protocol, including Layer 7 and Layer 4 protocols. Reference: IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Parameter	Type	Description
src_ip	String	Source IP address.
src_port	Integer	Source port. Value range: 0 - 65535.
src_domain	String	Source domain name.
src_geo	**src_geo** object	Geographical location of the source IP address.
dest_ip	String	Destination IP address.
dest_port	String	Destination port. Value range: 0 to 65535.
dest_domain	String	Destination domain name.
dest_geo	**dest_geo** object	Geographical location of the destination IP address.

Table 4-665 src_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-666 dest_geo

Parameter	Type	Description
latitude	Number	Latitude.
longitude	Number	Longitude.
city_code	String	City Code.
country_code	String	Country code. For details, see ISO 3166-1 alpha-2. For example, CN|US|DE|IT|SG.

Table 4-667 resource_list

Parameter	Type	Description
id	String	Cloud service resource ID.
name	String	Resource name.
type	String	Resource type, which is the same as the **type** field in the RMS service.
provider	String	Cloud service name, which is the same as the **provider** field in the RMS service.
region_id	String	Region. Enter the value based on the cloud region ID.
domain_id	String	ID of the account to which the resource belongs, in UUID format.
project_id	String	ID of the project to which the resource belongs, in UUID format.
ep_id	String	Enterprise project ID.
ep_name	String	Enterprise project name.
tags	String	Resource tags. 1. A maximum of 50 key-value pairs are supported. 2. The value can contain a maximum of 255 characters, including letters, digits, spaces, and special characters (+, -, =, ., _, :, /,@).

Table 4-668 remediation

Parameter	Type	Description
recommendation	String	Recommended solution.
url	String	URL, which points to the general handling details for the incident. The URL must be accessible from the public network with no credentials required.

Table 4-669 malware

Parameter	Type	Description
malware_family	String	Malicious family.
malware_class	String	Malware classification.

Table 4-670 process

Parameter	Type	Description
process_name	String	Process name.
process_path	String	Path of the process execution file.
process_pid	Integer	Process ID.
process_uid	Integer	User ID associated with the process.
process_cmdline	String	Process command line.
process_parent_name	String	Parent process name.
process_parent_path	String	Path of the parent process execution file.
process_parent_pid	Integer	Parent process ID.
process_parent_uid	Integer	User ID associated with the parent process.
process_parent_cmdline	String	Parent process command line.
process_child_name	String	Subprocess name.
process_child_path	String	Path of the subprocess execution file.
process_child_pid	Integer	Subprocess ID.
process_child_uid	Integer	User ID associated with the subprocess.
process_child_cmdline	String	Subprocess command line.

Parameter	Type	Description
process_launche_time	String	Process start time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
process_terminate_time	String	Process end time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms +Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.

Table 4-671 user_info

Parameter	Type	Description
user_id	String	User ID (UID).
user_name	String	Username.

Table 4-672 file_info

Parameter	Type	Description
file_path	String	File path/name.
file_content	String	File content.
file_new_path	String	New file path/name.
file_hash	String	File hashes.
file_md5	String	File MD5 value.
file_sha256	String	SHA256 value of the file.
file_attr	String	File attributes.

Table 4-673 dataclass_ref

Parameter	Type	Description
id	String	Unique identifier of a data class. The value is in UUID format and can contain a maximum of 36 characters.

Parameter	Type	Description
name	String	Data class name.

Status code: 400

Table 4-674 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-675 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Query the data object relationship list. Offset: 10. Quantity: 3.

```
{
  "limit" : 3,
  "offset" : 10
}
```

Example Responses

Status code: 200

Response body for querying associating data objects.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "total" : 41,
  "limit" : 3,
  "offset" : 10,
  "data" : null
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Query the data object relationship list. Offset: 10. Quantity: 3.


```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListDataobjectRelationsSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListDataobjectRelationsRequest request = new ListDataobjectRelationsRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withDataclassType("{dataclass_type}");
        request.withDataObjectId("{data_object_id}");
        request.withRelatedDataclassType("{related_dataclass_type}");
        DataobjectSearch body = new DataobjectSearch();
        body.withOffset(10);
        body.withLimit(3);
        request.withBody(body);
        try {
            ListDataobjectRelationsResponse response = client.listDataobjectRelations(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 data object relationship list. Offset: 10. Quantity: 3.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
```



```
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListDataobjectRelationsRequest()
        request.workspace_id = "{workspace_id}"
        request.dataclass_type = "{dataclass_type}"
        request.data_object_id = "{data_object_id}"
        request.related_dataclass_type = "{related_dataclass_type}"
        request.body = DataobjectSearch(
            offset=10,
            limit=3
        )
        response = client.list_dataobject_relations(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 data object relationship list. Offset: 10. Quantity: 3.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
```



```
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

    request := &model.ListDataobjectRelationsRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.DataclassType = "{dataclass_type}"
    request.DataObjectId = "{data_object_id}"
    request.RelatedDataclassType = "{related_dataclass_type}"
    offsetDataobjectSearch:= int32(10)
    limitDataobjectSearch:= int32(3)
    request.Body = &model.DataobjectSearch{
        Offset: &offsetDataobjectSearch,
        Limit: &limitDataobjectSearch,
    }
    response, err := client.ListDataobjectRelations(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	Response body for querying associating data objects.
400	Response body for failed requests for querying associating data objects.

Error Codes

See **Error Codes**.

4.11.2 Associating with a Data Object

Function

This API is used to associate with a data object.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}

Table 4-676 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
dataclass_type	Yes	String	Data class the association subject data object belongs to. The value must be plural and written in lowercase, for example, "alerts" and "incidents".
data_object_id	Yes	String	ID of the associated data object.
related_dataclass_type	Yes	String	Data class the associated data object belongs to. The value must be plural and written in lowercase, for example, "alerts" and "incidents".

Request Parameters

Table 4-677 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.
content-type	Yes	String	Content type.

Table 4-678 Request body parameters

Parameter	Mandatory	Type	Description
ids	No	Array of strings	The ID list of associated data objects.

Response Parameters

Status code: 200

Table 4-679 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-680 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
request_id	String	The request ID.
total	Integer	Total number.
limit	Integer	The number of records on each page.
offset	Integer	Offset.
success	Boolean	Successful or not.
data	**BatchOperateDataobjectResult** object	Returned object for batch operation on alerts.

Table 4-681 BatchOperateDataobjectResult

Parameter	Type	Description
error_ids	Array of strings	Failed IDs.
success_ids	Array of strings	Succeeded IDs.

Status code: 400

Table 4-682 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-683 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Create an incident relationship. Incident ID: f60bf0e7-73b8-4832-8fc4-8c2a12830552.

```
{
  "ids" : [ "f60bf0e7-73b8-4832-8fc4-8c2a12830552" ]
}
```

Example Responses

Status code: 200

Response body for the request for associating with a data object.

```
{
  "code" : 0,
  "message" : "Error message",
  "request_id" : "Error message",
  "success" : false,
  "total" : 41,
  "limit" : 3,
  "offset" : 10,
  "data" : {
    "success_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
    "error_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Create an incident relationship. Incident ID: f60bf0e7-73b8-4832-8fc4-8c2a12830552.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class CreateDataobjectRelationsSolution {
```



```
    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateDataobjectRelationsRequest request = new CreateDataobjectRelationsRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withDataclassType("{dataclass_type}");
        request.withDataObjectId("{data_object_id}");
        request.withRelatedDataclassType("{related_dataclass_type}");
        CreateDataobjectRelationsRequestBody body = new CreateDataobjectRelationsRequestBody();
        List<String> listbodyIds = new ArrayList<>();
        listbodyIds.add("f60bf0e7-73b8-4832-8fc4-8c2a12830552");
        body.withIds(listbodyIds);
        request.withBody(body);
        try {
            CreateDataobjectRelationsResponse response = client.createDataobjectRelations(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 an incident relationship. Incident ID: f60bf0e7-73b8-4832-8fc4-8c2a12830552.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = CreateDataobjectRelationsRequest()
    request.workspace_id = "{workspace_id}"
    request.dataclass_type = "{dataclass_type}"
    request.data_object_id = "{data_object_id}"
    request.related_dataclass_type = "{related_dataclass_type}"
    listIdsbody = [
        "f60bf0e7-73b8-4832-8fc4-8c2a12830552"
    ]
    request.body = CreateDataobjectRelationsRequestBody(
        ids=listIdsbody
    )
    response = client.create_dataobject_relations(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 incident relationship. Incident ID: f60bf0e7-73b8-4832-8fc4-8c2a12830552.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateDataobjectRelationsRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.DataclassType = "{dataclass_type}"
    request.DataObjectId = "{data_object_id}"
```



```
    request.RelatedDataclassType = "{related_dataclass_type}"
    var listIdsbody = []string{
        "f60bf0e7-73b8-4832-8fc4-8c2a12830552",
    }
    request.Body = &model.CreateDataobjectRelationsRequestBody{
        Ids: &listIdsbody,
    }
    response, err := client.CreateDataobjectRelations(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	Response body for the request for associating with a data object.
400	Response body for failed requests for associating with a data object.

Error Codes

See **Error Codes**.

4.11.3 Canceling the Association with a Data Object

Function

This API is used to cancel the association with a data object.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}

Table 4-684 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Parameter	Mandatory	Type	Description
workspace_id	Yes	String	Workspace ID.
dataclass_type	Yes	String	Data class the association subject data object belongs to. The value must be plural and written in lowercase, for example, "alerts" and "incidents".
data_object_id	Yes	String	ID of the associated data object.
related_dataclass_type	Yes	String	Data class the associated data object belongs to. The value must be plural and written in lowercase, for example, "alerts" and "incidents".

Request Parameters

Table 4-685 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.
content-type	Yes	String	Content type.

Table 4-686 Request body parameters

Parameter	Mandatory	Type	Description
ids	No	Array of strings	The ID list of associated data objects.

Response Parameters

Status code: 200

Table 4-687 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-688 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error message.
data	**BatchOperateDataobjectResult** object	Returned object for batch operation on alerts.

Table 4-689 BatchOperateDataobjectResult

Parameter	Type	Description
error_ids	Array of strings	Failed IDs.
success_ids	Array of strings	Succeeded IDs.

