安全云脑

API 参考

文档版本 06

发布日期 2024-03-20

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 使用前必读

1.1 概述

安全云脑（SecMaster）是华为云原生的新一代安全运营中心，集华为云多年安全经验，基于云原生安全，提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力，实现提前预防风险、感知安全事件、安全事件自动化闭环。

您可以使用本文档提供的API对云上安全态势对进行相关操作，如查询、更新等。支持的全部操作请参见**API概览**。

在调用安全云脑API之前，请确保已经充分了解安全云脑相关概念，详细信息请参见**产品介绍**。

1.2 调用说明

安全云脑提供了REST（Representational State Transfer）风格API，支持您通过HTTPS请求调用，调用方法请参见**如何调用API**。

1.3 终端节点

终端节点（Endpoint）即调用API的**请求地址**，不同服务不同区域的终端节点不同，您可以从**地区和终端节点**中查询服务的终端节点。

1.4 基本概念

- 账号

  用户注册时的账号，账号对其所拥有的资源及云服务具有完全的访问权限，可以重置用户密码、分配用户权限等。由于账号是付费主体，为了确保账号安全，建议您不要直接使用账号进行日常管理工作，而是创建用户并使用他们进行日常管理工作。

- 用户

  由账号在IAM中创建的用户，是云服务的使用人员，具有身份凭证（密码和访问密钥）。

在**我的凭证**下，您可以查看账号ID和用户ID。通常在调用API的鉴权过程中，您需要用到账号、用户和密码等信息。

- 区域（Region）

  从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。

  详情请参见**区域和可用区**。

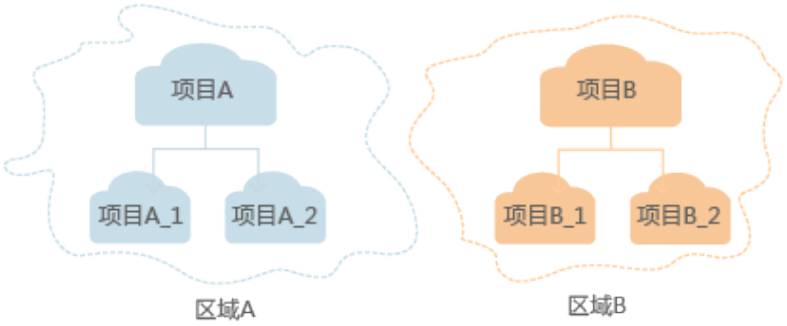
- 可用区（AZ，Availability Zone）

  一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

- 项目

  区域默认对应一个项目，这个项目由系统预置，用来隔离物理区域间的资源（计算资源、存储资源和网络资源），以默认项目为单位进行授权，用户可以访问您账号中该区域的所有资源。如果您希望进行更加精细的权限控制，可以在区域默认的项目中创建子项目，并在子项目中创建资源，然后以子项目为单位进行授权，使得用户仅能访问特定子项目中资源，使得资源的权限控制更加精确。

  图 1-1 项目隔离模型

- 企业项目

  企业项目是项目的升级版，针对企业不同项目间资源的分组和管理，是逻辑隔离。企业项目中可以包含多个区域的资源，且项目中的资源可以迁入迁出。

  关于企业项目ID的获取及企业项目特性的详细信息，请参见**企业管理服务用户指南**。

2 如何调用 API

2.1 构造请求

本节介绍如何构造REST API的请求，并以调用IAM服务的**获取用户Token**说明如何调用API，该API获取用户的Token，Token可以用于调用其他API时鉴权。

您还可以通过这个视频教程了解如何构造请求调用API：**https://bbs.huaweicloud.com/videos/102987**。

请求 URI

请求URI由如下部分组成。

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

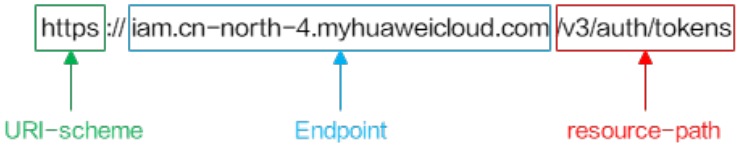
尽管请求URI包含在请求消息头中，但大多数语言或框架都要求您从请求消息中单独传递它，所以在此单独强调。

- **URI-scheme**：
  表示用于传输请求的协议，当前所有API均采用**HTTPS**协议。
- **Endpoint**：
  指定承载REST服务端点的服务器域名或IP，不同服务不同区域的Endpoint不同，您可以从**地区和终端节点**获取。
  例如IAM服务在“华北-北京四”区域的Endpoint为“iam.cn-north-4.myhuaweicloud.com”。
- **resource-path**：
  资源路径，也即API访问路径。从具体API的URI模块获取，例如“获取用户Token”API的resource-path为“/v3/auth/tokens”。
- **query-string**：
  查询参数，是可选部分，并不是每个API都有查询参数。查询参数前面需要带一个“？”，形式为“参数名=参数取值”，例如“limit=10”，表示查询不超过10条数据。

例如您需要获取IAM在“华北-北京四”区域的Token，则需使用“华北-北京四”区域的Endpoint（iam.cn-north-4.myhuaweicloud.com），并在**获取用户Token**的URI部分找到resource-path（/v3/auth/tokens），拼接起来如下所示。

```
https://iam.cn-north-4.myhuaweicloud.com/v3/auth/tokens
```

图 2-1 URI 示意图



说明

为查看方便，在每个具体API的URI部分，只给出resource-path部分，并将请求方法写在一起。这是因为URI-scheme都是HTTPS，同一个服务的Endpoint在同一个区域也相同，所以简洁起见将这两部分省略。

请求方法

HTTP请求方法（也称为操作或动词），它告诉服务你正在请求什么类型的操作。

- **GET**：请求服务器返回指定资源。
- **PUT**：请求服务器更新指定资源。
- **POST**：请求服务器新增资源或执行特殊操作。
- **DELETE**：请求服务器删除指定资源，如删除对象等。
- **HEAD**：请求服务器资源头部。
- **PATCH**：请求服务器更新资源的部分内容。当资源不存在的时候，PATCH可能会去创建一个新的资源。

在**获取用户Token**的URI部分，您可以看到其请求方法为“POST”，则其请求为：

```
POST https://iam.cn-north-4.myhuaweicloud.com/v3/auth/tokens
```

请求消息头

附加请求头字段，如指定的URI和HTTP方法所要求的字段。例如定义消息体类型的请求头“Content-Type”，请求鉴权信息等。

如下公共消息头需要添加到请求中。

- **Content-Type**：消息体的类型（格式），必选，默认取值为“application/json”，有其他取值时会在具体接口中专门说明。
- **X-Auth-Token**：用户Token，可选，当使用Token方式认证时，必须填充该字段。用户Token也就是调用**获取用户Token**接口的响应值，该接口是唯一不需要认证的接口。

  说明

  API同时支持使用AK/SK认证，AK/SK认证是使用SDK对请求进行签名，签名过程会自动往请求中添加Authorization（签名认证信息）和X-Sdk-Date（请求发送的时间）请求头。

  AK/SK认证的详细说明请参见**AK/SK认证**。

对于**获取用户Token**接口，由于不需要认证，所以只添加“Content-Type”即可，添加消息头后的请求如下所示。

```
POST https://iam.cn-north-4.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
```

请求消息体

请求消息体通常以结构化格式发出，与请求消息头中Content-type对应，传递除请求消息头之外的内容。若请求消息体中参数支持中文，则中文字符必须为UTF-8编码。

每个接口的请求消息体内容不同，也并不是每个接口都需要有请求消息体（或者说消息体为空），GET、DELETE操作类型的接口就不需要消息体，消息体具体内容需要根据具体接口而定。

对于**获取用户Token**接口，您可以从接口的请求部分看到所需的请求参数及参数说明。将消息体加入后的请求如下所示，加粗的斜体字段需要根据实际值填写，其中***username***为用户名，***domainname***为用户所属的账号名称，*********为用户登录密码，***xxxxxxxxxxxxxxxxxx***为project的名称，如“cn-north-4”，您可以从**地区和终端节点**获取，对应地区和终端节点页面的“区域”字段的值。

说明

scope参数定义了Token的作用域，下面示例中获取的Token仅能访问project下的资源。您还可以设置Token作用域为某个账号下所有资源或账号的某个project下的资源，详细定义请参见**获取用户Token**。

```
POST https://iam.cn-north-4.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxxxxxxxxxxxx"
            }
        }
    }
}
```

到这里为止这个请求需要的内容就具备齐全了，您可以使用**curl**、**Postman**或直接编写代码等方式发送请求调用API。对于获取用户Token接口，返回的响应消息头中“x-subject-token”就是需要获取的用户Token。有了Token之后，您就可以使用Token认证调用其他API。

2.2 认证鉴权

调用接口有如下两种认证方式，您可以选择其中一种进行认证鉴权。

- Token认证：通过Token认证调用请求。
- AK/SK认证：通过AK（Access Key ID）/SK（Secret Access Key）加密调用请求。推荐使用AK/SK认证，其安全性比Token认证要高。

Token 认证

> **说明**
>
> Token的有效期为24小时，需要使用一个Token鉴权时，可以先缓存起来，避免频繁调用。

Token在计算机系统中代表令牌（临时）的意思，拥有Token就代表拥有某种权限。Token认证就是在调用API的时候将Token加到请求消息头，从而通过身份认证，获得操作API的权限。

Token可通过调用**获取用户Token**接口获取，调用本服务API需要project级别的Token，即调用**获取用户Token**接口时，请求body中auth.scope的取值需要选择project，如下所示。