Status code: 400

Table 4-690 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-691 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Delete an incident relationship. Incident ID: f60bf0e7-73b8-4832-8fc4-8c2a12830552.

```
{
  "ids" : [ "f60bf0e7-73b8-4832-8fc4-8c2a12830552" ]
}
```

Example Responses

Status code: 200

Response body for the request for canceling the association with a data object.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "request_id" : "Error message",
  "success" : false,
  "total" : 41,
  "limit" : 3,
  "offset" : 10,
  "data" : {
    "success_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ],
    "error_ids" : [ "909494e3-558e-46b6-a9eb-07a8e18ca62f" ]
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Delete an incident relationship. Incident ID: f60bf0e7-73b8-4832-8fc4-8c2a12830552.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class DeleteDataobjectRelationsSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
            .withCredential(auth)
            .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
            .build();
        DeleteDataobjectRelationsRequest request = new DeleteDataobjectRelationsRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withDataclassType("{dataclass_type}");
        request.withDataObjectId("{data_object_id}");
        request.withRelatedDataclassType("{related_dataclass_type}");
        CreateDataobjectRelationsRequestBody body = new CreateDataobjectRelationsRequestBody();
        List<String> listbodyIds = new ArrayList<>();
        listbodyIds.add("f60bf0e7-73b8-4832-8fc4-8c2a12830552");
        body.withIds(listbodyIds);
        request.withBody(body);
        try {
            DeleteDataobjectRelationsResponse response = client.deleteDataobjectRelations(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 an incident relationship. Incident ID: f60bf0e7-73b8-4832-8fc4-8c2a12830552.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteDataobjectRelationsRequest()
        request.workspace_id = "{workspace_id}"
        request.dataclass_type = "{dataclass_type}"
```



```
        request.data_object_id = "{data_object_id}"
        request.related_dataclass_type = "{related_dataclass_type}"
        listIdsbody = [
            "f60bf0e7-73b8-4832-8fc4-8c2a12830552"
        ]
        request.body = CreateDataobjectRelationsRequestBody(
            ids=listIdsbody
        )
        response = client.delete_dataobject_relations(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 an incident relationship. Incident ID: f60bf0e7-73b8-4832-8fc4-8c2a12830552.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteDataobjectRelationsRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.DataclassType = "{dataclass_type}"
    request.DataObjectId = "{data_object_id}"
    request.RelatedDataclassType = "{related_dataclass_type}"
    var listIdsbody = []string{
        "f60bf0e7-73b8-4832-8fc4-8c2a12830552",
    }
    request.Body = &model.CreateDataobjectRelationsRequestBody{
        Ids: &listIdsbody,
    }
    response, err := client.DeleteDataobjectRelations(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	Response body for the request for canceling the association with a data object.
400	Response body for failed requests for canceling the association with a data object.

Error Codes

See **Error Codes**.

4.12 Data Class Management

4.12.1 Querying the Data Class List

Function

This API is used to query the data class list.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses

Table 4-692 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Table 4-693 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Offset.
limit	No	Integer	Data volume.
name	No	String	Search by name.
business_code	No	String	Service code.
description	No	String	Description.
is_built_in	No	Boolean	Built-in or not.

Request Parameters

Table 4-694 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.
content-type	Yes	String	Content type.

Response Parameters

Status code: 200

Table 4-695 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-696 Response body parameters

Parameter	Type	Description
dataclass_details	Array of **DataClassResponseBody** objects	Data class details.

Parameter	Type	Description
total	Number	Total data volume.

Table 4-697 DataClassResponseBody

Parameter	Type	Description
id	String	Data class ID.
create_time	String	Creation time.
update_time	String	Update time.
creator_id	String	Creator ID.
creator_name	String	Creator name.
modifier_id	String	ID of the editor.
modifier_name	String	Modifier name.
cloud_pack_version	String	Subscription package version.
region_id	String	Region ID.
project_id	String	Account ID.
workspace_id	String	Workspace ID.
domain_id	String	domain id
name	String	Data class name.
business_code	String	Business code of the data class.
description	String	Data class description.
is_built_in	Boolean	Built-in or not. **true**: Built in; **false**: Not built in.
parent_id	String	Parent ID.
type_num	Number	Number of subtypes.

Status code: 400

Table 4-698 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-699 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Query the data class list. Offset: 10. Quantity: 3.

```
{
  "limit" : 3,
  "offset" : 10
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total" : 41,
  "dataclass_details" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_name" : "Tom",
    "modifier_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "modifier_name" : "Peter",
    "cloud_pack_version" : "Subscribed package version.",
    "region_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "domain_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "name" : "Evidence.",
    "business_code" : "Evidence",
    "description" : "Data class description.",
    "is_built_in" : false,
    "parent_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "type_num" : 9
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Query the data class list. Offset: 10. Quantity: 3.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListDataclassSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListDataclassRequest request = new ListDataclassRequest();
        request.withWorkspaceId("{workspace_id}");
        try {
            ListDataclassResponse response = client.listDataclass(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 data class list. Offset: 10. Quantity: 3.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListDataclassRequest()
        request.workspace_id = "{workspace_id}"
        response = client.list_dataclass(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 data class list. Offset: 10. Quantity: 3.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListDataclassRequest{}
    request.WorkspaceId = "{workspace_id}"
    response, err := client.ListDataclass(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	Response body for failed requests for querying the data class list.

Error Codes

See **Error Codes**.

4.12.2 Querying the Field List

Function

This API is used to query the field list.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields

Table 4-700 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.
dataclass_id	Yes	String	Data class ID.

Table 4-701 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Offset.
limit	No	Integer	Data volume.
name	No	String	Search by name.
is_built_in	No	Boolean	Built-in or not.
field_category	No	String	Field category.

Parameter	Mandatory	Type	Description
mapping	No	Boolean	Whether to display in other places except the category mapping area.

Request Parameters

Table 4-702 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.
content-type	Yes	String	Content type.

Response Parameters

Status code: 200

Table 4-703 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-704 Response body parameters

Parameter	Type	Description
field_details	Array of **FieldResponseBody** objects	list of informations of field
total	Number	Total data volume.

Table 4-705 FieldResponseBody

Parameter	Type	Description
id	String	Id value
cloud_pack_version	String	Subscription package version.
business_id	String	ID of the associated service.
business_type	String	Associated services.
dataclass_name	String	Data class name.
business_code	String	Business code of the field.
field_key	String	Field key.
name	String	Field name.
description	String	Field description.
default_value	String	Default value.
display_type	String	Display type.
field_type	String	Field type, such as shorttext, radio, and grid.
extra_json	String	Additional JSON.
field_tooltip	String	Tool tips.
iu_type	String	Input and output type.
used_by	String	Related service.
json_schema	String	JSON.
is_built_in	Boolean	Built-in or not. **true**: Built in; **false**: Not built in.
case_sensitive	Boolean	**true**: Case sensitive; **false**: Case insensitive
read_only	Boolean	Read-only mode. The value can be **true** (read-only) or **false** (non-read-only).
required	Boolean	Whether the parameter is mandatory. **true**: Mandatory; **false**: Optional.
searchable	Boolean	Searchable or not. **true**: Searchable; **false**: Not searchable.
visible	Boolean	Visible or not. **true**: Visible; **false**: Invisible.

Parameter	Type	Description
maintainable	Boolean	Maintainable or not. **true**: Maintainable; **false**: Not maintainable.
editable	Boolean	Editable or not. **true**: Editable; **false**: Not editable.
creatable	Boolean	Creatable or not. **true**: Yes; **false**: No
mapping	Boolean	Whether to display in other places except the category mapping area.
target_api	String	Target API.
creator_id	String	Creator id value
creator_name	String	Creator name value
modifier_id	String	Modifier id value
modifier_name	String	Modifier name value
create_time	String	Create time
update_time	String	Update time

Status code: 400

Table 4-706 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-707 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Query the field list. Offset: 10. Quantity: 3.

```
{
  "limit" : 3,
  "offset" : 10
}
```


Example Responses

Status code: 200

Request succeeded.


```
{
  "total" : 41,
  "field_details" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "cloud_pack_version" : "Subscription package version.",
    "business_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "business_type" : "Service type.",
    "dataclass_name" : "Service ID.",
    "business_code" : "My Field",
    "field_key" : "Field key.",
    "name" : "Field name.",
    "description" : "Field description.",
    "default_value" : "Default value.",
    "display_type" : "Display type.",
    "field_type" : "shorttext",
    "extra_json" : "{}",
    "field_tooltip" : "Tool tips.",
    "iu_type" : "Input and output type.",
    "used_by" : "Related service.",
    "json_schema" : "{}",
    "is_built_in" : false,
    "case_sensitive" : false,
    "read_only" : false,
    "required" : false,
    "searchable" : false,
    "visible" : false,
    "maintainable" : false,
    "editable" : false,
    "creatable" : false,
    "mapping" : true,
    "target_api" : "Target API.",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_name" : "Tom",
    "modifier_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "modifier_name" : "Peter",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800"
  } ]
}
```


SDK Sample Code

The SDK sample code is as follows.

Java

Query the field list. Offset: 10. Quantity: 3.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListDataclassFieldsSolution {
```

```
    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListDataclassFieldsRequest request = new ListDataclassFieldsRequest();
        request.withWorkspaceId("{workspace_id}");
        request.withDataclassId("{dataclass_id}");
        try {
            ListDataclassFieldsResponse response = client.listDataclassFields(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 field list. Offset: 10. Quantity: 3.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()
```



```
    try:
        request = ListDataclassFieldsRequest()
        request.workspace_id = "{workspace_id}"
        request.dataclass_id = "{dataclass_id}"
        response = client.list_dataclass_fields(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 field list. Offset: 10. Quantity: 3.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListDataclassFieldsRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.DataclassId = "{dataclass_id}"
    response, err := client.ListDataclassFields(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	Response body for failed requests for querying the data class list.

Error Codes

See **Error Codes**.

4.13 Workflow Management

4.13.1 Querying the Workflow List

Function

This API is used to query the workflow list.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows

Table 4-708 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Table 4-709 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Offset.
limit	No	Integer	Data volume.
order	No	String	Sorting order. Options: **asc**: Ascending order; **desc**: Descending order.

Parameter	Mandatory	Type	Description
sortby	No	String	Sorting field. **create_time**: creation time; **category**: category name.
enabled	No	Boolean	Whether to enable this feature.
last_version	No	Boolean	Latest version number.
name	No	String	Workflow name.
description	No	String	Workflow description.
dataclass_id	No	String	Data class ID.
dataclass_name	No	String	Data class name.
aop_type	No	String	Workflow type.

Request Parameters

Table 4-710 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.
content-type	Yes	String	Content type.

Response Parameters

Status code: 200

Table 4-711 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-712 Response body parameters

Parameter	Type	Description
code	String	Response code.
total	Integer	Total data records.
offset	Integer	Current page size.
limit	Integer	Current page number.
message	String	The request ID.
success	Boolean	Successful or not.
data	Array of **AopWorkflowInfo** objects	Workflow list.

Table 4-713 AopWorkflowInfo

Parameter	Type	Description
id	String	Workflow ID.
name	String	Workflow name.
description	String	Description.
project_id	String	Account ID.
owner_id	String	Owner ID.
creator_id	String	Creator ID.
edit_role	String	Role of the editor.
use_role	String	Applicable role.
approve_role	String	Reviewer.
enabled	Boolean	Enabled or not.
workspace_id	String	Workspace ID.
version_id	String	Workflow version ID.
current_approval_version_id	String	Current version number to be reviewed.
current_rejected_versoin_id	String	Current version number that has been rejected.

Parameter	Type	Description
aop_type	String	AOP type. The options are as follows: **NORMAL**: General **SURVEY**: Investigation **HEMOSTASIS**: Prevention **EASE**: Mitigation
engine_type	String	Engine type. Shared and dedicated engines are available.
dataclass_id	String	Data class ID.

Status code: 400

Table 4-714 Response header parameters

Parameter	Type	Description
X-request-id	String	Request ID. Format: request_uuid-timestamp-hostname.

Table 4-715 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Query the workflow list. Offset: 10. Quantity: 3.