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

获取Token后，再调用其他接口时，您需要在请求消息头中添加“X-Auth-Token”，其值即为Token。例如Token值为“ABCDEFJ....”，则调用接口时将“X-Auth-Token: ABCDEFJ....”加到请求消息头即可，如下所示。

```
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

您还可以通过这个视频教程了解如何使用Token认证：**https://bbs.huaweicloud.com/videos/101333**。

AK/SK 认证

> **说明**
>
> AK/SK签名认证方式仅支持消息体大小12MB以内，12MB以上的请求请使用Token认证。

AK/SK认证就是使用AK/SK对请求进行签名，在请求时将签名信息添加到消息头，从而通过身份认证。

- AK(Access Key ID)：访问密钥ID。与私有访问密钥关联的唯一标识符；访问密钥ID和私有访问密钥一起使用，对请求进行加密签名。
- SK(Secret Access Key)：与访问密钥ID结合使用的密钥，对请求进行加密签名，可标识发送方，并防止请求被修改。

使用AK/SK认证时，您可以基于签名算法使用AK/SK对请求进行签名，也可以使用专门的签名SDK对请求进行签名。详细的签名方法和SDK使用方法请参见**API签名指南**。

须知

签名SDK只提供签名功能，与服务提供的SDK不同，使用时请注意。

2.3 返回结果

状态码

请求发送以后，您会收到响应，包含状态码、响应消息头和消息体。

状态码是一组从1xx到5xx的数字代码，状态码表示了请求响应的状态，完整的状态码列表请参见**状态码**。

对于**获取用户Token**接口，如果调用后返回状态码为“201”，则表示请求成功。

响应消息头

对应请求消息头，响应同样也有消息头，如“Content-type”。

对于**获取用户Token**接口，返回如**图2-2**所示的消息头，其中“x-subject-token”就是需要获取的用户Token。有了Token之后，您就可以使用Token认证调用其他API。

图 2-2 获取用户 Token 响应消息头

响应消息体（可选）

响应消息体通常以结构化格式返回，与响应消息头中Content-type对应，传递除响应消息头之外的内容。

对于**获取用户Token**接口，返回如下消息体。为篇幅起见，这里只展示部分内容。

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

当接口调用出错时，会返回错误码及错误信息说明，错误响应的Body体格式如下所示。

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

其中，error_code表示错误码，error_msg表示错误描述信息。

3 API 概览

通过使用安全云脑提供的接口，您可以完整的使用安全云脑的所有功能。

类型	说明
告警规则API接口	告警规则的接口，包括创建、删除、查看、启用等接口。
告警API接口	告警的接口，包括创建、删除、转事件等接口。
关系API接口	关系的接口，包括查询、创建、删除等接口。
事件API接口	事件的接口，包括创建、更新、获取等接口。
指标API接口	指标的接口，包括查询、创建、删除等接口。
剧本API接口	剧本的接口，包括查询、创建、修改等接口。
剧本版本API接口	剧本版本的接口，包括查询、创建、更新等接口。
剧本审核API接口	剧本审核的接口，包括审核剧本、查询剧本审核结果的接口。
剧本规则API接口	剧本规则的接口，包括创建、查询、删除等接口。
剧本动作API接口	剧本动作的接口，包括查询、创建、更新等接口。
剧本实例API接口	剧本实例的接口，包括查询、操作等接口。

4 API

4.1 告警管理

4.1.1 搜索告警列表

功能介绍

搜索告警列表

调用方法

请参见**如何调用API**。

URI

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

表 4-1 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**

请求参数

表 4-2 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

表 4-3 请求 Body 参数

参数	是否必选	参数类型	描述
limit	否	Integer	分页大小 最小值：**0** 最大值：**1000**
offset	否	Integer	偏移量 最小值：**0** 最大值：**1000**
sort_by	否	String	排序字段：create_time | update_time 最小长度：**0** 最大长度：**1000**
order	否	String	排序方式：DESC | ASC 最小长度：**0** 最大长度：**1000** 枚举值： • **DESC** • **ASC**
from_date	否	String	搜索开始时间，例如：2023-02-20T00:00:00.000Z 最小长度：**0** 最大长度：**64**

参数	是否必选	参数类型	描述
to_date	否	String	搜索结束时间，例如：2023-02-27T23:59:59.999Z 最小长度：**0** 最大长度：**64**
condition	否	**condition** object	搜索条件表达式

表 4-4 condition

参数	是否必选	参数类型	描述
conditions	否	Array of **conditions** objects	表达式列表 数组长度：**0 - 999**
logics	否	Array of strings	表达式名称列表 最小长度：**0** 最大长度：**100** 数组长度：**0 - 999**

表 4-5 conditions

参数	是否必选	参数类型	描述
name	否	String	表达式名称 最小长度：**0** 最大长度：**64**
data	否	Array of strings	表达式内容列表 最小长度：**0** 最大长度：**100** 数组长度：**0 - 999**

响应参数

状态码： 200

表 4-6 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-7 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误信息 最小长度：**0** 最大长度：**1024**
total	Integer	告警总数 最小值：**0** 最大值：**10000**
limit	Integer	分页大小 最小值：**0** 最大值：**10000**
offset	Integer	偏移量 最小值：**0** 最大值：**10000**
success	Boolean	是否成功
data	Array of **ListAlertDetail** objects	告警列表 数组长度：**0 - 10000**

表 4-8 ListAlertDetail

参数	参数类型	描述
data_object	**ListAlertRsp** object	告警详情
create_time	String	Create time 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
update_time	String	Update time 最小长度：**0** 最大长度：**64**
project_id	String	Id value 最小长度：**32** 最大长度：**64**
workspace_id	String	Id value 最小长度：**32** 最大长度：**64**
id	String	The name, display only 最小长度：**0** 最大长度：**1024**
type	String	The name, display only 最小长度：**0** 最大长度：**1024**
version	Integer	The name, display only 最小值：**0** 最大值：**1024**
format_version	Integer	The name, display only 最小值：**0** 最大值：**1024**
dataclass_ref	**dataclass_ref** object	dataclass对象

表 4-9 ListAlertRsp

参数	参数类型	描述
version	String	版本 最小长度：**1** 最大长度：**64**
environment	**environment** object	环境信息
data_source	**data_source** object	数据源信息

参数	参数类型	描述
first_observed_time	String	Update time 最小长度：**0** 最大长度：**64**
last_observed_time	String	Update time 最小长度：**0** 最大长度：**64**
create_time	String	Create time 最小长度：**0** 最大长度：**64**
arrive_time	String	Update time 最小长度：**0** 最大长度：**64**
title	String	The name, display only 最小长度：**0** 最大长度：**1024**
description	String	The description, display only 最小长度：**0** 最大长度：**1024**
source_url	String	事件URL链接 最小长度：**1** 最大长度：**64**
count	Integer	事件发生次数 最小值：**0** 最大值：**5**
confidence	Integer	置信度 最小值：**0** 最大值：**5**
severity	String	严重性等级 最小长度：**1** 最大长度：**64**
criticality	Integer	关键性，是指事件涉及的资源的重要性级别。 最小值：**0** 最大值：**5**
alert_type	Object	事件分类

参数	参数类型	描述
network_list	Array of **network_list** objects	network_list 数组长度：**0 - 100**
resource_list	Array of **resource_list** objects	network_list 数组长度：**0 - 100**
remediation	**remediation** object	补救措施
verification_state	String	验证状态 最小长度：**1** 最大长度：**64**
handle_status	String	事件处理状态 最小长度：**1** 最大长度：**64**
sla	String	sla 最小长度：**1** 最大长度：**64**
update_time	String	Create time 最小长度：**0** 最大长度：**64**
close_time	String	Create time 最小长度：**0** 最大长度：**64**
chop_phase	String	周期/处置阶段编号 最小长度：**4** 最大长度：**64**
ipdrr_phase	String	周期/处置阶段编号 最小长度：**4** 最大长度：**64**
ppdr_phase	String	周期/处置阶段编号 最小长度：**4** 最大长度：**64**
simulation	String	是否为调试事件. 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
actor	String	委托人 最小长度：**0** 最大长度：**64**
owner	String	The name, display only 最小长度：**0** 最大长度：**1024**
creator	String	The name, display only 最小长度：**0** 最大长度：**1024**
close_reason	String	关闭原因 最小长度：**32** 最大长度：**64**
close_comment	String	关闭原因 最小长度：**0** 最大长度：**64**
malware	**malware** object	恶意软件
system_info	Object	系统信息
process	Array of **process** objects	进程信息 数组长度：**0 - 100**
user_info	Array of **user_info** objects	用户信息 数组长度：**0 - 100**
file_info	Array of **file_info** objects	文件信息 数组长度：**0 - 100**
system_alert_table	Object	系统信息
id	String	Id value 最小长度：**32** 最大长度：**64**
workspace_id	String	workspace id 最小长度：**32** 最大长度：**64**

表 4-10 environment

参数	参数类型	描述
vendor_type	String	The name, display only 最小长度：**0** 最大长度：**1024**
domain_id	String	Id value 最小长度：**32** 最大长度：**64**
region_id	String	Id value 最小长度：**1** 最大长度：**64**
project_id	String	Id value 最小长度：**32** 最大长度：**64**

表 4-11 data_source

参数	参数类型	描述
source_type	Integer	current page count 最小值：**0** 最大值：**9999**
domain_id	String	Id value 最小长度：**32** 最大长度：**64**
project_id	String	Id value 最小长度：**32** 最大长度：**64**
region_id	String	Id value 最小长度：**1** 最大长度：**64**

表 4-12 network_list

参数	参数类型	描述
direction	Object	方向，取值范围：IN | OUT

参数	参数类型	描述
protocol	String	协议，参考：IANA registered name 最小长度：**1** 最大长度：**64**
src_ip	String	源IP地址 最小长度：**0** 最大长度：**64**
src_port	Integer	源端口，0–65535 最小值：**0** 最大值：**65535**
src_domain	String	源域名，最大128个字符 最小长度：**0** 最大长度：**128**
dest_ip	String	目的IP地址 最小长度：**0** 最大长度：**64**
dest_port	String	目的端口，0–65535 最小长度：**0** 最大长度：**64**
dest_domain	String	目的域名，最大128个字符 最小长度：**0** 最大长度：**128**
src_geo	Object	源IP的地理位置信息
dest_geo	Object	目的IP的地理位置信息

表 4-13 resource_list

参数	参数类型	描述
id	String	Id value 最小长度：**32** 最大长度：**64**
name	String	The name, display only 最小长度：**0** 最大长度：**1024**

参数	参数类型	描述
type	String	The name, display only 最小长度：**0** 最大长度：**1024**
domain_id	String	Id value 最小长度：**32** 最大长度：**64**
project_id	String	Id value 最小长度：**32** 最大长度：**64**
region_id	String	Id value 最小长度：**0** 最大长度：**64**
ep_id	String	Id value 最小长度：**0** 最大长度：**64**
ep_name	String	The name, display only 最小长度：**0** 最大长度：**1024**
tags	String	Id value 最小长度：**0** 最大长度：**64**

表 4-14 remediation

参数	参数类型	描述
recommendation	String	The name, display only 最小长度：**0** 最大长度：**1024**
url	String	The name, display only 最小长度：**0** 最大长度：**1024**

表 4-15 malware

参数	参数类型	描述
malware_family	String	恶意家族 最小长度：**0** 最大长度：**64**
malware_class	String	恶意软件分类 最小长度：**0** 最大长度：**64**

表 4-16 process

参数	参数类型	描述
process_name	String	The name, display only 最小长度：**0** 最大长度：**1024**
process_path	String	The name, display only 最小长度：**0** 最大长度：**1024**
process_pid	Integer	Id value 最小值：**0** 最大值：**65535**
process_uid	Integer	Id value 最小值：**0** 最大值：**65535**
process_cmdline	String	The name, display only 最小长度：**0** 最大长度：**1024**

表 4-17 user_info

参数	参数类型	描述
user_id	String	Id value 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
user_name	String	The name, display only 最小长度：**0** 最大长度：**1024**

表 4-18 file_info

参数	参数类型	描述
file_path	String	The name, display only 最小长度：**0** 最大长度：**1024**
file_content	String	The name, display only 最小长度：**0** 最大长度：**1024**
file_new_path	String	The name, display only 最小长度：**0** 最大长度：**1024**
file_hash	String	The name, display only 最小长度：**0** 最大长度：**1024**
file_md5	String	The name, display only 最小长度：**0** 最大长度：**1024**
file_sha256	String	The name, display only 最小长度：**0** 最大长度：**1024**
file_attr	String	The name, display only 最小长度：**0** 最大长度：**1024**

表 4-19 dataclass_ref

参数	参数类型	描述
id	String	Id value 最小长度：**32** 最大长度：**64**

参数	参数类型	描述
name	String	The name, display only 最小长度：**0** 最大长度：**1024**

状态码： 400

表 4-20 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-21 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

查询告警列表请求样例，查询2024年1月20号到2024年1月26号，告警等级为中危且处理状态为打开的告警，按照创建时间降序排序，返回第一页，每页10条数据

```
{
  "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"
}
```

响应示例

状态码： 200

搜索告警列表返回body体


```
{
  "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,
      "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 – 未知，True_Positive – 确认，False_Positive – 误报。默认填写
Unknown",
    "handle_status" : "Open – 打开，Block – 阻塞，Closed – 关闭。默认填写Open",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-
Activity",
    "simulation" : "false",
    "actor" : "刘一博",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "误检;已解决;重复;其他",
    "close_comment" : "误检;已解决;重复;其他",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "恶意占用内存"
    },
    "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 代码示例

SDK代码示例如下。

Java

查询告警列表请求样例，查询2024年1月20号到2024年1月26号，告警等级为中危且处理状态为打开的告警，按照创建时间降序排序，返回第一页，每页10条数据

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListAlertsRequest request = new ListAlertsRequest();
        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

查询告警列表请求样例，查询2024年1月20号到2024年1月26号，告警等级为中危且处理状态为打开的告警，按照创建时间降序排序，返回第一页，每页10条数据

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListAlertsRequest()
        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

查询告警列表请求样例，查询2024年1月20号到2024年1月26号，告警等级为中危且处理状态为打开的告警，按照创建时间降序排序，返回第一页，每页10条数据

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAlertsRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	搜索告警列表返回body体
400	搜索告警列表错误返回body体

错误码

请参见**错误码**。

4.1.2 创建告警

功能介绍

创建告警

调用方法

请参见**如何调用API**。

URI

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

表 4-22 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**

请求参数

表 4-23 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

表 4-24 请求 Body 参数

参数	是否必选	参数类型	描述
data_object	是	**Alert** object	告警实体信息

表 4-25 Alert

参数	是否必选	参数类型	描述
version	否	String	告警对象的版本，该字段的值必须为华为云SSA服务确定的官方发布版本之一 最小长度：**0** 最大长度：**64**
id	否	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
domain_id	否	String	数据投递后，被委托用户的domain_id 最小长度：**0** 最大长度：**36**
region_id	否	String	数据投递后，被委托用户的region_id 最小长度：**0** 最大长度：**36**
workspace_id	否	String	当前的工作空间id 最小长度：**0** 最大长度：**36**
labels	否	String	标签，仅展示 最小长度：**0** 最大长度：**1024**
environment	否	**environment** object	告警产生的环境坐标信息
data_source	否	**data_source** object	首次上报数据源

参数	是否必选	参数类型	描述
first_observed_time	否	String	首次发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
last_observed_time	否	String	最近发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
create_time	否	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
arrive_time	否	String	接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
title	否	String	告警标题 最小长度：**0** 最大长度：**255**
description	否	String	告警描述信息 最小长度：**0** 最大长度：**1024**
source_url	否	String	告警URL链接，指向数据源产品中有关当前事件说明的页面 最小长度：**0** 最大长度：**1024**

参数	是否必选	参数类型	描述
count	否	Integer	事件发生次数 最小值：**0** 最大值：**999**
confidence	否	Integer	事件的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100，0表示置信度为0%，100表示置信度为100% 最小值：**0** 最大值：**100**
severity	否	String	严重性等级，取值范围：Tips | Low | Medium | High | Fatal 说明： 0: Tips – 未发现任何问题。 1: Low – 无需针对问题执行任何操作。 2: Medium – 问题需要处理，但不紧急。 3: High – 问题必须优先处理。 4: Fatal – 问题必须立即处理，以防止产生进一步的损害 最小长度：**3** 最大长度：**6** 枚举值： • **Tips** • **Low** • **Medium** • **High** • **Fatal**
criticality	否	Integer	关键性，是指事件涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源 最小值：**0** 最大值：**100**
alert_type	否	**alert_type** object	告警分类，详细定义参考《告警类型定义》
network_list	否	Array of **network_list** objects	网络信息 数组长度：**0 - 999**
resource_list	否	Array of **resource_list** objects	受影响资源 数组长度：**0 - 999**