```
{
  "limit" : 3,
  "offset" : 10
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "total" : 41,
  "limit" : 2,
  "offset" : 1,
```



```
 "success" : true,
 "data" : [ {
  "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "name" : "Workflow name.",
  "description" : "Description.",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "owner_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "edit_role" : "Editor.",
  "use_role" : "User.",
  "approve_role" : "Approver.",
  "enabled" : true,
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "version_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "current_approval_version_id" : "v2",
  "current_rejected_versoin_id" : "v1",
  "aop_type" : "**EASE**: Mitigation",
  "engine_type" : "public_engine",
  "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
 } ]
}
```


SDK Sample Code

The SDK sample code is as follows.

Java

Query the workflow list. Offset: 10. Quantity: 3.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListWorkflowsSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListWorkflowsRequest request = new ListWorkflowsRequest();
        request.withWorkspaceId("{workspace_id}");
        try {
            ListWorkflowsResponse response = client.listWorkflows(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 workflow list. Offset: 10. Quantity: 3.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListWorkflowsRequest()
        request.workspace_id = "{workspace_id}"
        response = client.list_workflows(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 workflow list. Offset: 10. Quantity: 3.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListWorkflowsRequest{}
    request.WorkspaceId = "{workspace_id}"
    response, err := client.ListWorkflows(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	Response body for failed requests for querying the data class list.

Error Codes

See **Error Codes**.

4.14 Data Space Management

4.14.1 Creating a Data Space

Function

This API is used to create a data space.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces

Table 4-716 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-717 Request body parameters

Parameter	Mandatory	Type	Description
dataspace_name	Yes	String	Data space name.
description	Yes	String	Description.

Response Parameters

Status code: 200

Table 4-718 Response body parameters

Parameter	Type	Description
domain_id	String	Account ID.
region_id	String	region ID
project_id	String	Project ID.
dataspace_id	String	Workspace ID.
dataspace_name	String	Workspace name.

Parameter	Type	Description
dataspace_type	String	Data space type. The value can be **system-defined** or **user-defined**.
description	String	Description.
create_by	String	Creator.
create_time	Long	Creation time.
update_by	String	Updater.
update_time	Long	Update time.

Example Requests

```
{
  "dataspace_name" : "dataspace-01",
  "description" : "test dataspace"
}
```

Example Responses

Status code: 200

Response value to a successful creation.

```
{
  "domain_id" : "0531ed520xxxxxxebedb6e57xxxxxxxx",
  "region_id" : "region_id",
  "project_id" : "2b31ed520xxxxxxebedb6e57xxxxxxxx",
  "dataspace_id" : "a00106ba-bede-453c-8488-b60c70bd6aed",
  "dataspace_name" : "dataspace-01",
  "dataspace_type" : "system-defined",
  "description" : "test dataspace",
  "create_by" : "0642ed520xxxxxxebedb6e57xxxxxxxx",
  "create_time" : 1584883694354,
  "update_by" : "0642ed520xxxxxxebedb6e57xxxxxxxx",
  "update_time" : 1584883694354
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class CreateDataspaceSolution {
```



```
    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateDataspaceRequest request = new CreateDataspaceRequest();
        request.withWorkspaceId("{workspace_id}");
        CreateDataspaceRequestBody body = new CreateDataspaceRequestBody();
        request.withBody(body);
        try {
            CreateDataspaceResponse response = client.createDataspace(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
```



```
        request = CreateDataspaceRequest()
        request.workspace_id = "{workspace_id}"
        request.body = CreateDataspaceRequestBody(
        )
        response = client.create_dataspace(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateDataspaceRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.Body = &model.CreateDataspaceRequestBody{
    }
    response, err := client.CreateDataspace(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	Response value to a successful creation.

Error Codes

See **Error Codes**.

4.15 Pipeline Management

4.15.1 Creating a Data Pipeline

Function

This API is used to create a data pipeline.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/pipes

Table 4-719 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-720 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 4-721 Request body parameters

Parameter	Mandatory	Type	Description
dataspace_id	Yes	String	Workspace ID.
pipe_name	Yes	String	Data pipeline name.
description	No	String	Description.
storage_period	Yes	Integer	Data storage duration, in days. The default value is 30. The value ranges from 1 to 3,600.
shards	Yes	Integer	Number of pipeline partitions. One partition is created by default. A maximum of 64 partitions can be created.
timestamp_field	No	String	Timestamp.
mapping	No	Map<String,**KeyIndex**>	Index field mapping. Each key object carries information about a field. There are multiple key objects. The key is variable and indicates the field name. Nesting is supported.

Table 4-722 KeyIndex

Parameter	Mandatory	Type	Description
type	No	String	Field type. The options are text (full-text index field), keyword (structured field), Long, Integer, Double, Float (time field), and Date (time field).
is_chinese_exist	No	Boolean	Whether non-English characters are contained.
properties	No	Map<String,**KeyIndex**>	Nested structure.

Response Parameters

Status code: 200

Table 4-723 Response body parameters

Parameter	Type	Description
domain_id	String	User domain ID.
project_id	String	Project ID.
dataspace_id	String	Data space ID.
dataspace_name	String	Data space name.
pipe_id	String	Pipeline ID.
pipe_name	String	Pipeline name.
pipe_type	String	Pipeline type. **system-defined**: Predefined by the system; **user-defined**: Custom pipeline.
description	String	Description.
storage_period	Integer	Index storage duration, measured in days.
shards	Integer	Number of index shards.
create_by	String	Creator.
create_time	Integer	Creation time.
update_by	String	Updater.
update_time	Integer	Update time.

Status code: 400

Table 4-724 Response body parameters

Parameter	Type	Description
error_msg	String	Invalid request message.
error_code	String	Error code.

Status code: 401

Table 4-725 Response body parameters

Parameter	Type	Description
error_msg	String	Insufficient permission.
error_code	String	Error code.

Status code: 403

Table 4-726 Response body parameters

Parameter	Type	Description
error_msg	String	Invalid request message.
error_code	String	Error code.

Status code: 500

Table 4-727 Response body parameters

Parameter	Type	Description
error_msg	String	Internal system error.
error_code	String	Error code.

Example Requests

```
{
  "dataspace_id" : "a00106ba-bede-453c-8488-b60c70bd6aed",
  "pipe_name" : "pipe-01",
  "description" : "test pipe",
  "storage_period" : 30,
  "shards" : 3,
  "mapping" : {
    "name" : {
      "type" : "text"
    },
    "id" : {
      "type" : "text"
    },
    "publish_time" : {
      "type" : "data"
    }
  }
}
```

Example Responses

Status code: 200

Response value to a successful creation.

```
{
  "domain_id" : "0531ed520xxxxxxebedb6e57xxxxxxxx",
  "project_id" : "2b31ed520xxxxxxebedb6e57xxxxxxxx",
  "dataspace_id" : "a00106ba-bede-453c-8488-b60c70bd6aed",
  "dataspace_name" : "dataspace-01",
  "pipe_id" : "b22106ba-bede-453c-8488-b60c70bd6aed",
  "pipe_name" : "pipe-01",
  "pipe_type" : "system-defined",
  "description" : "test pipe",
  "storage_period" : 30,
  "shards" : 3,
```



```
  "create_by" : "0642ed520xxxxxxebedb6e57xxxxxxxx",
  "create_time" : 1584883694354,
  "update_by" : "0642ed520xxxxxxebedb6e57xxxxxxxx",
  "update_time" : 1584883694354
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class CreatePipeSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePipeRequest request = new CreatePipeRequest();
        request.withWorkspaceId("{workspace_id}");
        CreatePipeRequestBody body = new CreatePipeRequestBody();
        request.withBody(body);
        try {
            CreatePipeResponse response = client.createPipe(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreatePipeRequest()
        request.workspace_id = "{workspace_id}"
        request.body = CreatePipeRequestBody(
        )
        response = client.create_pipe(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
```



```
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePipeRequest{}
    request.WorkspaceId = "{workspace_id}"
    request.Body = &model.CreatePipeRequestBody{
    }
    response, err := client.CreatePipe(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	Response value to a successful creation.
400	Request error.
401	Authentication failed.
403	Access denied.
500	Internal system error.

Error Codes

See **Error Codes**.

4.16 Workspace Management

4.16.1 Creating a Workspace

Function

Before using the baseline inspection, alert management, security analysis, and security orchestration in SecMaster, you need to create at least one workspace first. You can use workspaces to group your resources by application scenario. This will make security operations more efficient.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces

Table 4-728 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-729 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-730 Request body parameters

Parameter	Mandatory	Type	Description
region_id	Yes	String	Region ID.
enterprise_project_id	No	String	Enterprise project ID.
enterprise_project_name	No	String	Enterprise project name.
view_bind_id	No	String	ID of the workspace associated with the view.
is_view	No	Boolean	Whether the workspace is a workspace view.
name	Yes	String	Workspace name.
description	No	String	Workspace description.

Parameter	Mandatory	Type	Description
project_name	Yes	String	Project name.
tags	No	Array of **TagsPojo** objects	Adding a Tag to Arrays

Table 4-731 TagsPojo

Parameter	Mandatory	Type	Description
key	No	String	Tag key.
value	No	String	Tag value.

Response Parameters

Status code: 200

Table 4-732 Response body parameters

Parameter	Type	Description
id	String	Workspace ID.
create_time	String	Creation time.
update_time	String	Update time.
name	String	Workspace name.
description	String	Workspace description.
creator_id	String	Creator ID.
creator_name	String	Creator name.
modifier_id	String	Modifier ID.
modifier_name	String	Modifier name.
project_id	String	Project ID.
project_name	String	Project name.
domain_id	String	Tenant ID.
domain_name	String	Tenant name.
enterprise_project_id	String	Enterprise project ID.

Parameter	Type	Description
enterprise_project_name	String	Enterprise project name.
is_view	Boolean	Whether the workspace is a workspace view.
region_id	String	Region ID.
view_bind_id	String	ID of the workspace associated with the view.
view_bind_name	String	Name of the workspace associated with the view.
workspace_agency_list	Array of **workspace_agency_list** objects	The list of managed workspaces.

Table 4-733 workspace_agency_list

Parameter	Type	Description
project_id	String	ID of the project the workspace agency belongs to.
id	String	Workspace agency ID.
name	String	Workspace agency name.
region_id	String	ID of the region the workspace agency belongs to.
workspace_attribution	String	**THIS_ACCOUNT**: The workspace belongs to the current account; **CROSS_ACCOUNT**: The workspace is accessible across different accounts.
agency_version	String	Agency version.
domain_id	String	ID of the delegation account.
domain_name	String	Name of the delegation account.
iam_agency_id	String	IAM agency ID.
iam_agency_name	String	IAM agency name.
resource_spec_code	Array of strings	Workspace agency edition.
selected	Boolean	Whether the workspace is selected for an agency view.

Status code: 400

Table 4-734 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500

Table 4-735 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

Request body for creating a workspace.