参数	是否必选	参数类型	描述
remediation	否	**remediation** object	补救措施
verification_state	否	String	验证状态，标识事件的准确性。可选类型如下： Unknown – 未知 True_Positive – 确认 False_Positive – 误报 默认填写 Unknown 最小长度：**32** 最大长度：**64** 枚举值： • **Unknown** • **True_Positive** • **False_Positive**
handle_status	否	String	事件处理状态，可选类型如下：Open – 打开，默认 Block – 阻塞 Closed – 关闭 默认填写 Open 最小长度：**4** 最大长度：**5** 枚举值： • **Open** • **Block** • **Closed**
sla	否	Integer	约束闭环时间：设置风险接受持续时间。单位：小时 最小值：**0** 最大值：**999**
update_time	否	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
close_time	否	String	关闭时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	是否必选	参数类型	描述
ipdrr_phase	否	String	周期/处置阶段编号 Prepartion| Detection and Analysis| Containm，Eradication& Recovery|Post-Incident-Activity 最小长度：**0** 最大长度：**64** 枚举值： • **Prepartion** • **Detection and Analysis** • **Containm，Eradication& Recovery** • **Post-Incident-Activity**
simulation	否	String	调试字段 最小长度：**0** 最大长度：**64**
actor	否	String	告警调查员 最小长度：**0** 最大长度：**64**
owner	否	String	责任人、服务责任人 最小长度：**0** 最大长度：**64**
creator	否	String	创建人 最小长度：**0** 最大长度：**64**
close_reason	否	String	关闭原因: 误检 - False detection 已解决 - Resolved 重复 - Repeated 其他 - Other 最小长度：**0** 最大长度：**64** 枚举值： • **False detection** • **Resolved** • **Repeated** • **Other**
close_comment	否	String	关闭评论 最小长度：**0** 最大长度：**1024**

参数	是否必选	参数类型	描述
malware	否	**malware** object	恶意软件
system_info	否	Object	系统信息
process	否	Array of **process** objects	进程信息 数组长度：**0 - 999**
user_info	否	Array of **user_info** objects	用户信息 数组长度：**0 - 999**
file_info	否	Array of **file_info** objects	文件信息 数组长度：**0 - 999**
system_alert_table	否	Object	告警管理列表的布局字段

表 4-26 environment

参数	是否必选	参数类型	描述
vendor_type	否	String	环境供应商：HWCP/HWC/AWS/Azure/GCP 最小长度：**0** 最大长度：**64**
domain_id	否	String	租户id 最小长度：**0** 最大长度：**64**
region_id	否	String	区域od，全局服务global 最小长度：**0** 最大长度：**64**
cross_workspace_id	否	String	数据投递前的源工作空间id，在源空间下值为null，投递后为被委托用户的id 最小长度：**0** 最大长度：**64**
project_id	否	String	项目id， 全局服务默认null 最小长度：**0** 最大长度：**64**

表 4-27 data_source

参数	是否必选	参数类型	描述
source_type	否	Integer	数据源类型，取值范围如下： 1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**1** 最大值：**3** 枚举值： • **1** • **2** • **3**
domain_id	否	String	数据源产品所属账号的id 最小长度：**0** 最大长度：**36**
project_id	否	String	数据源产品所属项目的id 最小长度：**0** 最大长度：**64**
region_id	否	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义，例如cn-north-1 最小长度：**0** 最大长度：**64**
company_name	否	String	数据源产品所属公司的名称 最小长度：**0** 最大长度：**16**
product_name	否	String	数据源产品的名称 最小长度：**0** 最大长度：**24**
product_feature	否	String	产品功能特性名称，用来指明检测到当前事件的产品的功能特性 最小长度：**0** 最大长度：**24**
product_module	否	String	检测模块列表 最小长度：**0** 最大长度：**1024**

表 4-28 alert_type

参数	是否必选	参数类型	描述
category	否	String	类别 最小长度：**0** 最大长度：**1024**
alert_type	否	String	告警类型 最小长度：**0** 最大长度：**1024**

表 4-29 network_list

参数	是否必选	参数类型	描述
direction	否	String	方向，取值范围：IN | OUT 最小长度：**0** 最大长度：**3** 枚举值： • **IN** • **OUT**
protocol	否	String	协议，包含7层和4层的协议 参考：IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml 最小长度：**0** 最大长度：**64**
src_ip	否	String	源IP地址 最小长度：**0** 最大长度：**64**
src_port	否	Integer	源端口，0–65535 最小值：**0** 最大值：**65535**
src_domain	否	String	源域名 最小长度：**0** 最大长度：**128**
src_geo	否	**src_geo** object	源IP的地理位置信息

参数	是否必选	参数类型	描述
dest_ip	否	String	目的IP地址 最小长度：**32** 最大长度：**64**
dest_port	否	String	目的端口，0–65535 最小长度：**0** 最大长度：**65535**
dest_domain	否	String	目的域名 最小长度：**0** 最大长度：**128**
dest_geo	否	**dest_geo** object	目标IP的地理位置信息

表 4-30 src_geo

参数	是否必选	参数类型	描述
latitude	否	Number	纬度 最小值：**0** 最大值：**90**
longitude	否	Number	经度 最小值：**0** 最大值：**180**
city_code	否	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	否	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-31 dest_geo

参数	是否必选	参数类型	描述
latitude	否	Number	纬度 最小值：**0** 最大值：**90**

参数	是否必选	参数类型	描述
longitude	否	Number	经度 最小值：**0** 最大值：**180**
city_code	否	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	否	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-32 resource_list

参数	是否必选	参数类型	描述
id	否	String	云服务资源id 最小长度：**0** 最大长度：**36**
name	否	String	资源名称 最小长度：**0** 最大长度：**255**
type	否	String	资源类型；引用华为云RMS type字段 最小长度：**0** 最大长度：**64**
provider	否	String	云服务名称；引用华为云RMS provider字段 最小长度：**0** 最大长度：**64**
region_id	否	String	区域；按照华为云regionId填写，如cn-north-1等 最小长度：**0** 最大长度：**36**
domain_id	否	String	资源所属账号ID，UUID格式 最小长度：**0** 最大长度：**36**

参数	是否必选	参数类型	描述
project_id	否	String	资源所属项目ID，UUID格式 最小长度：**0** 最大长度：**36**
ep_id	否	String	企业项目id 最小长度：**0** 最大长度：**128**
ep_name	否	String	企业项目名称 最小长度：**0** 最大长度：**128**
tags	否	String	资源标签 1、最多50个key/values对 2、values：最大255字符，取值范围：字母数字,空格,+, -, =, ., _, :, /,@ 最小长度：**0** 最大长度：**2048**

表 4-33 remediation

参数	是否必选	参数类型	描述
recommendation	否	String	推荐处理方法 最小长度：**0** 最大长度：**128**
url	否	String	链接，指向该事件的一般修复信息。该URL必须可以从公网访问，不需要提供凭证 最小长度：**0** 最大长度：**2048**

表 4-34 malware

参数	是否必选	参数类型	描述
malware_family	否	String	恶意家族 最小长度：**0** 最大长度：**64**
malware_class	否	String	恶意软件分类 最小长度：**0** 最大长度：**64**

表 4-35 process

参数	是否必选	参数类型	描述
process_name	否	String	进程名 最小长度：**0** 最大长度：**64**
process_path	否	String	进程执行文件路径 最小长度：**0** 最大长度：**512**
process_pid	否	Integer	进程id 最小值：**0** 最大值：**65535**
process_uid	否	Integer	进程用户id 最小值：**0** 最大值：**655350**
process_cmdline	否	String	进程命令行 最小长度：**0** 最大长度：**128**
process_parent_name	否	String	父进程名称 最小长度：**0** 最大长度：**64**
process_parent_path	否	String	父进程执行文件路径 最小长度：**0** 最大长度：**512**
process_parent_pid	否	Integer	父进程id 最小值：**0** 最大值：**65535**
process_parent_uid	否	Integer	父进程用户id 最小值：**0** 最大值：**655350**
process_parent_cmdline	否	String	父进程命令行 最小长度：**0** 最大长度：**128**
process_child_name	否	String	子进程名称 最小长度：**0** 最大长度：**64**

参数	是否必选	参数类型	描述
process_child_path	否	String	子进程执行文件路径 最小长度：**0** 最大长度：**512**
process_child_pid	否	Integer	子进程id 最小值：**0** 最大值：**65535**
process_child_uid	否	Integer	子进程用户id 最小值：**0** 最大值：**655350**
process_child_cmdline	否	String	子进程命令行 最小长度：**0** 最大长度：**128**
process_launche_time	否	String	进程启动时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
process_terminate_time	否	String	进程结束时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

表 4-36 user_info

参数	是否必选	参数类型	描述
user_id	否	String	用户uid 最小长度：**0** 最大长度：**36**
user_name	否	String	用户名称 最小长度：**32** 最大长度：**64**

表 4-37 file_info

参数	是否必选	参数类型	描述
file_path	否	String	文件路径/名称 最小长度：**0** 最大长度：**128**
file_content	否	String	文件内容 最小长度：**0** 最大长度：**1024**
file_new_path	否	String	文件新路径/名称 最小长度：**32** 最大长度：**64**
file_hash	否	String	文件hash 最小长度：**0** 最大长度：**128**
file_md5	否	String	文件md5 最小长度：**0** 最大长度：**128**
file_sha256	否	String	文件sha256 最小长度：**0** 最大长度：**128**
file_attr	否	String	文件属性 最小长度：**0** 最大长度：**1024**

响应参数

状态码： 200

表 4-38 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-39 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误信息 最小长度：**0** 最大长度：**1024**
data	**AlertDetail** object	

表 4-40 AlertDetail

参数	参数类型	描述
create_time	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
data_object	**Alert** object	告警实体信息
dataclass_ref	**dataclass_ref** object	数据类对象
format_version	Integer	格式版本 最小值：**0** 最大值：**999**
id	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
project_id	String	当前项目的id 最小长度：**0** 最大长度：**64**
update_time	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	参数类型	描述
version	Integer	版本 最小值：**0** 最大值：**999**
workspace_id	String	当前的工作空间id 最小长度：**0** 最大长度：**36**

表 4-41 Alert

参数	参数类型	描述
version	String	告警对象的版本，该字段的值必须为华为云SSA服务确定的官方发布版本之一 最小长度：**0** 最大长度：**64**
id	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
domain_id	String	数据投递后，被委托用户的domain_id 最小长度：**0** 最大长度：**36**
region_id	String	数据投递后，被委托用户的region_id 最小长度：**0** 最大长度：**36**
workspace_id	String	当前的工作空间id 最小长度：**0** 最大长度：**36**
labels	String	标签，仅展示 最小长度：**0** 最大长度：**1024**
environment	**environment** object	告警产生的环境坐标信息
data_source	**data_source** object	首次上报数据源

参数	参数类型	描述
first_observed_time	String	首次发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
last_observed_time	String	最近发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
create_time	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
arrive_time	String	接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
title	String	告警标题 最小长度：**0** 最大长度：**255**
description	String	告警描述信息 最小长度：**0** 最大长度：**1024**
source_url	String	告警URL链接，指向数据源产品中有关当前事件说明的页面 最小长度：**0** 最大长度：**1024**
count	Integer	事件发生次数 最小值：**0** 最大值：**999**

参数	参数类型	描述
confidence	Integer	事件的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100，0表示置信度为0%，100表示置信度为100% 最小值：**0** 最大值：**100**
severity	String	严重性等级，取值范围：Tips | Low | Medium | High | Fatal 说明： 0: Tips – 未发现任何问题。 1: Low – 无需针对问题执行任何操作。 2: Medium – 问题需要处理，但不紧急。 3: High – 问题必须优先处理。 4: Fatal – 问题必须立即处理，以防止产生进一步的损害 最小长度：**3** 最大长度：**6** 枚举值： • **Tips** • **Low** • **Medium** • **High** • **Fatal**
criticality	Integer	关键性，是指事件涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源 最小值：**0** 最大值：**100**
alert_type	**alert_type** object	告警分类，详细定义参考《告警类型定义》
network_list	Array of **network_list** objects	网络信息 数组长度：**0 - 999**
resource_list	Array of **resource_list** objects	受影响资源 数组长度：**0 - 999**
remediation	**remediation** object	补救措施

参数	参数类型	描述
verification_state	String	验证状态，标识事件的准确性。可选类型如下：Unknown – 未知 True_Positive – 确认 False_Positive – 误报 默认填写Unknown 最小长度：**32** 最大长度：**64** 枚举值： • **Unknown** • **True_Positive** • **False_Positive**
handle_status	String	事件处理状态，可选类型如下： Open – 打开，默认 Block – 阻塞 Closed – 关闭 默认填写Open 最小长度：**4** 最大长度：**5** 枚举值： • **Open** • **Block** • **Closed**
sla	Integer	约束闭环时间：设置风险接受持续时间。单位：小时 最小值：**0** 最大值：**999**
update_time	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
close_time	String	关闭时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	参数类型	描述
ipdrr_phase	String	周期/处置阶段编号 Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-Activity 最小长度：**0** 最大长度：**64** 枚举值： • **Prepartion** • **Detection and Analysis** • **Containm，Eradication& Recovery** • **Post-Incident-Activity**
simulation	String	调试字段 最小长度：**0** 最大长度：**64**
actor	String	告警调查员 最小长度：**0** 最大长度：**64**
owner	String	责任人、服务责任人 最小长度：**0** 最大长度：**64**
creator	String	创建人 最小长度：**0** 最大长度：**64**
close_reason	String	关闭原因: 误检 - False detection 已解决 - Resolved 重复 - Repeated 其他 - Other 最小长度：**0** 最大长度：**64** 枚举值： • **False detection** • **Resolved** • **Repeated** • **Other**
close_comment	String	关闭评论 最小长度：**0** 最大长度：**1024**
malware	**malware** object	恶意软件
system_info	Object	系统信息

参数	参数类型	描述
process	Array of **process** objects	进程信息 数组长度：**0 - 999**
user_info	Array of **user_info** objects	用户信息 数组长度：**0 - 999**
file_info	Array of **file_info** objects	文件信息 数组长度：**0 - 999**
system_alert_table	Object	告警管理列表的布局字段