```
{
  "name" : "My Workspaces",
  "region_id" : "region_id",
  "project_name" : "project_name",
  "enterprise_project_id" : "",
  "enterprise_project_name" : "",
  "tags" : [ {
    "key" : "tag1",
    "value" : "value1"
  } ],
  "description" : "My Workspaces"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "create_time" : "2024-07-02T09:25:17Z+0800",
  "creator_id" : "b4**********************************46a",
  "creator_name" : "l0******",
  "description" : "My Workspaces",
  "domain_id" : "ac**********************************bf4",
  "domain_name" : "scc****09",
  "enterprise_project_id" : "",
  "enterprise_project_name" : "",
  "id" : "39************bf",
  "is_view" : false,
  "modifier_id" : "",
  "modifier_name" : "",
  "name" : "My Workspaces",
  "project_id" : "15**************************da6",
```



```
  "project_name" : "project_name",
  "region_id" : "region_id",
  "update_time" : "2024-07-02T09:25:17Z+0800",
  "view_bind_id" : "",
  "view_bind_name" : "",
  "workspace_agency_list" : [ ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Request body for creating a workspace.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class CreateWorkspaceSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateWorkspaceRequest request = new CreateWorkspaceRequest();
        CreateWorkspaceRequestBody body = new CreateWorkspaceRequestBody();
        List<TagsPojo> listbodyTags = new ArrayList<>();
        listbodyTags.add(
            new TagsPojo()
                .withKey("tag1")
                .withValue("value1")
        );
        body.withTags(listbodyTags);
        body.withProjectName("project_name");
        body.withDescription("My Workspaces");
        body.withName("My Workspaces");
        body.withEnterpriseProjectName("");
        body.withEnterpriseProjectId("");
        body.withRegionId("region_id");
        request.withBody(body);
```



```
        try {
            CreateWorkspaceResponse response = client.createWorkspace(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

Request body for creating a workspace.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateWorkspaceRequest()
        listTagsbody = [
            TagsPojo(
                key="tag1",
                value="value1"
            )
        ]
        request.body = CreateWorkspaceRequestBody(
            tags=listTagsbody,
            project_name="project_name",
            description="My Workspaces",
            name="My Workspaces",
            enterprise_project_name="",
            enterprise_project_id="",
            region_id="region_id"
        )
        response = client.create_workspace(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

Request body for creating a workspace.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateWorkspaceRequest{}
    keyTags:= "tag1"
    valueTags:= "value1"
    var listTagsbody = []model.TagsPojo{
        {
            Key: &keyTags,
            Value: &valueTags,
        },
    }
    descriptionCreateWorkspaceRequestBody:= "My Workspaces"
    enterpriseProjectNameCreateWorkspaceRequestBody:= ""
    enterpriseProjectIdCreateWorkspaceRequestBody:= ""
    request.Body = &model.CreateWorkspaceRequestBody{
        Tags: &listTagsbody,
        ProjectName: "project_name",
        Description: &descriptionCreateWorkspaceRequestBody,
        Name: "My Workspaces",
        EnterpriseProjectName: &enterpriseProjectNameCreateWorkspaceRequestBody,
        EnterpriseProjectId: &enterpriseProjectIdCreateWorkspaceRequestBody,
        RegionId: "region_id",
    }
    response, err := client.CreateWorkspace(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 request parameter.
500	Request failed.

Error Codes

See **Error Codes**.

4.16.2 Querying the Workspace List

Function

This API is used to query the workspace list. You can filter workspaces by workspace name, workspace description, and creation time.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces

Table 4-736 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 4-737 Query Parameters

Parameter	Mandatory	Type	Description
offset	Yes	Number	Offset. An offset specifies the start position of the record to be returned. The value must be a number no less than 0.
limit	Yes	Number	Number of records displayed on each page.
region_id	No	String	Region ID.
name	No	String	Search by name.
description	No	String	Search by description.
view_bind_id	No	String	ID of the workspace associated with the view.
view_bind_name	No	String	Name of the workspace associated with the view.
create_time_start	No	String	Creation start time, for example, 2024-04-26T16:08:09Z+0800.
create_time_end	No	String	Creation end time, for example, 2024-04-2T16:08:09Z+0800.
is_view	No	Boolean	Whether to query the view. The value can be true or false.
ids	No	String	Workspace ID array. IDs are separated by commas (,).
normal_project_id	No	String	General project ID.
enterprise_project_id	No	String	Enterprise project ID.

Request Parameters

Table 4-738 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-739 Response body parameters

Parameter	Type	Description
workspaces	Array of **CreateWorkspaceResponseBody** objects	list of informations of workspaces
count	Number	Total data volume.

Table 4-740 CreateWorkspaceResponseBody

Parameter	Type	Description
id	String	Workspace ID.
create_time	String	Creation time.
update_time	String	Update time.
name	String	Workspace name.
description	String	Workspace description.
creator_id	String	Creator ID.
creator_name	String	Creator name.
modifier_id	String	Modifier ID.
modifier_name	String	Modifier name.

Parameter	Type	Description
project_id	String	Project ID.
project_name	String	Project name.
domain_id	String	Tenant ID.
domain_name	String	Tenant name.
enterprise_project_id	String	Enterprise project ID.
enterprise_project_name	String	Enterprise project name.
is_view	Boolean	Whether the workspace is a workspace view.
region_id	String	Region ID.
view_bind_id	String	ID of the workspace associated with the view.
view_bind_name	String	Name of the workspace associated with the view.
workspace_agency_list	Array of **workspace_agency_list** objects	The list of managed workspaces.

Table 4-741 workspace_agency_list

Parameter	Type	Description
project_id	String	ID of the project the workspace agency belongs to.
id	String	Workspace agency ID.
name	String	Workspace agency name.
region_id	String	ID of the region the workspace agency belongs to.
workspace_attribution	String	**THIS_ACCOUNT**: The workspace belongs to the current account; **CROSS_ACCOUNT**: The workspace is accessible across different accounts.
agency_version	String	Agency version.
domain_id	String	ID of the delegation account.
domain_name	String	Name of the delegation account.

Parameter	Type	Description
iam_agency_id	String	IAM agency ID.
iam_agency_name	String	IAM agency name.
resource_spec_code	Array of strings	Workspace agency edition.
selected	Boolean	Whether the workspace is selected for an agency view.

Status code: 400

Table 4-742 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500

Table 4-743 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.


```
{
  "count" : 1,
  "workspaces" : [ {
    "create_time" : "2024-07-02T09:25:17Z+0800",
    "creator_id" : "b4****************************46a",
    "creator_name" : "l0******",
    "description" : "My Workspaces",
    "domain_id" : "ac****************************bf4",
    "domain_name" : "scc****09",
    "enterprise_project_id" : "",
```

```
    "enterprise_project_name" : "",
    "id" : "39************bf",
    "is_view" : false,
    "modifier_id" : "",
    "modifier_name" : "",
    "name" : "My Workspaces",
    "project_id" : "15*************************da6",
    "project_name" : "project_name",
    "region_id" : "region_id",
    "update_time" : "2024-07-02T09:25:17Z+0800",
    "view_bind_id" : "",
    "view_bind_name" : "",
    "workspace_agency_list" : [ ]
  } ]
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ListWorkspacesSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListWorkspacesRequest request = new ListWorkspacesRequest();
        try {
            ListWorkspacesResponse response = client.listWorkspaces(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListWorkspacesRequest()
        response = client.list_workspaces(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListWorkspacesRequest{}
    response, err := client.ListWorkspaces(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 request parameter.
500	Request failed.

Error Codes

See **Error Codes**.

4.16.3 Updating a Workspace

Function

This API is used to update the name, description, and other information of a workspace.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v1/{project_id}/workspaces/{workspace_id}

Table 4-744 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-745 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.
content-type	Yes	String	application/json;charset=UTF-8

Table 4-746 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Workspace name.
description	No	String	Workspace description.
view_bind_id	No	String	ID of the workspace associated with the view.

Response Parameters

Status code: 200

Table 4-747 Response body parameters

Parameter	Type	Description
id	String	Workspace ID.
create_time	String	Creation time.
update_time	String	Update time.

Parameter	Type	Description
name	String	Workspace name.
description	String	Workspace description.
creator_id	String	Creator ID.
creator_name	String	Creator name.
modifier_id	String	Modifier ID.
modifier_name	String	Modifier name.
project_id	String	Project ID.
project_name	String	Project name.
domain_id	String	Tenant ID.
domain_name	String	Tenant name.
enterprise_project_id	String	Enterprise project ID.
enterprise_project_name	String	Enterprise project name.
is_view	Boolean	Whether the workspace is a workspace view.
region_id	String	Region ID.
view_bind_id	String	ID of the workspace associated with the view.
view_bind_name	String	Name of the workspace associated with the view.
workspace_agency_list	Array of **workspace_agency_list** objects	The list of managed workspaces.

Table 4-748 workspace_agency_list

Parameter	Type	Description
project_id	String	ID of the project the workspace agency belongs to.
id	String	Workspace agency ID.
name	String	Workspace agency name.
region_id	String	ID of the region the workspace agency belongs to.

Parameter	Type	Description
workspace_attribution	String	**THIS_ACCOUNT**: The workspace belongs to the current account; **CROSS_ACCOUNT**: The workspace is accessible across different accounts.
agency_version	String	Agency version.
domain_id	String	ID of the delegation account.
domain_name	String	Name of the delegation account.
iam_agency_id	String	IAM agency ID.
iam_agency_name	String	IAM agency name.
resource_spec_code	Array of strings	Workspace agency edition.
selected	Boolean	Whether the workspace is selected for an agency view.

Status code: 400

Table 4-749 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500

Table 4-750 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

Request body for updating a workspace.

```
{
  "name" : "Updating a Workspace",
  "description" : "Updating a Workspace"
}
```


Example Responses

Status code: 200

Request succeeded.