表 4-42 environment

参数	参数类型	描述
vendor_type	String	环境供应商：HWCP/HWC/AWS/Azure/GCP 最小长度：**0** 最大长度：**64**
domain_id	String	租户id 最小长度：**0** 最大长度：**64**
region_id	String	区域od，全局服务global 最小长度：**0** 最大长度：**64**
cross_workspace_id	String	数据投递前的源工作空间id，在源空间下值为null，投递后为被委托用户的id 最小长度：**0** 最大长度：**64**
project_id	String	项目id， 全局服务默认null 最小长度：**0** 最大长度：**64**

表 4-43 data_source

参数	参数类型	描述
source_type	Integer	数据源类型，取值范围如下： 1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**1** 最大值：**3** 枚举值： • **1** • **2** • **3**
domain_id	String	数据源产品所属账号的id 最小长度：**0** 最大长度：**36**
project_id	String	数据源产品所属项目的id 最小长度：**0** 最大长度：**64**
region_id	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义，例如cn-north-1 最小长度：**0** 最大长度：**64**
company_name	String	数据源产品所属公司的名称 最小长度：**0** 最大长度：**16**
product_name	String	数据源产品的名称 最小长度：**0** 最大长度：**24**
product_feature	String	产品功能特性名称，用来指明检测到当前事件的产品的功能特性 最小长度：**0** 最大长度：**24**
product_module	String	检测模块列表 最小长度：**0** 最大长度：**1024**

表 4-44 alert_type

参数	参数类型	描述
category	String	类别 最小长度：**0** 最大长度：**1024**
alert_type	String	告警类型 最小长度：**0** 最大长度：**1024**

表 4-45 network_list

参数	参数类型	描述
direction	String	方向，取值范围：IN | OUT 最小长度：**0** 最大长度：**3** 枚举值： • **IN** • **OUT**
protocol	String	协议，包含7层和4层的协议 参考：IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml 最小长度：**0** 最大长度：**64**
src_ip	String	源IP地址 最小长度：**0** 最大长度：**64**
src_port	Integer	源端口，0–65535 最小值：**0** 最大值：**65535**
src_domain	String	源域名 最小长度：**0** 最大长度：**128**
src_geo	**src_geo** object	源IP的地理位置信息

参数	参数类型	描述
dest_ip	String	目的IP地址 最小长度：**32** 最大长度：**64**
dest_port	String	目的端口，0–65535 最小长度：**0** 最大长度：**65535**
dest_domain	String	目的域名 最小长度：**0** 最大长度：**128**
dest_geo	**dest_geo** object	目标IP的地理位置信息

表 4-46 src_geo

参数	参数类型	描述
latitude	Number	纬度 最小值：**0** 最大值：**90**
longitude	Number	经度 最小值：**0** 最大值：**180**
city_code	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-47 dest_geo

参数	参数类型	描述
latitude	Number	纬度 最小值：**0** 最大值：**90**

参数	参数类型	描述
longitude	Number	经度 最小值：**0** 最大值：**180**
city_code	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-48 resource_list

参数	参数类型	描述
id	String	云服务资源id 最小长度：**0** 最大长度：**36**
name	String	资源名称 最小长度：**0** 最大长度：**255**
type	String	资源类型；引用华为云RMS type字段 最小长度：**0** 最大长度：**64**
provider	String	云服务名称；引用华为云RMS provider字段 最小长度：**0** 最大长度：**64**
region_id	String	区域；按照华为云regionId填写，如cn-north-1等 最小长度：**0** 最大长度：**36**
domain_id	String	资源所属账号ID，UUID格式 最小长度：**0** 最大长度：**36**
project_id	String	资源所属项目ID，UUID格式 最小长度：**0** 最大长度：**36**

参数	参数类型	描述
ep_id	String	企业项目id 最小长度：**0** 最大长度：**128**
ep_name	String	企业项目名称 最小长度：**0** 最大长度：**128**
tags	String	资源标签 1、最多50个key/values对 2、values：最大255字符，取值范围：字母数字,空格,+, -, =, ., _, :, /,@ 最小长度：**0** 最大长度：**2048**

表 4-49 remediation

参数	参数类型	描述
recommendation	String	推荐处理方法 最小长度：**0** 最大长度：**128**
url	String	链接，指向该事件的一般修复信息。该URL必须可以从公网访问，不需要提供凭证 最小长度：**0** 最大长度：**2048**

表 4-50 malware

参数	参数类型	描述
malware_family	String	恶意家族 最小长度：**0** 最大长度：**64**
malware_class	String	恶意软件分类 最小长度：**0** 最大长度：**64**

表 4-51 process

参数	参数类型	描述
process_name	String	进程名 最小长度：**0** 最大长度：**64**
process_path	String	进程执行文件路径 最小长度：**0** 最大长度：**512**
process_pid	Integer	进程id 最小值：**0** 最大值：**65535**
process_uid	Integer	进程用户id 最小值：**0** 最大值：**655350**
process_cmdline	String	进程命令行 最小长度：**0** 最大长度：**128**
process_parent_name	String	父进程名称 最小长度：**0** 最大长度：**64**
process_parent_path	String	父进程执行文件路径 最小长度：**0** 最大长度：**512**
process_parent_pid	Integer	父进程id 最小值：**0** 最大值：**65535**
process_parent_uid	Integer	父进程用户id 最小值：**0** 最大值：**655350**
process_parent_cmdline	String	父进程命令行 最小长度：**0** 最大长度：**128**
process_child_name	String	子进程名称 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
process_child_path	String	子进程执行文件路径 最小长度：**0** 最大长度：**512**
process_child_pid	Integer	子进程id 最小值：**0** 最大值：**65535**
process_child_uid	Integer	子进程用户id 最小值：**0** 最大值：**655350**
process_child_cmdline	String	子进程命令行 最小长度：**0** 最大长度：**128**
process_launche_time	String	进程启动时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
process_terminate_time	String	进程结束时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

表 4-52 user_info

参数	参数类型	描述
user_id	String	用户uid 最小长度：**0** 最大长度：**36**
user_name	String	用户名称 最小长度：**32** 最大长度：**64**

表 4-53 file_info

参数	参数类型	描述
file_path	String	文件路径/名称 最小长度：**0** 最大长度：**128**
file_content	String	文件内容 最小长度：**0** 最大长度：**1024**
file_new_path	String	文件新路径/名称 最小长度：**32** 最大长度：**64**
file_hash	String	文件hash 最小长度：**0** 最大长度：**128**
file_md5	String	文件md5 最小长度：**0** 最大长度：**128**
file_sha256	String	文件sha256 最小长度：**0** 最大长度：**128**
file_attr	String	文件属性 最小长度：**0** 最大长度：**1024**

表 4-54 dataclass_ref

参数	参数类型	描述
id	String	数据类唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
name	String	数据类名称 最小长度：**0** 最大长度：**36**

状态码： 400

表 4-55 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-56 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

创建一条告警，告警名称为MyXXX，标签为MyXXX，URL为http://xxx，发生次数为4次，置信度为4，严重等级为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 – 未知，True_Positive – 确认，False_Positive – 误报。默认填写Unknown",
  "handle_status" : "Open – 打开，Block – 阻塞，Closed – 关闭。默认填写Open",
  "sla" : 60000,
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "close_time" : "2021-01-30T23:00:00Z+0800",
  "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-
Activity",
  "simulation" : "false",
  "actor" : "刘一博",
  "owner" : "MyXXX",
  "creator" : "MyXXX",
  "close_reason" : "误检;已解决;重复;其他",
  "close_comment" : "误检;已解决;重复;其他",
  "malware" : {
    "malware_family" : "family",
    "malware_class" : "恶意占用内存"
  },
  "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"
  }
}
```

响应示例

状态码： 200

创建告警返回body体

```
{
  "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 – 未知，True_Positive – 确认，False_Positive – 误报。默认填写
Unknown",
    "handle_status" : "Open – 打开，Block – 阻塞，Closed – 关闭。默认填写Open",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-
Activity",
    "simulation" : "false",
    "actor" : "刘一博",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "误检;已解决;重复;其他",
    "close_comment" : "误检;已解决;重复;其他",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "恶意占用内存"
    },
    "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 代码示例

SDK代码示例如下。

Java

创建一条告警，告警名称为MyXXX，标签为MyXXX，URL为http://xxx，发生次数为4次，置信度为4，严重等级为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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateAlertRequest request = new CreateAlertRequest();
        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("恶意占用内存");
```

```
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 – 未知,True_Positive – 确认,False_Positive – 误报。默认填写Unknown"))
            .withHandleStatus(Alert.HandleStatusEnum.fromValue("Open – 打开,Block – 阻塞,Closed – 关闭。默认填写Open"))
            .withSla(60000)
            .withUpdateTime("2021-01-30T23:00:00Z+0800")
            .withCloseTime("2021-01-30T23:00:00Z+0800")
            .withIpdrrPhase(Alert.IpdrrPhaseEnum.fromValue("Prepartion|Detection and Analysis|Containm,Eradication& Recovery| Post-Incident-Activity"))
            .withSimulation("false")
            .withActor("刘一博")
            .withOwner("MyXXX")
            .withCreator("MyXXX")
            .withCloseReason(Alert.CloseReasonEnum.fromValue("误检;已解决;重复;其他"))
            .withCloseComment("误检;已解决;重复;其他")
            .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

创建一条告警，告警名称为MyXXX，标签为MyXXX，URL为http://xxx，发生次数为4次，置信度为4，严重等级为tips。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
```

```
    request = CreateAlertRequest()
    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="恶意占用内存"
    )
    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 – 未知,True_Positive – 确认,False_Positive – 误报。默认填写Unknown",
            handle_status="Open – 打开,Block – 阻塞,Closed – 关闭。默认填写Open",
            sla=60000,
            update_time="2021-01-30T23:00:00Z+0800",
            close_time="2021-01-30T23:00:00Z+0800",
            ipdrr_phase="Prepartion|Detection and Analysis|Containm,Eradication& Recovery| Post-Incident-
Activity",
            simulation="false",
            actor="刘一博",
            owner="MyXXX",
            creator="MyXXX",
            close_reason="误检;已解决;重复;其他",
            close_comment="误检;已解决;重复;其他",
            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

创建一条告警，告警名称为MyXXX，标签为MyXXX，URL为http://xxx，发生次数为4次，置信度为4，严重等级为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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateAlertRequest{}
    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:= "恶意占用内存"
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_-_未
知,TRUE_POSITIVE_-_确认,FALSE_POSITIVE_-_误报。默认填写UNKNOWN
    handleStatusDataObject:= model.GetAlertHandleStatusEnum().OPEN_-_打开,BLOCK_-_阻塞,CLOSED_-_关
闭。默认填写OPEN
    slaDataObject:= int32(60000)
    updateTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    closeTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    ipdrrPhaseDataObject:= model.GetAlertIpdrrPhaseEnum().PREPARTION|DETECTION_AND_ANALYSIS|
CONTAINM,ERADICATION&_RECOVERY|_POST_INCIDENT_ACTIVITY
    simulationDataObject:= "false"
    actorDataObject:= "刘一博"
    ownerDataObject:= "MyXXX"
    creatorDataObject:= "MyXXX"
    closeReasonDataObject:= model.GetAlertCloseReasonEnum().误检;已解决;重复;其他
    closeCommentDataObject:= "误检;已解决;重复;其他"
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	创建告警返回body体
400	创建告警错误返回body体

错误码

请参见**错误码**。

4.1.3 删除告警

功能介绍

删除告警

调用方法

请参见**如何调用API**。

URI

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

表 4-57 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**

请求参数

表 4-58 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

表 4-59 请求 Body 参数

参数	是否必选	参数类型	描述
batch_ids	否	Array of strings	删除告警的ID列表 最小长度：**0** 最大长度：**100** 数组长度：**0 - 999**

响应参数

状态码： 200

表 4-60 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-61 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误信息 最小长度：**0** 最大长度：**1024**
data	**BatchOperateAlertResult** object	批量操作告警返回对象

表 4-62 BatchOperateAlertResult

参数	参数类型	描述
error_ids	Array of strings	失败id 最小长度：**0** 最大长度：**100** 数组长度：**0 - 100**

参数	参数类型	描述
success_ids	Array of strings	成功id 最小长度：**0** 最大长度：**100** 数组长度：**0 - 100**

状态码： 400

表 4-63 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-64 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

删除id为909494e3-558e-46b6-a9eb-07a8e18ca621的告警

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

响应示例

状态码： 200

删除告警返回body体

```
{
  "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 代码示例

SDK代码示例如下。

Java

删除id为909494e3-558e-46b6-a9eb-07a8e18ca621的告警

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteAlertRequest request = new DeleteAlertRequest();
        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

删除id为909494e3-558e-46b6-a9eb-07a8e18ca621的告警

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = DeleteAlertRequest()
        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

删除id为909494e3-558e-46b6-a9eb-07a8e18ca621的告警

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
```

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

    request := &model.DeleteAlertRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	删除告警返回body体
400	删除告警错误返回body体

错误码

请参见**错误码**。

4.1.4 告警转事件

功能介绍

告警转事件

调用方法

请参见**如何调用API**。

URI

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

表 4-65 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**

请求参数

表 4-66 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

表 4-67 请求 Body 参数

参数	是否必选	参数类型	描述
ids	否	Array of strings	转事件的告警id列表 最小长度：**0** 最大长度：**100** 数组长度：**0 - 999**
incident_content	否	**incident_content** object	事件内容

表 4-68 incident_content

参数	是否必选	参数类型	描述
title	否	String	事件名称 最小长度：**0** 最大长度：**255**
incident_type	否	**incident_type** object	事件类型

表 4-69 incident_type

参数	是否必选	参数类型	描述
id	否	String	事件类型id 最小长度：**0** 最大长度：**255**
category	否	String	事件类型父类 最小长度：**0** 最大长度：**255**
incident_type	否	String	事件类型子类 最小长度：**0** 最大长度：**255**

响应参数

状态码： 200

表 4-70 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-71 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
message	String	错误信息 最小长度：**0** 最大长度：**1024**
data	**BatchOperateAlertResult** object	批量操作告警返回对象

表 4-72 BatchOperateAlertResult

参数	参数类型	描述
error_ids	Array of strings	失败id 最小长度：**0** 最大长度：**100** 数组长度：**0 - 100**
success_ids	Array of strings	成功id 最小长度：**0** 最大长度：**100** 数组长度：**0 - 100**

状态码： 400

表 4-73 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-74 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

将一条告警转为事件，告警ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，事件ID为909494e3-558e-46b6-a9eb-07a8e18ca621，告警状态为已关闭，是否标记为证据为否。

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

响应示例

状态码： 200

告警转事件返回body体

```
{
  "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 代码示例

SDK代码示例如下。

Java

将一条告警转为事件，告警ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，事件ID为909494e3-558e-46b6-a9eb-07a8e18ca621，告警状态为已关闭，是否标记为证据为否。

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateBatchOrderAlertsRequest request = new CreateBatchOrderAlertsRequest();
        OrderAlert body = new OrderAlert();
        OrderAlertIncidentContentIncidentType incidentTypeIncidentContent = new
OrderAlertIncidentContentIncidentType();
        incidentTypeIncidentContent.withId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withCategory("DDoS攻击")
            .withIncidentType("DNS协议攻击");
        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

将一条告警转为事件，告警ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，事件ID为909494e3-558e-46b6-a9eb-07a8e18ca621，告警状态为已关闭，是否标记为证据为否。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

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

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

    try:
        request = CreateBatchOrderAlertsRequest()
        incidentTypeIncidentContent = OrderAlertIncidentContentIncidentType(
            id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
            category="DDoS攻击",
            incident_type="DNS协议攻击"
        )
        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

将一条告警转为事件，告警ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，事件ID为909494e3-558e-46b6-a9eb-07a8e18ca621，告警状态为已关闭，是否标记为证据为否。

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateBatchOrderAlertsRequest{}
```

```
    idIncidentType:= "909494e3-558e-46b6-a9eb-07a8e18ca62f"
    categoryIncidentType:= "DDoS攻击"
    incidentTypeIncidentType:= "DNS协议攻击"
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	告警转事件返回body体
400	告警转事件错误返回body体

错误码

请参见**错误码**。

4.1.5 获取告警详情

功能介绍

获取告警详情

调用方法

请参见**如何调用API**。

URI

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

表 4-75 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**
alert_id	是	String	告警ID 最小长度：**32** 最大长度：**36**

请求参数

表 4-76 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

响应参数

状态码： 200

表 4-77 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-78 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误信息 最小长度：**0** 最大长度：**1024**
data	**AlertDetail** object	

表 4-79 AlertDetail

参数	参数类型	描述
create_time	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
data_object	**Alert** object	告警实体信息
dataclass_ref	**dataclass_ref** object	数据类对象
format_version	Integer	格式版本 最小值：**0** 最大值：**999**
id	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
project_id	String	当前项目的id 最小长度：**0** 最大长度：**64**
update_time	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	参数类型	描述
version	Integer	版本 最小值：**0** 最大值：**999**
workspace_id	String	当前的工作空间id 最小长度：**0** 最大长度：**36**

表 4-80 Alert

参数	参数类型	描述
version	String	告警对象的版本，该字段的值必须为华为云SSA服务确定的官方发布版本之一 最小长度：**0** 最大长度：**64**
id	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
domain_id	String	数据投递后，被委托用户的domain_id 最小长度：**0** 最大长度：**36**
region_id	String	数据投递后，被委托用户的region_id 最小长度：**0** 最大长度：**36**
workspace_id	String	当前的工作空间id 最小长度：**0** 最大长度：**36**
labels	String	标签，仅展示 最小长度：**0** 最大长度：**1024**
environment	**environment** object	告警产生的环境坐标信息
data_source	**data_source** object	首次上报数据源

参数	参数类型	描述
first_observed_time	String	首次发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
last_observed_time	String	最近发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
create_time	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
arrive_time	String	接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
title	String	告警标题 最小长度：**0** 最大长度：**255**
description	String	告警描述信息 最小长度：**0** 最大长度：**1024**
source_url	String	告警URL链接，指向数据源产品中有关当前事件说明的页面 最小长度：**0** 最大长度：**1024**
count	Integer	事件发生次数 最小值：**0** 最大值：**999**

参数	参数类型	描述
confidence	Integer	事件的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100，0表示置信度为0%，100表示置信度为100% 最小值：**0** 最大值：**100**
severity	String	严重性等级，取值范围：Tips | Low | Medium | High | Fatal 说明： 0: Tips – 未发现任何问题。 1: Low – 无需针对问题执行任何操作。 2: Medium – 问题需要处理，但不紧急。 3: High – 问题必须优先处理。 4: Fatal – 问题必须立即处理，以防止产生进一步的损害 最小长度：**3** 最大长度：**6** 枚举值： • **Tips** • **Low** • **Medium** • **High** • **Fatal**
criticality	Integer	关键性，是指事件涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源 最小值：**0** 最大值：**100**
alert_type	**alert_type** object	告警分类，详细定义参考《告警类型定义》
network_list	Array of **network_list** objects	网络信息 数组长度：**0 - 999**
resource_list	Array of **resource_list** objects	受影响资源 数组长度：**0 - 999**
remediation	**remediation** object	补救措施

参数	参数类型	描述
verification_state	String	验证状态，标识事件的准确性。可选类型如下：Unknown – 未知 True_Positive – 确认 False_Positive – 误报 默认填写Unknown 最小长度：**32** 最大长度：**64** 枚举值： • **Unknown** • **True_Positive** • **False_Positive**
handle_status	String	事件处理状态，可选类型如下： Open – 打开，默认 Block – 阻塞 Closed – 关闭 默认填写Open 最小长度：**4** 最大长度：**5** 枚举值： • **Open** • **Block** • **Closed**
sla	Integer	约束闭环时间：设置风险接受持续时间。单位：小时 最小值：**0** 最大值：**999**
update_time	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
close_time	String	关闭时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	参数类型	描述
ipdrr_phase	String	周期/处置阶段编号 Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-Activity 最小长度：**0** 最大长度：**64** 枚举值： • **Prepartion** • **Detection and Analysis** • **Containm，Eradication& Recovery** • **Post-Incident-Activity**
simulation	String	调试字段 最小长度：**0** 最大长度：**64**
actor	String	告警调查员 最小长度：**0** 最大长度：**64**
owner	String	责任人、服务责任人 最小长度：**0** 最大长度：**64**
creator	String	创建人 最小长度：**0** 最大长度：**64**
close_reason	String	关闭原因: 误检 - False detection 已解决 - Resolved 重复 - Repeated 其他 - Other 最小长度：**0** 最大长度：**64** 枚举值： • **False detection** • **Resolved** • **Repeated** • **Other**
close_comment	String	关闭评论 最小长度：**0** 最大长度：**1024**
malware	**malware** object	恶意软件
system_info	Object	系统信息

参数	参数类型	描述
process	Array of **process** objects	进程信息 数组长度：**0 - 999**
user_info	Array of **user_info** objects	用户信息 数组长度：**0 - 999**
file_info	Array of **file_info** objects	文件信息 数组长度：**0 - 999**
system_alert_table	Object	告警管理列表的布局字段

表 4-81 environment

参数	参数类型	描述
vendor_type	String	环境供应商：HWCP/HWC/AWS/Azure/GCP 最小长度：**0** 最大长度：**64**
domain_id	String	租户id 最小长度：**0** 最大长度：**64**
region_id	String	区域od，全局服务global 最小长度：**0** 最大长度：**64**
cross_workspace_id	String	数据投递前的源工作空间id，在源空间下值为null，投递后为被委托用户的id 最小长度：**0** 最大长度：**64**
project_id	String	项目id， 全局服务默认null 最小长度：**0** 最大长度：**64**

表 4-82 data_source

参数	参数类型	描述
source_type	Integer	数据源类型，取值范围如下： 1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**1** 最大值：**3** 枚举值： • **1** • **2** • **3**
domain_id	String	数据源产品所属账号的id 最小长度：**0** 最大长度：**36**
project_id	String	数据源产品所属项目的id 最小长度：**0** 最大长度：**64**
region_id	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义，例如cn-north-1 最小长度：**0** 最大长度：**64**
company_name	String	数据源产品所属公司的名称 最小长度：**0** 最大长度：**16**
product_name	String	数据源产品的名称 最小长度：**0** 最大长度：**24**
product_feature	String	产品功能特性名称，用来指明检测到当前事件的产品的功能特性 最小长度：**0** 最大长度：**24**
product_module	String	检测模块列表 最小长度：**0** 最大长度：**1024**

表 4-83 alert_type

参数	参数类型	描述
category	String	类别 最小长度：**0** 最大长度：**1024**
alert_type	String	告警类型 最小长度：**0** 最大长度：**1024**

表 4-84 network_list

参数	参数类型	描述
direction	String	方向，取值范围：IN | OUT 最小长度：**0** 最大长度：**3** 枚举值： • **IN** • **OUT**
protocol	String	协议，包含7层和4层的协议 参考：IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml 最小长度：**0** 最大长度：**64**
src_ip	String	源IP地址 最小长度：**0** 最大长度：**64**
src_port	Integer	源端口，0–65535 最小值：**0** 最大值：**65535**
src_domain	String	源域名 最小长度：**0** 最大长度：**128**
src_geo	**src_geo** object	源IP的地理位置信息

参数	参数类型	描述
dest_ip	String	目的IP地址 最小长度：**32** 最大长度：**64**
dest_port	String	目的端口，0–65535 最小长度：**0** 最大长度：**65535**
dest_domain	String	目的域名 最小长度：**0** 最大长度：**128**
dest_geo	**dest_geo** object	目标IP的地理位置信息

表 4-85 src_geo

参数	参数类型	描述
latitude	Number	纬度 最小值：**0** 最大值：**90**
longitude	Number	经度 最小值：**0** 最大值：**180**
city_code	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-86 dest_geo

参数	参数类型	描述
latitude	Number	纬度 最小值：**0** 最大值：**90**

参数	参数类型	描述
longitude	Number	经度 最小值：**0** 最大值：**180**
city_code	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-87 resource_list

参数	参数类型	描述
id	String	云服务资源id 最小长度：**0** 最大长度：**36**
name	String	资源名称 最小长度：**0** 最大长度：**255**
type	String	资源类型；引用华为云RMS type字段 最小长度：**0** 最大长度：**64**
provider	String	云服务名称；引用华为云RMS provider字段 最小长度：**0** 最大长度：**64**
region_id	String	区域；按照华为云regionId填写，如cn-north-1等 最小长度：**0** 最大长度：**36**
domain_id	String	资源所属账号ID，UUID格式 最小长度：**0** 最大长度：**36**
project_id	String	资源所属项目ID，UUID格式 最小长度：**0** 最大长度：**36**

参数	参数类型	描述
ep_id	String	企业项目id 最小长度：**0** 最大长度：**128**
ep_name	String	企业项目名称 最小长度：**0** 最大长度：**128**
tags	String	资源标签 1、最多50个key/values对 2、values：最大255字符，取值范围：字母数字,空格,+, -, =, ., _, :, /,@ 最小长度：**0** 最大长度：**2048**

表 4-88 remediation

参数	参数类型	描述
recommendation	String	推荐处理方法 最小长度：**0** 最大长度：**128**
url	String	链接，指向该事件的一般修复信息。该URL必须可以从公网访问，不需要提供凭证 最小长度：**0** 最大长度：**2048**

表 4-89 malware

参数	参数类型	描述
malware_family	String	恶意家族 最小长度：**0** 最大长度：**64**
malware_class	String	恶意软件分类 最小长度：**0** 最大长度：**64**

表 4-90 process

参数	参数类型	描述
process_name	String	进程名 最小长度：**0** 最大长度：**64**
process_path	String	进程执行文件路径 最小长度：**0** 最大长度：**512**
process_pid	Integer	进程id 最小值：**0** 最大值：**65535**
process_uid	Integer	进程用户id 最小值：**0** 最大值：**655350**
process_cmdline	String	进程命令行 最小长度：**0** 最大长度：**128**
process_parent_name	String	父进程名称 最小长度：**0** 最大长度：**64**
process_parent_path	String	父进程执行文件路径 最小长度：**0** 最大长度：**512**
process_parent_pid	Integer	父进程id 最小值：**0** 最大值：**65535**
process_parent_uid	Integer	父进程用户id 最小值：**0** 最大值：**655350**
process_parent_cmdline	String	父进程命令行 最小长度：**0** 最大长度：**128**
process_child_name	String	子进程名称 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
process_child_path	String	子进程执行文件路径 最小长度：**0** 最大长度：**512**
process_child_pid	Integer	子进程id 最小值：**0** 最大值：**65535**
process_child_uid	Integer	子进程用户id 最小值：**0** 最大值：**655350**
process_child_cmdline	String	子进程命令行 最小长度：**0** 最大长度：**128**
process_launche_time	String	进程启动时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
process_terminate_time	String	进程结束时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

表 4-91 user_info

参数	参数类型	描述
user_id	String	用户uid 最小长度：**0** 最大长度：**36**
user_name	String	用户名称 最小长度：**32** 最大长度：**64**

表 4-92 file_info

参数	参数类型	描述
file_path	String	文件路径/名称 最小长度：**0** 最大长度：**128**
file_content	String	文件内容 最小长度：**0** 最大长度：**1024**
file_new_path	String	文件新路径/名称 最小长度：**32** 最大长度：**64**
file_hash	String	文件hash 最小长度：**0** 最大长度：**128**
file_md5	String	文件md5 最小长度：**0** 最大长度：**128**
file_sha256	String	文件sha256 最小长度：**0** 最大长度：**128**
file_attr	String	文件属性 最小长度：**0** 最大长度：**1024**

表 4-93 dataclass_ref

参数	参数类型	描述
id	String	数据类唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
name	String	数据类名称 最小长度：**0** 最大长度：**36**

状态码： 400

表 4-94 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-95 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

获取告警详情返回body体