```
{
  "create_time" : "2024-07-02T09:25:17Z+0800",
  "creator_id" : "b4****************************46a",
  "creator_name" : "l0******",
  "description" : "Updating a Workspace",
  "domain_id" : "ac****************************bf4",
  "domain_name" : "scc****09",
  "enterprise_project_id" : "",
  "enterprise_project_name" : "",
  "id" : "39************bf",
  "is_view" : false,
  "modifier_id" : "b4****************************46a",
  "modifier_name" : "l0******",
  "name" : "Updating a Workspace",
  "project_id" : "15************************da6",
  "project_name" : "project_name",
  "region_id" : "region_id",
  "update_time" : "2024-07-02T09:25:17Z+0800",
  "view_bind_id" : "",
  "view_bind_name" : "",
  "workspace_agency_list" : [ ]
}
```


SDK Sample Code

The SDK sample code is as follows.

Java

Request body for updating a workspace.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class UpdateWorkspaceSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
```

```
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateWorkspaceRequest request = new UpdateWorkspaceRequest();
        request.withWorkspaceId("{workspace_id}");
        UpdateWorkspaceRequestBody body = new UpdateWorkspaceRequestBody();
        body.withDescription("Updating a Workspace");
        body.withName("Updating a Workspace");
        request.withBody(body);
        try {
            UpdateWorkspaceResponse response = client.updateWorkspace(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

Request body for updating a workspace.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateWorkspaceRequest()
        request.workspace_id = "{workspace_id}"
        request.body = UpdateWorkspaceRequestBody(
            description="Updating a Workspace",
            name="Updating a Workspace"
        )
        response = client.update_workspace(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

Request body for updating a workspace.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateWorkspaceRequest{}
    request.WorkspaceId = "{workspace_id}"
    descriptionUpdateWorkspaceRequestBody:= "Updating a Workspace"
    nameUpdateWorkspaceRequestBody:= "Updating a Workspace"
    request.Body = &model.UpdateWorkspaceRequestBody{
        Description: &descriptionUpdateWorkspaceRequestBody,
        Name: &nameUpdateWorkspaceRequestBody,
    }
    response, err := client.UpdateWorkspace(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 request parameters.

Status Code	Description
500	Request failed.

Error Codes

See **Error Codes**.

4.16.4 Querying Details About a Workspace

Function

This API is used to query details about a workspace, such as the workspace name and description.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/workspaces/{workspace_id}

Table 4-751 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-752 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Table 4-753 Response body parameters

Parameter	Type	Description
workspace	**workspace** object	Workspace details.

Table 4-754 workspace

Parameter	Type	Description
id	String	Workspace ID.
create_time	String	Creation time.
update_time	String	Update time.
name	String	Workspace name.
description	String	Workspace description.
creator_id	String	Creator ID.
creator_name	String	Creator name.
modifier_id	String	Modifier ID.
modifier_name	String	Modifier name.
project_id	String	Project ID.
project_name	String	Project name.
domain_id	String	Tenant ID.
domain_name	String	Tenant name.
enterprise_project_id	String	Enterprise project ID.
enterprise_project_name	String	Enterprise project name.
is_view	Boolean	Whether the workspace is a workspace view.
region_id	String	Region ID.
view_bind_id	String	ID of the workspace associated with the view.
view_bind_name	String	Name of the workspace associated with the view.

Parameter	Type	Description
workspace_agency_list	Array of **workspace_agency_list** objects	The list of managed workspaces.

Table 4-755 workspace_agency_list

Parameter	Type	Description
project_id	String	ID of the project the workspace agency belongs to.
id	String	Workspace agency ID.
name	String	Workspace agency name.
region_id	String	ID of the region the workspace agency belongs to.
workspace_attribution	String	**THIS_ACCOUNT**: The workspace belongs to the current account; **CROSS_ACCOUNT**: The workspace is accessible across different accounts.
agency_version	String	Agency version.
domain_id	String	ID of the delegation account.
domain_name	String	Name of the delegation account.
iam_agency_id	String	IAM agency ID.
iam_agency_name	String	IAM agency name.
resource_spec_code	Array of strings	Workspace agency edition.
selected	Boolean	Whether the workspace is selected for an agency view.

Status code: 400

Table 4-756 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500

Table 4-757 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

None

Example Responses

Status code: 200

Request succeeded.

```
{
  "workspace" : {
    "create_time" : "2024-07-02T09:25:17Z+0800",
    "creator_id" : "b4****************************46a",
    "creator_name" : "l0******",
    "description" : "My Workspaces",
    "domain_id" : "ac****************************bf4",
    "domain_name" : "scc****09",
    "enterprise_project_id" : "",
    "enterprise_project_name" : "",
    "id" : "39************bf",
    "is_view" : false,
    "modifier_id" : "",
    "modifier_name" : "",
    "name" : "My Workspaces",
    "project_id" : "15************************da6",
    "project_name" : "project_name",
    "region_id" : "region_id",
    "update_time" : "2024-07-02T09:25:17Z+0800",
    "view_bind_id" : "",
    "view_bind_name" : "",
    "workspace_agency_list" : [ ]
  }
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class ShowWorkspaceSolution {
```



```
    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowWorkspaceRequest request = new ShowWorkspaceRequest();
        request.withWorkspaceId("{workspace_id}");
        try {
            ShowWorkspaceResponse response = client.showWorkspace(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowWorkspaceRequest()
        request.workspace_id = "{workspace_id}"
```



```
        response = client.show_workspace(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowWorkspaceRequest{}
    request.WorkspaceId = "{workspace_id}"
    response, err := client.ShowWorkspace(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 request parameters.

Status Code	Description
500	Request failed.

Error Codes

See **Error Codes**.

4.16.5 Deleting a Workspace

Function

This API is used to delete a workspace.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v1/{project_id}/workspaces/{workspace_id}

Table 4-758 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Table 4-759 Query Parameters

Parameter	Mandatory	Type	Description
permanent_delete	No	Boolean	Permanent deletion. The value can be **true** or **false**.

Request Parameters

Table 4-760 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.
content-type	Yes	String	application/json;charset=UTF-8

Response Parameters

Status code: 200

Request succeeded.

Status code: 400

Table 4-761 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Status code: 500

Table 4-762 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error description.

Example Requests

None

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class DeleteWorkspaceSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteWorkspaceRequest request = new DeleteWorkspaceRequest();
        request.withWorkspaceId("{workspace_id}");
        try {
            DeleteWorkspaceResponse response = client.deleteWorkspace(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteWorkspaceRequest()
        request.workspace_id = "{workspace_id}"
        response = client.delete_workspace(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"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteWorkspaceRequest{}
    request.WorkspaceId = "{workspace_id}"
    response, err := client.DeleteWorkspace(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 request parameters.
500	Request failed.

Error Codes

See **Error Codes**.

4.17 Metering and Billing

4.17.1 Subscribing to Pay-per-Use SecMaster

Function

This API is used to enable SecMaster billed on a pay-per-use basis.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/subscriptions/orders

Table 4-763 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-764 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.
X-Language	Yes	String	Current environment language. The value can be **zh-cn** or **en-us**.

Table 4-765 Request body parameters

Parameter	Mandatory	Type	Description
region_id	Yes	String	Region ID.
domain_id	Yes	String	domainId
tag_list	No	Array of **TagInfo** objects	Billing tag.
product_list	No	Array of **ProductPostPaid** objects	Product list.
operate_type	No	String	Operation type. The options are **create** for creating product and **addition** for increasing the quota.

Table 4-766 TagInfo

Parameter	Mandatory	Type	Description
key	Yes	String	ID. Only letters, digits, underscores (_), and hyphens (-) are allowed. Length: [2, 36].

Parameter	Mandatory	Type	Description
value	Yes	String	Content. Only letters, digits, underscores (_), and hyphens (-) are allowed. Length: [2, 36].

Table 4-767 ProductPostPaid

Parameter	Mandatory	Type	Description
id	Yes	String	ID, which is used to identify the mapping between the inquiry result and the request. The ID must be unique in an inquiry.
product_id	Yes	String	Product ID, which can be obtained from CBC.
cloud_service_type	Yes	String	Cloud service type. The fixed value is fixed at **hws.service.type.sa** for this service.
resource_type	Yes	String	Resource type of the cloud service product you purchase. For example, the resource type value is **hws.resource.type.secmaster.typical** for the typical scenario configuration of SecMaster.
resource_spec_code	Yes	String	Resource specifications of the cloud service product you purchase. For example, the resource specifications for SecMaster basic edition is **secmaster.basic**.

Parameter	Mandatory	Type	Description
usage_measure_id	Yes	Integer	Usage measurement unit. This parameter is mandatory for a pay-per-use inquiry. For example, the resources are billed by the hour, the usage value is 1, and the usage measurement unit is hour. The options are: **4**: Hours **10**: Gbit/s. Bandwidth usage is measured in Gbit/s based on traffic. **11**: Mbit/s. Bandwidth usage is measured in Mbit/s based on traffic.
usage_value	Yes	Number	Usage value. This parameter is mandatory for a pay-per-use inquiry. For example, the resources are billed by the hour, the usage value is 1, and the usage measurement unit is hour.
resource_size	Yes	Integer	Number of quotas.
usage_factor	Yes	String	Usage factor. This parameter is mandatory for pay-per-use billing. The value is the same as the usage factor in SDRs. The mappings between cloud services and usage factors are as follows: Typical configuration: Duration Situation management: duration Security orchestration: count Intelligent analysis: flow
resource_id	No	String	Resource ID, which is required only when you want to increase the quota.

Response Parameters

Status code: 200

Request succeeded.