```
{
  "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 – 未知，True_Positive – 确认，False_Positive – 误报。默认填写
Unknown",
    "handle_status" : "Open – 打开，Block – 阻塞，Closed – 关闭。默认填写Open",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-
Activity",
    "simulation" : "false",
    "actor" : "刘一博",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "误检;已解决;重复;其他",
    "close_comment" : "误检;已解决;重复;其他",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "恶意占用内存"
    },
    "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 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowAlertRequest request = new ShowAlertRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ShowAlertRequest()
        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")

    auth := basic.NewCredentialsBuilder().
```

```
        WithAk(ak).
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	获取告警详情返回body体
400	获取告警详情错误返回body体

错误码

请参见**错误码**。

4.1.6 更新告警

功能介绍

编辑告警，根据实际修改的属性更新，未修改的列不更新

调用方法

请参见**如何调用API**。

URI

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

表 4-96 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**
alert_id	是	String	告警ID 最小长度：**32** 最大长度：**36**

请求参数

表 4-97 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

表 4-98 请求 Body 参数

参数	是否必选	参数类型	描述
batch_ids	否	Array of strings	更新告警的ID列表 最小长度：**0** 最大长度：**100** 数组长度：**0 - 999**
data_object	否	**Alert** object	告警实体信息

表 4-99 Alert

参数	是否必选	参数类型	描述
version	否	String	告警对象的版本，该字段的值必须为华为云SSA服务确定的官方发布版本之一 最小长度：**0** 最大长度：**64**
id	否	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
domain_id	否	String	数据投递后，被委托用户的domain_id 最小长度：**0** 最大长度：**36**
region_id	否	String	数据投递后，被委托用户的region_id 最小长度：**0** 最大长度：**36**
workspace_id	否	String	当前的工作空间id 最小长度：**0** 最大长度：**36**
labels	否	String	标签，仅展示 最小长度：**0** 最大长度：**1024**
environment	否	**environment** object	告警产生的环境坐标信息
data_source	否	**data_source** object	首次上报数据源
first_observed_time	否	String	首次发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	是否必选	参数类型	描述
last_observed_time	否	String	最近发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
create_time	否	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
arrive_time	否	String	接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
title	否	String	告警标题 最小长度：**0** 最大长度：**255**
description	否	String	告警描述信息 最小长度：**0** 最大长度：**1024**
source_url	否	String	告警URL链接，指向数据源产品中有关当前事件说明的页面 最小长度：**0** 最大长度：**1024**
count	否	Integer	事件发生次数 最小值：**0** 最大值：**999**

参数	是否必选	参数类型	描述
confidence	否	Integer	事件的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100，0表示置信度为0%，100表示置信度为100% 最小值：**0** 最大值：**100**
severity	否	String	严重性等级，取值范围：Tips | Low | Medium | High | Fatal 说明： 0: Tips – 未发现任何问题。 1: Low – 无需针对问题执行任何操作。 2: Medium – 问题需要处理，但不紧急。 3: High – 问题必须优先处理。 4: Fatal – 问题必须立即处理，以防止产生进一步的损害 最小长度：**3** 最大长度：**6** 枚举值： • **Tips** • **Low** • **Medium** • **High** • **Fatal**
criticality	否	Integer	关键性，是指事件涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源 最小值：**0** 最大值：**100**
alert_type	否	**alert_type** object	告警分类，详细定义参考《告警类型定义》
network_list	否	Array of **network_list** objects	网络信息 数组长度：**0 - 999**
resource_list	否	Array of **resource_list** objects	受影响资源 数组长度：**0 - 999**
remediation	否	**remediation** object	补救措施

参数	是否必选	参数类型	描述
verification_state	否	String	验证状态，标识事件的准确性。可选类型如下： Unknown – 未知 True_Positive – 确认 False_Positive – 误报 默认填写 Unknown 最小长度：**32** 最大长度：**64** 枚举值： • **Unknown** • **True_Positive** • **False_Positive**
handle_status	否	String	事件处理状态，可选类型如下：Open – 打开，默认 Block – 阻塞 Closed – 关闭 默认填写 Open 最小长度：**4** 最大长度：**5** 枚举值： • **Open** • **Block** • **Closed**
sla	否	Integer	约束闭环时间：设置风险接受持续时间。单位：小时 最小值：**0** 最大值：**999**
update_time	否	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
close_time	否	String	关闭时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	是否必选	参数类型	描述
ipdrr_phase	否	String	周期/处置阶段编号 Prepartion| Detection and Analysis| Containm，Eradication& Recovery|Post-Incident-Activity 最小长度：**0** 最大长度：**64** 枚举值： • **Prepartion** • **Detection and Analysis** • **Containm，Eradication& Recovery** • **Post-Incident-Activity**
simulation	否	String	调试字段 最小长度：**0** 最大长度：**64**
actor	否	String	告警调查员 最小长度：**0** 最大长度：**64**
owner	否	String	责任人、服务责任人 最小长度：**0** 最大长度：**64**
creator	否	String	创建人 最小长度：**0** 最大长度：**64**
close_reason	否	String	关闭原因: 误检 - False detection 已解决 - Resolved 重复 - Repeated 其他 - Other 最小长度：**0** 最大长度：**64** 枚举值： • **False detection** • **Resolved** • **Repeated** • **Other**
close_comment	否	String	关闭评论 最小长度：**0** 最大长度：**1024**

参数	是否必选	参数类型	描述
malware	否	**malware** object	恶意软件
system_info	否	Object	系统信息
process	否	Array of **process** objects	进程信息 数组长度：**0 - 999**
user_info	否	Array of **user_info** objects	用户信息 数组长度：**0 - 999**
file_info	否	Array of **file_info** objects	文件信息 数组长度：**0 - 999**
system_alert_table	否	Object	告警管理列表的布局字段

表 4-100 environment

参数	是否必选	参数类型	描述
vendor_type	否	String	环境供应商：HWCP/HWC/AWS/Azure/GCP 最小长度：**0** 最大长度：**64**
domain_id	否	String	租户id 最小长度：**0** 最大长度：**64**
region_id	否	String	区域od，全局服务global 最小长度：**0** 最大长度：**64**
cross_workspace_id	否	String	数据投递前的源工作空间id，在源空间下值为null，投递后为被委托用户的id 最小长度：**0** 最大长度：**64**
project_id	否	String	项目id， 全局服务默认null 最小长度：**0** 最大长度：**64**

表 4-101 data_source

参数	是否必选	参数类型	描述
source_type	否	Integer	数据源类型，取值范围如下： 1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**1** 最大值：**3** 枚举值： • **1** • **2** • **3**
domain_id	否	String	数据源产品所属账号的id 最小长度：**0** 最大长度：**36**
project_id	否	String	数据源产品所属项目的id 最小长度：**0** 最大长度：**64**
region_id	否	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义，例如cn-north-1 最小长度：**0** 最大长度：**64**
company_name	否	String	数据源产品所属公司的名称 最小长度：**0** 最大长度：**16**
product_name	否	String	数据源产品的名称 最小长度：**0** 最大长度：**24**
product_feature	否	String	产品功能特性名称，用来指明检测到当前事件的产品的功能特性 最小长度：**0** 最大长度：**24**
product_module	否	String	检测模块列表 最小长度：**0** 最大长度：**1024**

表 4-102 alert_type

参数	是否必选	参数类型	描述
category	否	String	类别 最小长度：**0** 最大长度：**1024**
alert_type	否	String	告警类型 最小长度：**0** 最大长度：**1024**

表 4-103 network_list

参数	是否必选	参数类型	描述
direction	否	String	方向，取值范围：IN | OUT 最小长度：**0** 最大长度：**3** 枚举值： • **IN** • **OUT**
protocol	否	String	协议，包含7层和4层的协议 参考：IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml 最小长度：**0** 最大长度：**64**
src_ip	否	String	源IP地址 最小长度：**0** 最大长度：**64**
src_port	否	Integer	源端口，0–65535 最小值：**0** 最大值：**65535**
src_domain	否	String	源域名 最小长度：**0** 最大长度：**128**
src_geo	否	**src_geo** object	源IP的地理位置信息

参数	是否必选	参数类型	描述
dest_ip	否	String	目的IP地址 最小长度：**32** 最大长度：**64**
dest_port	否	String	目的端口，0–65535 最小长度：**0** 最大长度：**65535**
dest_domain	否	String	目的域名 最小长度：**0** 最大长度：**128**
dest_geo	否	**dest_geo** object	目标IP的地理位置信息

表 4-104 src_geo

参数	是否必选	参数类型	描述
latitude	否	Number	纬度 最小值：**0** 最大值：**90**
longitude	否	Number	经度 最小值：**0** 最大值：**180**
city_code	否	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	否	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-105 dest_geo

参数	是否必选	参数类型	描述
latitude	否	Number	纬度 最小值：**0** 最大值：**90**

参数	是否必选	参数类型	描述
longitude	否	Number	经度 最小值：**0** 最大值：**180**
city_code	否	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	否	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-106 resource_list

参数	是否必选	参数类型	描述
id	否	String	云服务资源id 最小长度：**0** 最大长度：**36**
name	否	String	资源名称 最小长度：**0** 最大长度：**255**
type	否	String	资源类型；引用华为云RMS type字段 最小长度：**0** 最大长度：**64**
provider	否	String	云服务名称；引用华为云RMS provider字段 最小长度：**0** 最大长度：**64**
region_id	否	String	区域；按照华为云regionId填写，如cn-north-1等 最小长度：**0** 最大长度：**36**
domain_id	否	String	资源所属账号ID，UUID格式 最小长度：**0** 最大长度：**36**

参数	是否必选	参数类型	描述
project_id	否	String	资源所属项目ID，UUID格式 最小长度：**0** 最大长度：**36**
ep_id	否	String	企业项目id 最小长度：**0** 最大长度：**128**
ep_name	否	String	企业项目名称 最小长度：**0** 最大长度：**128**
tags	否	String	资源标签 1、最多50个key/values对 2、values：最大255字符，取值范围：字母数字,空格,+, -, =, ., _, :, /,@ 最小长度：**0** 最大长度：**2048**

表 4-107 remediation

参数	是否必选	参数类型	描述
recommendation	否	String	推荐处理方法 最小长度：**0** 最大长度：**128**
url	否	String	链接，指向该事件的一般修复信息。该URL必须可以从公网访问，不需要提供凭证 最小长度：**0** 最大长度：**2048**

表 4-108 malware

参数	是否必选	参数类型	描述
malware_family	否	String	恶意家族 最小长度：**0** 最大长度：**64**
malware_class	否	String	恶意软件分类 最小长度：**0** 最大长度：**64**

表 4-109 process

参数	是否必选	参数类型	描述
process_name	否	String	进程名 最小长度：**0** 最大长度：**64**
process_path	否	String	进程执行文件路径 最小长度：**0** 最大长度：**512**
process_pid	否	Integer	进程id 最小值：**0** 最大值：**65535**
process_uid	否	Integer	进程用户id 最小值：**0** 最大值：**655350**
process_cmdline	否	String	进程命令行 最小长度：**0** 最大长度：**128**
process_parent_name	否	String	父进程名称 最小长度：**0** 最大长度：**64**
process_parent_path	否	String	父进程执行文件路径 最小长度：**0** 最大长度：**512**
process_parent_pid	否	Integer	父进程id 最小值：**0** 最大值：**65535**
process_parent_uid	否	Integer	父进程用户id 最小值：**0** 最大值：**655350**
process_parent_cmdline	否	String	父进程命令行 最小长度：**0** 最大长度：**128**
process_child_name	否	String	子进程名称 最小长度：**0** 最大长度：**64**

参数	是否必选	参数类型	描述
process_child_path	否	String	子进程执行文件路径 最小长度：**0** 最大长度：**512**
process_child_pid	否	Integer	子进程id 最小值：**0** 最大值：**65535**
process_child_uid	否	Integer	子进程用户id 最小值：**0** 最大值：**655350**
process_child_cmdline	否	String	子进程命令行 最小长度：**0** 最大长度：**128**
process_launche_time	否	String	进程启动时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
process_terminate_time	否	String	进程结束时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

表 4-110 user_info

参数	是否必选	参数类型	描述
user_id	否	String	用户uid 最小长度：**0** 最大长度：**36**
user_name	否	String	用户名称 最小长度：**32** 最大长度：**64**

表 4-111 file_info

参数	是否必选	参数类型	描述
file_path	否	String	文件路径/名称 最小长度：**0** 最大长度：**128**
file_content	否	String	文件内容 最小长度：**0** 最大长度：**1024**
file_new_path	否	String	文件新路径/名称 最小长度：**32** 最大长度：**64**
file_hash	否	String	文件hash 最小长度：**0** 最大长度：**128**
file_md5	否	String	文件md5 最小长度：**0** 最大长度：**128**
file_sha256	否	String	文件sha256 最小长度：**0** 最大长度：**128**
file_attr	否	String	文件属性 最小长度：**0** 最大长度：**1024**

响应参数

状态码： 200

表 4-112 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-113 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误信息 最小长度：**0** 最大长度：**1024**
data	**AlertDetail** object	

表 4-114 AlertDetail

参数	参数类型	描述
create_time	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
data_object	**Alert** object	告警实体信息
dataclass_ref	**dataclass_ref** object	数据类对象
format_version	Integer	格式版本 最小值：**0** 最大值：**999**
id	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
project_id	String	当前项目的id 最小长度：**0** 最大长度：**64**
update_time	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	参数类型	描述
version	Integer	版本 最小值：**0** 最大值：**999**
workspace_id	String	当前的工作空间id 最小长度：**0** 最大长度：**36**

表 4-115 Alert

参数	参数类型	描述
version	String	告警对象的版本，该字段的值必须为华为云SSA服务确定的官方发布版本之一 最小长度：**0** 最大长度：**64**
id	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
domain_id	String	数据投递后，被委托用户的domain_id 最小长度：**0** 最大长度：**36**
region_id	String	数据投递后，被委托用户的region_id 最小长度：**0** 最大长度：**36**
workspace_id	String	当前的工作空间id 最小长度：**0** 最大长度：**36**
labels	String	标签，仅展示 最小长度：**0** 最大长度：**1024**
environment	**environment** object	告警产生的环境坐标信息
data_source	**data_source** object	首次上报数据源

参数	参数类型	描述
first_observed_time	String	首次发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
last_observed_time	String	最近发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
create_time	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
arrive_time	String	接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
title	String	告警标题 最小长度：**0** 最大长度：**255**
description	String	告警描述信息 最小长度：**0** 最大长度：**1024**
source_url	String	告警URL链接，指向数据源产品中有关当前事件说明的页面 最小长度：**0** 最大长度：**1024**
count	Integer	事件发生次数 最小值：**0** 最大值：**999**

参数	参数类型	描述
confidence	Integer	事件的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100，0表示置信度为0%，100表示置信度为100% 最小值：**0** 最大值：**100**
severity	String	严重性等级，取值范围：Tips | Low | Medium | High | Fatal 说明： 0: Tips – 未发现任何问题。 1: Low – 无需针对问题执行任何操作。 2: Medium – 问题需要处理，但不紧急。 3: High – 问题必须优先处理。 4: Fatal – 问题必须立即处理，以防止产生进一步的损害 最小长度：**3** 最大长度：**6** 枚举值： • **Tips** • **Low** • **Medium** • **High** • **Fatal**
criticality	Integer	关键性，是指事件涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源 最小值：**0** 最大值：**100**
alert_type	**alert_type** object	告警分类，详细定义参考《告警类型定义》
network_list	Array of **network_list** objects	网络信息 数组长度：**0 - 999**
resource_list	Array of **resource_list** objects	受影响资源 数组长度：**0 - 999**
remediation	**remediation** object	补救措施

参数	参数类型	描述
verification_state	String	验证状态，标识事件的准确性。可选类型如下：Unknown – 未知 True_Positive – 确认 False_Positive – 误报 默认填写Unknown 最小长度：**32** 最大长度：**64** 枚举值： • **Unknown** • **True_Positive** • **False_Positive**
handle_status	String	事件处理状态，可选类型如下： Open – 打开，默认 Block – 阻塞 Closed – 关闭 默认填写Open 最小长度：**4** 最大长度：**5** 枚举值： • **Open** • **Block** • **Closed**
sla	Integer	约束闭环时间：设置风险接受持续时间。单位：小时 最小值：**0** 最大值：**999**
update_time	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
close_time	String	关闭时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	参数类型	描述
ipdrr_phase	String	周期/处置阶段编号 Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-Activity 最小长度：**0** 最大长度：**64** 枚举值： • **Prepartion** • **Detection and Analysis** • **Containm，Eradication& Recovery** • **Post-Incident-Activity**
simulation	String	调试字段 最小长度：**0** 最大长度：**64**
actor	String	告警调查员 最小长度：**0** 最大长度：**64**
owner	String	责任人、服务责任人 最小长度：**0** 最大长度：**64**
creator	String	创建人 最小长度：**0** 最大长度：**64**
close_reason	String	关闭原因: 误检 - False detection 已解决 - Resolved 重复 - Repeated 其他 - Other 最小长度：**0** 最大长度：**64** 枚举值： • **False detection** • **Resolved** • **Repeated** • **Other**
close_comment	String	关闭评论 最小长度：**0** 最大长度：**1024**
malware	**malware** object	恶意软件
system_info	Object	系统信息

参数	参数类型	描述
process	Array of **process** objects	进程信息 数组长度：**0 - 999**
user_info	Array of **user_info** objects	用户信息 数组长度：**0 - 999**
file_info	Array of **file_info** objects	文件信息 数组长度：**0 - 999**
system_alert_table	Object	告警管理列表的布局字段

表 4-116 environment

参数	参数类型	描述
vendor_type	String	环境供应商：HWCP/HWC/AWS/Azure/GCP 最小长度：**0** 最大长度：**64**
domain_id	String	租户id 最小长度：**0** 最大长度：**64**
region_id	String	区域od，全局服务global 最小长度：**0** 最大长度：**64**
cross_workspace_id	String	数据投递前的源工作空间id，在源空间下值为null，投递后为被委托用户的id 最小长度：**0** 最大长度：**64**
project_id	String	项目id， 全局服务默认null 最小长度：**0** 最大长度：**64**

表 4-117 data_source

参数	参数类型	描述
source_type	Integer	数据源类型，取值范围如下： 1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**1** 最大值：**3** 枚举值： • **1** • **2** • **3**
domain_id	String	数据源产品所属账号的id 最小长度：**0** 最大长度：**36**
project_id	String	数据源产品所属项目的id 最小长度：**0** 最大长度：**64**
region_id	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义，例如cn-north-1 最小长度：**0** 最大长度：**64**
company_name	String	数据源产品所属公司的名称 最小长度：**0** 最大长度：**16**
product_name	String	数据源产品的名称 最小长度：**0** 最大长度：**24**
product_feature	String	产品功能特性名称，用来指明检测到当前事件的产品的功能特性 最小长度：**0** 最大长度：**24**
product_module	String	检测模块列表 最小长度：**0** 最大长度：**1024**

表 4-118 alert_type

参数	参数类型	描述
category	String	类别 最小长度：**0** 最大长度：**1024**
alert_type	String	告警类型 最小长度：**0** 最大长度：**1024**

表 4-119 network_list

参数	参数类型	描述
direction	String	方向，取值范围：IN | OUT 最小长度：**0** 最大长度：**3** 枚举值： • **IN** • **OUT**
protocol	String	协议，包含7层和4层的协议 参考：IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml 最小长度：**0** 最大长度：**64**
src_ip	String	源IP地址 最小长度：**0** 最大长度：**64**
src_port	Integer	源端口，0–65535 最小值：**0** 最大值：**65535**
src_domain	String	源域名 最小长度：**0** 最大长度：**128**
src_geo	**src_geo** object	源IP的地理位置信息

参数	参数类型	描述
dest_ip	String	目的IP地址 最小长度：**32** 最大长度：**64**
dest_port	String	目的端口，0–65535 最小长度：**0** 最大长度：**65535**
dest_domain	String	目的域名 最小长度：**0** 最大长度：**128**
dest_geo	**dest_geo** object	目标IP的地理位置信息

表 4-120 src_geo

参数	参数类型	描述
latitude	Number	纬度 最小值：**0** 最大值：**90**
longitude	Number	经度 最小值：**0** 最大值：**180**
city_code	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-121 dest_geo

参数	参数类型	描述
latitude	Number	纬度 最小值：**0** 最大值：**90**

参数	参数类型	描述
longitude	Number	经度 最小值：**0** 最大值：**180**
city_code	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-122 resource_list

参数	参数类型	描述
id	String	云服务资源id 最小长度：**0** 最大长度：**36**
name	String	资源名称 最小长度：**0** 最大长度：**255**
type	String	资源类型；引用华为云RMS type字段 最小长度：**0** 最大长度：**64**
provider	String	云服务名称；引用华为云RMS provider字段 最小长度：**0** 最大长度：**64**
region_id	String	区域；按照华为云regionId填写，如cn-north-1等 最小长度：**0** 最大长度：**36**
domain_id	String	资源所属账号ID，UUID格式 最小长度：**0** 最大长度：**36**
project_id	String	资源所属项目ID，UUID格式 最小长度：**0** 最大长度：**36**

参数	参数类型	描述
ep_id	String	企业项目id 最小长度：**0** 最大长度：**128**
ep_name	String	企业项目名称 最小长度：**0** 最大长度：**128**
tags	String	资源标签 1、最多50个key/values对 2、values：最大255字符，取值范围：字母数字,空格,+, -, =, ., _, :, /,@ 最小长度：**0** 最大长度：**2048**

表 4-123 remediation

参数	参数类型	描述
recommendation	String	推荐处理方法 最小长度：**0** 最大长度：**128**
url	String	链接，指向该事件的一般修复信息。该URL必须可以从公网访问，不需要提供凭证 最小长度：**0** 最大长度：**2048**

表 4-124 malware

参数	参数类型	描述
malware_family	String	恶意家族 最小长度：**0** 最大长度：**64**
malware_class	String	恶意软件分类 最小长度：**0** 最大长度：**64**

表 4-125 process

参数	参数类型	描述
process_name	String	进程名 最小长度：**0** 最大长度：**64**
process_path	String	进程执行文件路径 最小长度：**0** 最大长度：**512**
process_pid	Integer	进程id 最小值：**0** 最大值：**65535**
process_uid	Integer	进程用户id 最小值：**0** 最大值：**655350**
process_cmdline	String	进程命令行 最小长度：**0** 最大长度：**128**
process_parent_name	String	父进程名称 最小长度：**0** 最大长度：**64**
process_parent_path	String	父进程执行文件路径 最小长度：**0** 最大长度：**512**
process_parent_pid	Integer	父进程id 最小值：**0** 最大值：**65535**
process_parent_uid	Integer	父进程用户id 最小值：**0** 最大值：**655350**
process_parent_cmdline	String	父进程命令行 最小长度：**0** 最大长度：**128**
process_child_name	String	子进程名称 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
process_child_path	String	子进程执行文件路径 最小长度：**0** 最大长度：**512**
process_child_pid	Integer	子进程id 最小值：**0** 最大值：**65535**
process_child_uid	Integer	子进程用户id 最小值：**0** 最大值：**655350**
process_child_cmdline	String	子进程命令行 最小长度：**0** 最大长度：**128**
process_launche_time	String	进程启动时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
process_terminate_time	String	进程结束时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

表 4-126 user_info

参数	参数类型	描述
user_id	String	用户uid 最小长度：**0** 最大长度：**36**
user_name	String	用户名称 最小长度：**32** 最大长度：**64**

表 4-127 file_info

参数	参数类型	描述
file_path	String	文件路径/名称 最小长度：**0** 最大长度：**128**
file_content	String	文件内容 最小长度：**0** 最大长度：**1024**
file_new_path	String	文件新路径/名称 最小长度：**32** 最大长度：**64**
file_hash	String	文件hash 最小长度：**0** 最大长度：**128**
file_md5	String	文件md5 最小长度：**0** 最大长度：**128**
file_sha256	String	文件sha256 最小长度：**0** 最大长度：**128**
file_attr	String	文件属性 最小长度：**0** 最大长度：**1024**

表 4-128 dataclass_ref

参数	参数类型	描述
id	String	数据类唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
name	String	数据类名称 最小长度：**0** 最大长度：**36**

状态码： 400

表 4-129 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-130 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

更新一条告警，告警名称为MyXXX，URL为http://xxx，发生次数为4次，置信度为4，严重等级为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 – 未知，True_Positive – 确认，False_Positive – 误报。默认填写Unknown",
  "handle_status" : "Open – 打开，Block – 阻塞，Closed – 关闭。默认填写Open",
  "sla" : 60000,
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "close_time" : "2021-01-30T23:00:00Z+0800",
  "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-
Activity",
  "simulation" : "false",
  "actor" : "刘一博",
  "owner" : "MyXXX",
  "creator" : "MyXXX",
  "close_reason" : "误检;已解决;重复;其他",
  "close_comment" : "误检;已解决;重复;其他",
  "malware" : {
    "malware_family" : "family",
    "malware_class" : "恶意占用内存"
  },
  "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"
```

```
  }
}
```

响应示例

状态码： 200

更新告警返回body体

```
{
  "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 – 未知，True_Positive – 确认，False_Positive – 误报。默认填写
Unknown",
    "handle_status" : "Open – 打开，Block – 阻塞，Closed – 关闭。默认填写Open",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-
Activity",
    "simulation" : "false",
    "actor" : "刘一博",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "误检;已解决;重复;其他",
    "close_comment" : "误检;已解决;重复;其他",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "恶意占用内存"
    },
    "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 代码示例

SDK代码示例如下。

Java

更新一条告警，告警名称为MyXXX，URL为http://xxx，发生次数为4次，置信度为4，严重等级为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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ChangeAlertRequest request = new ChangeAlertRequest();
        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("恶意占用内存");
```