None

Example Requests

```
https://{endpoint}/v1/{projectId}/subscriptions/orders

{
  "domain_id" : "abcdef8a41164a2280ec65f1f4c4mlnyz",
  "region_id" : "region_id",
  "product_list" : [ {
    "product_id" : "OFFI908269345109094402",
    "cloud_service_type" : "hws.service.type.sa",
    "id" : "E52E1A22-9408-459A-9F67-7B5C11B1E71A",
    "resource_spec_code" : "secmaster.professional",
    "resource_type" : "hws.resource.type.secmaster.typical",
    "usage_factor" : "duration",
    "usage_value" : 1,
    "usage_measure_id" : 4,
    "resource_size" : 1
  } ]
}
```

Example Responses

Status code: 400

Parameter error.

```
{
  "error_msg" : "You are using SecMaster standard edition. You can upgrade the SecMaster edition in-use or increase the quota as needed.",
  "error_code" : "SecMaster.00010201"
}
```

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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

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

public class CreatePostPaidOrderSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePostPaidOrderRequest request = new CreatePostPaidOrderRequest();
        PostPaidParam body = new PostPaidParam();
        List<ProductPostPaid> listbodyProductList = new ArrayList<>();
        listbodyProductList.add(
            new ProductPostPaid()
                .withId("E52E1A22-9408-459A-9F67-7B5C11B1E71A")
                .withProductId("OFFI908269345109094402")
                .withCloudServiceType("hws.service.type.sa")
                .withResourceType("hws.resource.type.secmaster.typical")
                .withResourceSpecCode("secmaster.professional")
                .withUsageMeasureId(ProductPostPaid.UsageMeasureIdEnum.NUMBER_4)
                .withUsageValue(java.math.BigDecimal.valueOf(1))
                .withResourceSize(1)
                .withUsageFactor("duration")
        );
        body.withProductList(listbodyProductList);
        body.withDomainId("abcdef8a41164a2280ec65f1f4c4mlnyz");
        body.withRegionId("region_id");
        request.withBody(body);
        try {
            CreatePostPaidOrderResponse response = client.createPostPaidOrder(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 huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
```



```
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreatePostPaidOrderRequest()
        listProductListbody = [
            ProductPostPaid(
                id="E52E1A22-9408-459A-9F67-7B5C11B1E71A",
                product_id="OFFI908269345109094402",
                cloud_service_type="hws.service.type.sa",
                resource_type="hws.resource.type.secmaster.typical",
                resource_spec_code="secmaster.professional",
                usage_measure_id=4,
                usage_value=1,
                resource_size=1,
                usage_factor="duration"
            )
        ]
        request.body = PostPaidParam(
            product_list=listProductListbody,
            domain_id="abcdef8a41164a2280ec65f1f4c4mlnyz",
            region_id="region_id"
        )
        response = client.create_post_paid_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

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePostPaidOrderRequest{}
    var listProductListbody = []model.ProductPostPaid{
        {
            Id: "E52E1A22-9408-459A-9F67-7B5C11B1E71A",
```



```
            ProductId: "OFFI908269345109094402",
            CloudServiceType: "hws.service.type.sa",
            ResourceType: "hws.resource.type.secmaster.typical",
            ResourceSpecCode: "secmaster.professional",
            UsageMeasureId: model.GetProductPostPaidUsageMeasureIdEnum().E_4,
            UsageValue: float32(1),
            ResourceSize: int32(1),
            UsageFactor: "duration",
        },
    }
    request.Body = &model.PostPaidParam{
        ProductList: &listProductListbody,
        DomainId: "abcdef8a41164a2280ec65f1f4c4mlnyz",
        RegionId: "region_id",
    }
    response, err := client.CreatePostPaidOrder(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	Parameter error.
403	Insufficient permissions.

Error Codes

See **Error Codes**.

4.18 Querying Metrics

4.18.1 Batch Querying Metrics

Function

This API is used to batch query metrics.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/workspaces/{workspace_id}/sa/metrics/hits

Table 4-768 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Table 4-769 Query Parameters

Parameter	Mandatory	Type	Description
timespan	No	String	The time range for querying metrics. The format is ISO 8601, for example, 2007-03-01T13:00:00Z/2008-05-11T15:30:00Z, 2007-03-01T13:00:00Z/P1Y2M10DT2H30M, or P1Y2M10DT2H30M/2008-05-11T15:30:00Z.
cache	No	Boolean	Whether to enable the cache. The default value is **true**. **false**: The cache is disabled.

Request Parameters

Table 4-770 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 4-771 Request body parameters

Parameter	Mandatory	Type	Description
metric_ids	Yes	Array of strings	The ID list of the metrics to be queried. For details about how to obtain the existing metrics, see the related information in the appendix.
workspace_ids	No	Array of strings	Workspace list. This parameter is mandatory when the data from multiple workspaces can be obtained for metrics.
params	No	Array of Map<String,String> objects	The parameter list for the metric to be queried. Each element in the list is a <String, String> key-value pair. The number of elements must be the same as that of the **metric_ids** list. For details, see the appendix.
interactive_params	No	Array of Map<String,String> objects	Interactive parameter query. If the metric supports interactive parameters, enter a parameter list, which contains <String, String> key-value pairs. For details, see the appendix.
field_ids	No	Array of strings	Metric card ID list.

Response Parameters

Status code: 200

Table 4-772 Response body parameters

Parameter	Type	Description
[items]	Array of **ShowMetricResultResponseBody** objects	Results of batch querying metrics.

Table 4-773 ShowMetricResultResponseBody

Parameter	Type	Description
metric_id	String	Metric ID.
result	**result** object	Metric query result.
metric_format	Array of **MetricFormat** objects	Metric format. The value is fixed based on different metrics.
log_msg	String	Result log information.
status	String	Query result status. The options are as follows: **SUCCESS**: The query is successful. **FAILED**: The query fails. **FALLBACK**: The default value is used.

Table 4-774 result

Parameter	Type	Description
labels	Array of strings	Title of the metric query result table.
datarows	Array<Array<Object>>	Metric query result table.
effective_column	String	Effective column. If this parameter is specified, the specified column is used as the metric data result.

Table 4-775 MetricFormat

Parameter	Type	Description
data	String	Data format.
display	String	Display format.
display_param	Map<String,String>	Display parameters.
data_param	Map<String,String>	Data parameters.

Example Requests

Query the alert severity distribution from June 25 to the current time through the metric API.


```
https://{endpoint}/v1/{project_id}/workspaces/{workspace_id}/sa/metrics/hits

{
  "metric_ids" : [ "1f0f5e29-5a92-17a5-2c16-5f37c6dc109c" ],
  "params" : [ {
    "start_date" : "2024-06-25T00:00:00.000+08:00"
  } ]
}
```

Example Responses

Status code: 200

Request succeeded.

```
[ {
  "metric_id" : "1f0f5e29-5a92-17a5-2c16-5f37c6dc109c",
  "result" : {
    "labels" : [ "label1" ],
    "datarows" : [ [ { } ] ],
    "effective_column" : "0:1"
  },
  "status" : "SUCCESS"
} ]
```

SDK Sample Code

The SDK sample code is as follows.

Java

Query the alert severity distribution from June 25 to the current time through the metric API.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;

import java.util.List;
import java.util.ArrayList;
import java.util.Map;
import java.util.HashMap;

public class BatchSearchMetricHitsSolution {

    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);
```



```
        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        BatchSearchMetricHitsRequest request = new BatchSearchMetricHitsRequest();
        request.withWorkspaceId("{workspace_id}");
        BatchSearchMetricHitsRequestBody body = new BatchSearchMetricHitsRequestBody();
        Map<String, String> listParamsParams = new HashMap<>();
        listParamsParams.put("start_date", "2024-06-25T00:00:00.000+08:00");
        List<Map<String, String>> listbodyParams = new ArrayList<>();
        listbodyParams.add(listParamsParams);
        List<String> listbodyMetricIds = new ArrayList<>();
        listbodyMetricIds.add("1f0f5e29-5a92-17a5-2c16-5f37c6dc109c");
        body.withParams(listbodyParams);
        body.withMetricIds(listbodyMetricIds);
        request.withBody(body);
        try {
            BatchSearchMetricHitsResponse response = client.batchSearchMetricHits(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 alert severity distribution from June 25 to the current time through the metric API.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchSearchMetricHitsRequest()
        request.workspace_id = "{workspace_id}"
        listParamsParams = {
            "start_date": "2024-06-25T00:00:00.000+08:00"
```



```
        }
        listParamsbody = [
            listParamsParams
        ]
        listMetricIdsbody = [
            "1f0f5e29-5a92-17a5-2c16-5f37c6dc109c"
        ]
        request.body = BatchSearchMetricHitsRequestBody(
            params=listParamsbody,
            metric_ids=listMetricIdsbody
        )
        response = client.batch_search_metric_hits(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 alert severity distribution from June 25 to the current time through the metric API.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchSearchMetricHitsRequest{}
    request.WorkspaceId = "{workspace_id}"
    var listParamsParams = map[string]string{
        "start_date": "2024-06-25T00:00:00.000+08:00",
    }
    var listParamsbody = []map[string]string{
        listParamsParams,
    }
    var listMetricIdsbody = []string{
        "1f0f5e29-5a92-17a5-2c16-5f37c6dc109c",
    }
    request.Body = &model.BatchSearchMetricHitsRequestBody{
        Params: &listParamsbody,
```

```
        MetricIds: listMetricIdsbody,
    }
    response, err := client.BatchSearchMetricHits(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**.

4.19 Baseline Inspection

4.19.1 Querying the List of Baseline Inspection Results

Function

This API is used to query the list of baseline inspection results.

Calling Method

For details, see **Calling APIs**.

URI

POST /v2/{project_id}/workspaces/{workspace_id}/sa/baseline/search

Table 4-776 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
workspace_id	Yes	String	Workspace ID.

Request Parameters

Table 4-777 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token.
X-Language	Yes	String	Language. Reference value: zh-CN or en-US.
content-type	Yes	String	Content type.

Table 4-778 Request body parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	The number of records on each page.
offset	No	Integer	Offset. The records after this offset will be queried.
sort_by	No	String	Sorting keyword.
order	No	String	"DESC": Descending order; **ESC**: Ascending order.
from_date	No	String	Start time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
to_date	No	String	End time. The format is ISO 8601: YYYY-MM-DDTHH:mm:ss.ms+Time zone. Time zone refers to where the incident occurred. If this parameter cannot be parsed, the default time zone GMT+8 is used.
condition	No	Object	Search condition expression.

Response Parameters

Status code: 200

Table 4-779 Response body parameters

Parameter	Type	Description
code	String	Error code.
total	Integer	Total number of queried results.
size	Integer	The number of records on each page.
page	Integer	Offset.
success	Boolean	Successful or not.
data	Array of strings	Query result list.

Status code: 400

Table 4-780 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Status code: 401

Table 4-781 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Status code: 500

Table 4-782 Response body parameters

Parameter	Type	Description
code	String	Error code.
message	String	Error description.

Example Requests

Query the baseline inspection results. Time range: June 20, 2024 to June 27, 2024. Compliance package ID: 6add7d71-2261-4195-bab7-8ada0f0ed4d2. Directory ID:

0b78937f-4d9b-4223-9a46-2361e5090be0. Resource type: iam_user. The results are sorted in descending order of the update time. Each page contains 10 records.

```
{
  "limit" : 10,
  "offset" : 0,
  "sort_by" : "last_observed_time",
  "order" : "DESC",
  "from_date" : "2024-06-20T00:00:00.000Z",
  "to_date" : "2024-06-27T23:59:59.999Z",
  "condition" : {
    "conditions" : [ {
      "name" : "compliance_package_id",
      "data" : [ "compliance_package_id", "=", "6add7d71-2261-4195-bab7-8ada0f0ed4d2" ]
    }, {
      "name" : "catalog_id",
      "data" : [ "catalog_id", "=", "0b78937f-4d9b-4223-9a46-2361e5090be0" ]
    }, {
      "name" : "resource.type",
      "data" : [ "resource.type", "=", "iam_user" ]
    } ],
    "logics" : [ "compliance_package_id", "AND", "catalog_id", "AND", "resource.type" ]
  }
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "code" : "00000000",
  "data" : [ {
    "create_time" : "2024-01-03T01:16:21.666+08:00",
    "data_object" : {
      "arrive_time" : "2024-01-03T11:28:03.993Z+0800",
      "baseline_type" : {
        "baseline_type" : "Compliance Check",
        "baseline_type_en" : "Compliance Check",
        "baseline_type_zh" : "Compliance Check",
        "category" : "",
        "category_en" : "",
        "category_zh" : "",
        "id" : "23f48a58cXXX162846076cd0"
      },
      "catalog_id" : "9378d1e8-XXX-4aae-XXX-c41cf6829ede",
      "checkitem_id" : "13fcc967-cb49-XXX-811a-9f72ce6ce8ac",
      "compliance_package_id" : "39488f96-XXX-4cc6-XXX-ad3c29b3a6c2",
      "create_time" : "2024-01-02T17:16:21.666Z+0800",
      "data_source" : {
        "company_name" : "xxx",
        "domain_id" : "ac7438b990efXXXb45e8bf4",
        "product_feature" : "SA",
        "product_module" : "Base-line",
        "product_name" : "SecMaster",
        "project_id" : "15645222e8XXX93dab6341da6",
        "region_id" : "xxx",
        "source_type" : 1
      },
      "dataclass_id" : "f846c8e0-XXX-XXX-bcbf-f77190847f08",
      "domain_id" : "ac7438b990eXXX1004eb45e8bf4",
      "domain_name" : "ac7438b99XXX1004eb45e8bf4",
      "end_time" : "2024-01-03T11:28:51.564Z+0800",
      "execitem_id" : "ca2a1361-5738-479c-8c40-d078e775a23a",
      "execitem_version" : 1,
      "first_observed_time" : "2024-01-03T11:28:50.955Z+0800",
      "handle_status" : "qualified",
```



```
    "id" : "39c56d70a9c2492XXXd91934cb5cb_13fcc967-XXX-494b-XXX-9f72ce6ce8ac",
    "is_deleted" : false,
    "last_observed_time" : "2024-01-03T11:28:51.564Z+0800",
    "method" : 1,
    "origin_id" : "",
    "project_id" : "15645222e874XXX93dab6341da6",
    "region_id" : "xxx",
    "region_name" : "xxx",
    "resource" : {
      "domain_id" : "ac7438b990eXXX04eb45e8bf4",
      "id" : "39c56d70a9cXXX1934cb5cb",
      "name" : "adfasd",
      "project_id" : "15645222XXXc93dab6341da6",
      "provider" : "xxx",
      "region_id" : "xxx",
      "type" : "agency"
    },
    "severity" : "informational",
    "start_time" : "2024-01-03T11:28:50.955Z+0800",
    "task_id" : "10da8403-XXX-442d-XXX-fa2fdf42a3a1",
    "title" : "Checking Agency Permissions for Project-Level Services",
    "trigger_flag" : false,
    "update_time" : "2024-01-03T11:28:51.887Z+0800",
    "workspace_id" : "1350a050-XXX-45e2-XXX-9cbfef116de7"
  },
  "dataclass_ref" : {
    "id" : "f846c8e0-XXX-3767-XXX-f77190847f08"
  },
  "format_version" : 0,
  "id" : "39c56d7XXX278fXXX934cb5cb_13fcc967-cb49-XXX-811a-9f72ce6ce8ac",
  "update_time" : "2024-01-03T19:28:51.887+08:00",
  "version" : 0
}, {
  "create_time" : "2024-01-03T01:16:21.821+08:00",
  "data_object" : {
    "arrive_time" : "2024-01-03T11:28:03.993Z+0800",
    "baseline_type" : {
      "baseline_type" : "Compliance Check",
      "baseline_type_en" : "Compliance Check",
      "baseline_type_zh" : "Compliance Check",
      "category" : "",
      "category_en" : "",
      "category_zh" : "",
      "id" : "23f48a58c5b2fXXX162846076cd0"
    },
    "catalog_id" : "9378d1e8-XXX-4aae-XXX-c41cf6829ede",
    "checkitem_id" : "13fcc967-cb49-XXX-811a-9f72ce6ce8ac",
    "compliance_package_id" : "39488f96-XXX-4cc6-XXX-ad3c29b3a6c2",
    "create_time" : "2024-01-02T17:16:21.821Z+0800",
    "data_source" : {
      "company_name" : "xxx",
      "domain_id" : "ac7438b990efXXX004eb45e8bf4",
      "product_feature" : "SA",
      "product_module" : "Base-line",
      "product_name" : "SecMaster",
      "project_id" : "15645222XXX5c93dab6341da6",
      "region_id" : "xxx",
      "source_type" : 1
    },
    "dataclass_id" : "f846c8e0-XXX-3767-bcbf-f77190847f08",
    "domain_id" : "ac7438b990eXXXb741004eb45e8bf4",
    "domain_name" : "ac7438bXXX37b741004eb45e8bf4",
    "end_time" : "2024-01-03T11:28:51.701Z+0800",
    "execitem_id" : "ca2a1361-XXX-479c-XXX-d078e775a23a",
    "execitem_version" : 1,
    "first_observed_time" : "2024-01-03T11:28:51.565Z+0800",
    "handle_status" : "qualified",
    "id" : "f295575ab57XXX977d9be93ca9fe_13fcc967-XXX-494b-XXX-9f72ce6ce8ac",
    "is_deleted" : false,
```

```
    "last_observed_time" : "2024-01-03T11:28:51.701Z+0800",
    "method" : 1,
    "origin_id" : "",
    "project_id" : "15645222e8XXXa985c93dab6341da6",
    "region_id" : "xxx",
    "region_name" : "xxx",
    "resource" : {
      "domain_id" : "ac7438b99XXX1004eb45e8bf4",
      "id" : "f295575ab57bXXXd9be93ca9fe",
      "name" : "apigw_admin_trust_secmaster",
      "project_id" : "15645222e8XXX93dab6341da6",
      "provider" : "xxx",
      "region_id" : "xxx",
      "type" : "agency"
    },
    "severity" : "informational",
    "start_time" : "2024-01-03T11:28:51.565Z+0800",
    "task_id" : "10da8403-4955XXXd-a974-faXXX2a3a1",
    "title" : "Checking Agency Permissions for Project-Level Services",
    "trigger_flag" : false,
    "update_time" : "2024-01-03T11:28:52.023Z+0800",
    "workspace_id" : "1350a050-d09a-4XXX-9503-9cbfef116de7"
  },
  "dataclass_ref" : {
    "id" : "f846c8e0-cf0e-XXX-bcbf-XXX7f08"
  },
  "format_version" : 0,
  "id" : "f295575ab57b49XXXe93ca9fe_13fcc967-XXX-494b-XXX-9f72ce6ce8ac",
  "update_time" : "2024-01-03T19:28:52.023+08:00",
  "version" : 0
 } ],
 "page" : 0,
 "size" : 10,
 "success" : true,
 "total" : 2
}
```


Status code: 400

Request failed.


```
{
 "error_code" : "SecMaster.00040006",
 "error_msg" : "Invalid request parameters"
}
```


Status code: 401

Insufficient permissions.


```
{
 "error_code" : "SecMaster.90010015",
 "error_msg" : "Unauthorized request"
}
```


Status code: 500

Request failed.


```
{
 "error_code" : "SecMaster.00040011",
 "error_msg" : "Internal system error."
}
```


SDK Sample Code

The SDK sample code is as follows.

Java

Query the baseline inspection results. Time range: June 20, 2024 to June 27, 2024. Compliance package ID: 6add7d71-2261-4195-bab7-8ada0f0ed4d2. Directory ID: 0b78937f-4d9b-4223-9a46-2361e5090be0. Resource type: iam_user. The results are sorted in descending order of the update time. Each page contains 10 records.

```
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.secmaster.v2.region.SecMasterRegion;
import com.huaweicloud.sdk.secmaster.v2.*;
import com.huaweicloud.sdk.secmaster.v2.model.*;


public class SearchBaselineSolution {

    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);

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        SearchBaselineRequest request = new SearchBaselineRequest();
        request.withWorkspaceId("{workspace_id}");
        BaselineSearchRequestBody body = new BaselineSearchRequestBody();
        body.withCondition("{\"logics\":[\"compliance_package_id\",\"AND\",\"catalog_id\",\"AND\",\"resource.type\"],\"conditions\":[{\"data\":[\"compliance_package_id\",\"=\",\"6add7d71-2261-4195-bab7-8ada0f0ed4d2\"],\"name\":\"compliance_package_id\"},{\"data\":[\"catalog_id\",\"=\",\"0b78937f-4d9b-4223-9a46-2361e5090be0\"],\"name\":\"catalog_id\"},{\"data\":[\"resource.type\",\"=\",\"iam_user\"],\"name\":\"resource.type\"}]}");
        body.withToDate("2024-06-27T23:59:59.999Z");
        body.withFromDate("2024-06-20T00:00:00.000Z");
        body.withOrder("DESC");
        body.withSortBy("last_observed_time");
        body.withOffset(0);
        body.withLimit(10);
        request.withBody(body);
        try {
            SearchBaselineResponse response = client.searchBaseline(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 baseline inspection results. Time range: June 20, 2024 to June 27, 2024. Compliance package ID: 6add7d71-2261-4195-bab7-8ada0f0ed4d2. Directory ID: 0b78937f-4d9b-4223-9a46-2361e5090be0. Resource type: iam_user. The results are sorted in descending order of the update time. Each page contains 10 records.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdksecmaster.v2.region.secmaster_region import SecMasterRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdksecmaster.v2 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 = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = SearchBaselineRequest()
        request.workspace_id = "{workspace_id}"
        request.body = BaselineSearchRequestBody(
            condition="{\"logics\":[\"compliance_package_id\",\"AND\",\"catalog_id\",\"AND\",\"resource.type\"],\"conditions\":[{\"data\":[\"compliance_package_id\",\"=\",\"6add7d71-2261-4195-bab7-8ada0f0ed4d2\"],\"name\":\"compliance_package_id\"},{\"data\":[\"catalog_id\",\"=\",\"0b78937f-4d9b-4223-9a46-2361e5090be0\"],\"name\":\"catalog_id\"},{\"data\":[\"resource.type\",\"=\",\"iam_user\"],\"name\":\"resource.type\"}]}",
            to_date="2024-06-27T23:59:59.999Z",
            from_date="2024-06-20T00:00:00.000Z",
            order="DESC",
            sort_by="last_observed_time",
            offset=0,
            limit=10
        )
        response = client.search_baseline(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 baseline inspection results. Time range: June 20, 2024 to June 27, 2024. Compliance package ID: 6add7d71-2261-4195-bab7-8ada0f0ed4d2. Directory ID: 0b78937f-4d9b-4223-9a46-2361e5090be0. Resource type: iam_user. The results are sorted in descending order of the update time. Each page contains 10 records.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    secmaster "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/secmaster/v2/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 := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.SearchBaselineRequest{}
    request.WorkspaceId = "{workspace_id}"
    var conditionBaselineSearchRequestBody interface{} = "{\"logics\":[\"compliance_package_id\",\"AND\",\"catalog_id\",\"AND\",\"resource.type\"],\"conditions\":[{\"data\":[\"compliance_package_id\",\"=\",\"6add7d71-2261-4195-bab7-8ada0f0ed4d2\"],\"name\":\"compliance_package_id\"},{\"data\":[\"catalog_id\",\"=\",\"0b78937f-4d9b-4223-9a46-2361e5090be0\"],\"name\":\"catalog_id\"},{\"data\":[\"resource.type\",\"=\",\"iam_user\"],\"name\":\"resource.type\"}]}"
    toDateBaselineSearchRequestBody:= "2024-06-27T23:59:59.999Z"
    fromDateBaselineSearchRequestBody:= "2024-06-20T00:00:00.000Z"
    orderBaselineSearchRequestBody:= "DESC"
    sortByBaselineSearchRequestBody:= "last_observed_time"
    offsetBaselineSearchRequestBody:= int32(0)
    limitBaselineSearchRequestBody:= int32(10)
    request.Body = &model.BaselineSearchRequestBody{
        Condition: &conditionBaselineSearchRequestBody,
        ToDate: &toDateBaselineSearchRequestBody,
        FromDate: &fromDateBaselineSearchRequestBody,
        Order: &orderBaselineSearchRequestBody,
        SortBy: &sortByBaselineSearchRequestBody,
        Offset: &offsetBaselineSearchRequestBody,
        Limit: &limitBaselineSearchRequestBody,
    }
    response, err := client.SearchBaseline(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	Request failed.
401	Insufficient permissions.
500	Request failed.

Error Codes

See **Error Codes**.

A Appendix

A.1 Status Codes

- Normal

Status Code	Description
200	Request succeeded.
201	Request succeeded.

- Abnormal

Status Code	Status	Description
400	Bad Request	Parameter error.
401	Unauthorized	Authentication failed.
403	Forbidden	Access denied.
500	Internal Server Error	Internal server error.

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
400	SecMaster.11061001	alert process status error.
400	SecMaster.11061002	alert rule count out of range.
400	SecMaster.11061003	alert rule schedule out of range.

Status Code	Error Codes	Error Message
400	SecMaster.11061004	alert rule name already exist.
400	SecMaster.20010001	Invalid workspace ID.
400	SecMaster.20030001	Invalid parameters.
400	SecMaster.20030002	Invalid project ID.
400	SecMaster.20030003	Invalid name.
400	SecMaster.20030004	Failed to create the data object.
400	SecMaster.20030005	Failed to obtain the data object.
400	SecMaster.20030009	Invalid sorting field.
400	SecMaster.20030010	Invalid sorting.
400	SecMaster.20030011	Data object update error.
400	SecMaster.20030012	Data object deletion error.
400	SecMaster.20030013	Data object search error.
400	SecMaster.20030022	Failed to find one dataclass.
400	SecMaster.20030025	Failed to valid data object.
400	SecMaster.20039999	Unknown errors
400	SecMaster.20040000	Unknown Error.
400	SecMaster.20040402	Failed to query the data class.
400	SecMaster.20040516	The number of fields exceeds the maximum.
400	SecMaster.20041001	Invalid workspace ID.
400	SecMaster.20041002	Invalid parameters.
400	SecMaster.20041003	Invalid project ID.
400	SecMaster.20041031	Fail to get data object.
400	SecMaster.20041033	No associated data object is selected.
400	SecMaster.20041504	Failed to create the incident.
400	SecMaster.20041507	Failed to update the incident.
400	SecMaster.20041508	Failed to delete the incident.
400	SecMaster.20041509	The number of incidents created per day exceeds the upper limit.
400	SecMaster.20041804	Incorrect content included in the request for converting an alert to an incident.

Status Code	Error Codes	Error Message
400	SecMaster.20041805	Failed to create the alert.
400	SecMaster.20041808	Failed to update alert.
400	SecMaster.20041809	Failed to delete the alert.
400	SecMaster.20041810	The number of alerts created per day exceeds the upper limit.
400	SecMaster.20041811	The number of incidents transferred by alerts per day exceeds the upper limit.
400	SecMaster.20041903	Failed to find dataclass.
400	SecMaster.20041904	The indicator is not exist.
400	SecMaster.20041905	Failed to create indicator.
400	SecMaster.20041906	Failed to update indicator.
400	SecMaster.20041907	Failed to delete indicator.
400	SecMaster.20042501	The number of indicators created per day exceeds the upper limit.
400	SecMaster.20048001	The playbook cannot be deleted because it has a running instance or an activated version.
400	SecMaster.20048002	The playbook cannot be enabled because it does not have an activated version.
400	SecMaster.20048003	The playbook cannot be reviewed because it is in an incorrect state.
400	SecMaster.20048004	The resource does not exist.
400	SecMaster.20048005	The draft cannot be activated before it passes the review.
400	SecMaster.20048006	Incorrect playbook ID.
400	SecMaster.20048007	Incorrect playbook version ID.
400	SecMaster.20048008	Incorrect playbook action ID.
400	SecMaster.20048009	Incorrect playbook rule ID.
400	SecMaster.20048013	The playbook is being enabled. You cannot deactivate the version.
400	SecMaster.20048014	The playbook has been released and cannot be edited.
400	SecMaster.20048015	The playbook name must be unique.

Status Code	Error Codes	Error Message
400	SecMaster.20048016	Incorrect time range of the scheduled task.
400	SecMaster.20048017	Incorrect Corn expression of the scheduled task.
400	SecMaster.20048018	The number of versions has reached the upper limit.
400	SecMaster.20048019	A new version cannot be created because there is a version being reviewed.
400	SecMaster.20048020	Incorrect data object ID.
400	SecMaster.20048021	Invalid playbook search text.
400	SecMaster.20048022	The end time must be later than the start time.
400	SecMaster.20048023	Failed to register schedule job of playbook.
400	SecMaster.20048024	Failed to disable schedule job of playbook.
400	SecMaster.20048025	End time of the schedule playbook must be larger than start time.
400	SecMaster.20048026	End time of the schedule playbook is invalid.
400	SecMaster.20048027	The data class id of playbook is empty.
400	SecMaster.20048028	The matching process of playbook is not enabled. You cannot submit the version
400	SecMaster.20048029	Failed to convert data of playbook
400	SecMaster.20048030	The number of playbooks exceeds the limit.
400	SecMaster.20048031	The number of matching process exceeds the limit.
400	SecMaster.20048032	The scheduled interval of playbook is invalid.
400	SecMaster.20048033	The matching process of playbook can not be empty.
400	SecMaster.20048034	The dataclass of matching process is inconsistent with the dataclass of playbook.

Status Code	Error Codes	Error Message
400	SecMaster.20048035	The built-in playbook cannot be modified.
400	SecMaster.20048036	The built-in playbook cannot be deleted.

A.3 Obtaining a Project ID

Obtaining a Project ID by Calling an API

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

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

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

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

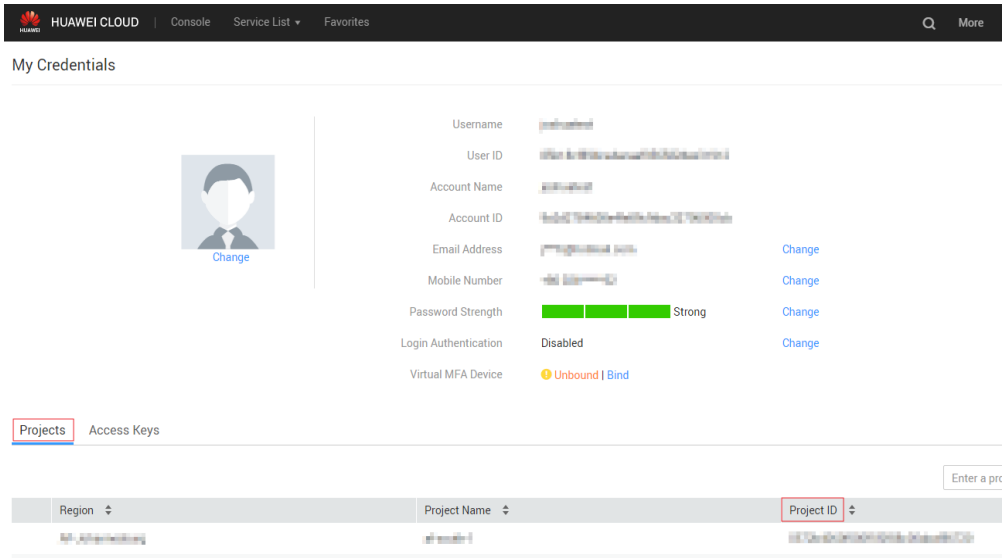
Obtaining a Project ID from the Console

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

1. Log in to the management console.
2. Click the username and choose **Basic Information** from the drop-down list.
3. On the **Account Info** page, click **Manage** next to **Security Credentials**.

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

Figure A-1 Viewing project IDs



A.4 About Metrics

Table A-1 Metric description

Metric	ID	Metric Description	Metric Parameter
Total assets	6f8d4892-713c-4d12-8584-dc04f7847b32	Total number of assets in the workspace	None
High-Risk Resources	a5597747-8cef-4342-9855-3fdaf00ad460	Total number of high-risk assets in the workspace	None
Number of assets at other risk levels	09ca4eb8-a4ca-4ef4-b75f-e9172f39393b	Total number of assets except high-risk assets in the workspace	None
Distribution of alerts by severity	1f0f5e29-5a92-17a5-2c16-5f37c6dc109c	Alert distribution by severity in the workspace from the specified start time to the current time	Set **params** to **start_date**, which indicates the start time of statistics collection. For example: "start_date": "2024-06-21T00:00:00.000+08:00"

Metric	ID	Metric Description	Metric Parameter
Distribution of vulnerabilities by severity	815c8a73-c855-fd29-63e2-b093d05a7ef0	Distribution of vulnerabilities at different severity levels in the workspace	None
Distribution of failed baseline check results	fee4d416-25b4-46c6-aa1b-851c7251e04b	Distribution of baseline check results at different levels for the past 30 days in the workspace	None
Security score trend	39d386dc-5868-adb6-a8e9-d5e92bb75663	Daily security scores for the last seven days in the workspace	None
Top 5 threat events	aaa6e851-601b-53c5-61ef-ffc95889ebf3	Top 5 threat alarm events in the workspace from the specified start time to the current time	Set **params** to **start_date**, which indicates the start time of statistics collection. For example: "start_date": "2024-06-21T00:00:00.000+08:00"
Workspace security score	cf6cce38-bc32-fd89-c0b5-3ba2cdf98eda	Latest security score in the workspace	None