```
        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 – 未知,True_Positive – 确
认,False_Positive – 误报。默认填写Unknown"))
            .withHandleStatus(Alert.HandleStatusEnum.fromValue("Open – 打开,Block – 阻塞,Closed – 关闭。默
```

```
认填写Open"))
            .withSla(60000)
            .withUpdateTime("2021-01-30T23:00:00Z+0800")
            .withCloseTime("2021-01-30T23:00:00Z+0800")
            .withIpdrrPhase(Alert.IpdrrPhaseEnum.fromValue("Prepartion|Detection and Analysis|
Containm,Eradication& Recovery| Post-Incident-Activity"))
            .withSimulation("false")
            .withActor("刘一博")
            .withOwner("MyXXX")
            .withCreator("MyXXX")
            .withCloseReason(Alert.CloseReasonEnum.fromValue("误检;已解决;重复;其他"))
            .withCloseComment("误检;已解决;重复;其他")
            .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

更新一条告警，告警名称为MyXXX，URL为http://xxx，发生次数为4次，置信度为4，严重等级为tips。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ChangeAlertRequest()
        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="恶意占用内存"
    )
    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 – 未知,True_Positive – 确认,False_Positive – 误报。默认填写Unknown",
            handle_status="Open – 打开,Block – 阻塞,Closed – 关闭。默认填写Open",
            sla=60000,
            update_time="2021-01-30T23:00:00Z+0800",
            close_time="2021-01-30T23:00:00Z+0800",
            ipdrr_phase="Prepartion|Detection and Analysis|Containm,Eradication& Recovery| Post-Incident-
Activity",
            simulation="false",
            actor="刘一博",
            owner="MyXXX",
            creator="MyXXX",
            close_reason="误检;已解决;重复;其他",
            close_comment="误检;已解决;重复;其他",
            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

更新一条告警，告警名称为MyXXX，URL为http://xxx，发生次数为4次，置信度为4，严重等级为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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ChangeAlertRequest{}
    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:= "恶意占用内存"
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_-_未
知,TRUE_POSITIVE_-_确认,FALSE_POSITIVE_-_误报。默认填写UNKNOWN
    handleStatusDataObject:= model.GetAlertHandleStatusEnum().OPEN_-_打开,BLOCK_-_阻塞,CLOSED_-_关
闭。默认填写OPEN
    slaDataObject:= int32(60000)
    updateTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    closeTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    ipdrrPhaseDataObject:= model.GetAlertIpdrrPhaseEnum().PREPARTION|DETECTION_AND_ANALYSIS|
CONTAINM,ERADICATION&_RECOVERY|_POST_INCIDENT_ACTIVITY
    simulationDataObject:= "false"
    actorDataObject:= "刘一博"
    ownerDataObject:= "MyXXX"
    creatorDataObject:= "MyXXX"
    closeReasonDataObject:= model.GetAlertCloseReasonEnum().误检;已解决;重复;其他
    closeCommentDataObject:= "误检;已解决;重复;其他"
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	更新告警返回body体
400	更新告警错误返回body体

错误码

请参见**错误码**。

4.2 事件管理

4.2.1 搜索事件列表

功能介绍

搜索事件列表

调用方法

请参见**如何调用API**。

URI

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

表 4-131 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**

请求参数

表 4-132 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

表 4-133 请求 Body 参数

参数	是否必选	参数类型	描述
limit	否	Integer	分页大小 最小值：**0** 最大值：**1000**

参数	是否必选	参数类型	描述
offset	否	Integer	偏移量 最小值：**0** 最大值：**1000**
sort_by	否	String	排序字段：create_time | update_time 最小长度：**0** 最大长度：**1000**
order	否	String	排序方式：DESC | ASC 最小长度：**0** 最大长度：**1000** 枚举值： • **DESC** • **ASC**
from_date	否	String	搜索开始时间，例如：2023-02-20T00:00:00.000Z 最小长度：**0** 最大长度：**64**
to_date	否	String	搜索结束时间，例如：2023-02-27T23:59:59.999Z 最小长度：**0** 最大长度：**64**
condition	否	**condition** object	搜索条件表达式

表 4-134 condition

参数	是否必选	参数类型	描述
conditions	否	Array of **conditions** objects	表达式列表 数组长度：**0 - 999**
logics	否	Array of strings	表达式名称列表 最小长度：**0** 最大长度：**100** 数组长度：**0 - 999**

表 4-135 conditions

参数	是否必选	参数类型	描述
name	否	String	表达式名称 最小长度：**0** 最大长度：**64**
data	否	Array of strings	表达式内容列表 最小长度：**0** 最大长度：**100** 数组长度：**0 - 999**

响应参数

状态码： 200

表 4-136 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-137 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误信息 最小长度：**0** 最大长度：**1024**
total	Integer	事件总数 最小值：**0** 最大值：**10000**
limit	Integer	分页大小 最小值：**0** 最大值：**10000**
offset	Integer	偏移量 最小值：**0** 最大值：**10000**

参数	参数类型	描述
success	Boolean	是否成功
data	Array of IncidentDetail objects	事件列表 数组长度：**0 - 10000**

表 4-138 IncidentDetail

参数	参数类型	描述
create_time	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
data_object	Incident object	事件实体信息
dataclass_ref	dataclass_ref object	数据类对象
format_version	Integer	格式版本 最小值：**0** 最大值：**999**
id	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
project_id	String	当前项目的id 最小长度：**0** 最大长度：**64**
update_time	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为告警发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
version	Integer	版本 最小值：**0** 最大值：**999**

参数	参数类型	描述
workspace_id	String	当前的工作空间id 最小长度：**0** 最大长度：**36**

表 4-139 Incident

参数	参数类型	描述
version	String	事件对象的版本，该字段的值必须为华为云SSA服务确定的官方发布版本之一 最小长度：**0** 最大长度：**64**
id	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
domain_id	String	数据投递后，被委托用户的domain_id 最小长度：**0** 最大长度：**36**
region_id	String	数据投递后，被委托用户的region_id 最小长度：**0** 最大长度：**36**
workspace_id	String	当前的工作空间id 最小长度：**0** 最大长度：**36**
labels	String	标签，仅展示 最小长度：**0** 最大长度：**1024**
environment	**environment** object	事件产生的环境坐标信息
data_source	**data_source** object	首次上报数据源
first_observed_time	String	首次发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	参数类型	描述
last_observed_time	String	最近发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
create_time	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
arrive_time	String	接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
title	String	事件标题 最小长度：**0** 最大长度：**255**
description	String	事件描述信息 最小长度：**0** 最大长度：**1024**
source_url	String	事件URL链接，指向数据源产品中有关当前事件说明的页面 最小长度：**0** 最大长度：**1024**
count	Integer	事件发生次数 最小值：**0** 最大值：**999**
confidence	Integer	事件的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100，0表示置信度为0%，100表示置信度为100% 最小值：**0** 最大值：**100**

参数	参数类型	描述
severity	String	严重性等级，取值范围：Tips | Low | Medium | High | Fatal 说明： 0: Tips – 未发现任何问题。 1: Low – 无需针对问题执行任何操作。 2: Medium – 问题需要处理，但不紧急。 3: High – 问题必须优先处理。 4: Fatal – 问题必须立即处理，以防止产生进一步的损害 最小长度：**3** 最大长度：**6** 枚举值： • **Tips** • **Low** • **Medium** • **High** • **Fatal**
criticality	Integer	关键性，是指事件涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源 最小值：**0** 最大值：**100**
incident_type	**incident_type** object	事件分类，详细定义参考《 告警事件类型定义 》
network_list	Array of **network_list** objects	网络信息 数组长度：**0 - 999**
resource_list	Array of **resource_list** objects	受影响资源 数组长度：**0 - 999**
remediation	**remediation** object	补救措施
verification_state	String	验证状态，标识事件的准确性。可选类型如下：Unknown – 未知 True_Positive – 确认 False_Positive – 误报 默认填写Unknown 最小长度：**32** 最大长度：**64** 枚举值： • **Unknown** • **True_Positive** • **False_Positive**

参数	参数类型	描述
handle_status	String	事件处理状态，可选类型如下： Open – 打开，默认 Block – 阻塞 Closed – 关闭 默认填写Open 最小长度：**4** 最大长度：**5** 枚举值： • **Open** • **Block** • **Closed**
sla	Integer	约束闭环时间：设置风险接受持续时间。单位：小时 最小值：**0** 最大值：**999**
update_time	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
close_time	String	关闭时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
ipdrr_phase	String	周期/处置阶段编号 Prepartion|Detection and Analysis|Containm，Eradication& Recovery|Post-Incident-Activity 最小长度：**0** 最大长度：**64** 枚举值： • **Prepartion** • **Detection and Analysis** • **Containm，Eradication& Recovery** • **Post-Incident-Activity**
simulation	String	调试字段 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
actor	String	事件调查员 最小长度：**0** 最大长度：**64**
owner	String	责任人、服务责任人 最小长度：**0** 最大长度：**64**
creator	String	创建人 最小长度：**0** 最大长度：**64**
close_reason	String	关闭原因: 误检 - False detection 已解决 - Resolved 重复 - Repeated 其他 - Other 最小长度：**0** 最大长度：**64** 枚举值： • **False detection** • **Resolved** • **Repeated** • **Other**
close_comment	String	关闭评论 最小长度：**0** 最大长度：**1024**
malware	**malware** object	恶意软件
system_info	Object	系统信息
process	Array of **process** objects	进程信息 数组长度：**0 - 999**
user_info	Array of **user_info** objects	用户信息 数组长度：**0 - 999**
file_info	Array of **file_info** objects	文件信息 数组长度：**0 - 999**
system_alert_table	Object	事件管理列表的布局字段

表 4-140 environment

参数	参数类型	描述
vendor_type	String	环境供应商：HWCP/HWC/AWS/Azure/GCP 最小长度：**0** 最大长度：**64**
domain_id	String	租户id 最小长度：**0** 最大长度：**64**
region_id	String	区域id，全局服务global 最小长度：**0** 最大长度：**64**
cross_workspace_id	String	数据投递前的源工作空间id，在源空间下值为null，投递后为被委托用户的id 最小长度：**0** 最大长度：**64**
project_id	String	项目id， 全局服务默认null 最小长度：**0** 最大长度：**64**

表 4-141 data_source

参数	参数类型	描述
source_type	Integer	数据源类型，取值范围如下： 1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**1** 最大值：**3** 枚举值： • **1** • **2** • **3**
domain_id	String	数据源产品所属账号的id 最小长度：**0** 最大长度：**36**
project_id	String	数据源产品所属项目的id 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
region_id	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义，例如cn-north-1 最小长度：**0** 最大长度：**64**
company_name	String	数据源产品所属公司的名称 最小长度：**0** 最大长度：**16**
product_name	String	数据源产品的名称 最小长度：**0** 最大长度：**24**
product_feature	String	产品功能特性名称，用来指明检测到当前事件的产品的功能特性 最小长度：**0** 最大长度：**24**
product_module	String	检测模块列表 最小长度：**0** 最大长度：**1024**

表 4-142 incident_type

参数	参数类型	描述
category	String	类别 最小长度：**0** 最大长度：**1024**
incident_type	String	事件类型 最小长度：**0** 最大长度：**1024**

表 4-143 network_list

参数	参数类型	描述
direction	String	方向，取值范围：IN | OUT 最小长度：**0** 最大长度：**3** 枚举值： • **IN** • **OUT**
protocol	String	协议，包含7层和4层的协议 参考：IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml 最小长度：**0** 最大长度：**64**
src_ip	String	源IP地址 最小长度：**0** 最大长度：**64**
src_port	Integer	源端口，0–65535 最小值：**0** 最大值：**65535**
src_domain	String	源域名 最小长度：**0** 最大长度：**128**
src_geo	**src_geo** object	源IP的地理位置信息
dest_ip	String	目的IP地址 最小长度：**32** 最大长度：**64**
dest_port	String	目的端口，0–65535 最小长度：**0** 最大长度：**65535**
dest_domain	String	目的域名 最小长度：**0** 最大长度：**128**
dest_geo	**dest_geo** object	目标IP的地理位置信息

表 4-144 src_geo

参数	参数类型	描述
latitude	Number	纬度 最小值：**0** 最大值：**90**
longitude	Number	经度 最小值：**0** 最大值：**180**
city_code	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-145 dest_geo

参数	参数类型	描述
latitude	Number	纬度 最小值：**0** 最大值：**90**
longitude	Number	经度 最小值：**0** 最大值：**180**
city_code	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-146 resource_list

参数	参数类型	描述
id	String	云服务资源id 最小长度：**0** 最大长度：**36**
name	String	资源名称 最小长度：**0** 最大长度：**255**
type	String	资源类型；引用华为云RMS type字段 最小长度：**0** 最大长度：**64**
provider	String	云服务名称；引用华为云RMS provider字段 最小长度：**0** 最大长度：**64**
region_id	String	区域；按照华为云regionId填写，如cn-north-1等 最小长度：**0** 最大长度：**36**
domain_id	String	资源所属账号ID，UUID格式 最小长度：**0** 最大长度：**36**
project_id	String	资源所属项目ID，UUID格式 最小长度：**0** 最大长度：**36**
ep_id	String	企业项目id 最小长度：**0** 最大长度：**128**
ep_name	String	企业项目名称 最小长度：**0** 最大长度：**128**
tags	String	资源标签 1、最多50个key/values对 2、values：最大255字符，取值范围：字母数字,空格,+, -, =, ., _, :, /,@ 最小长度：**0** 最大长度：**2048**

表 4-147 remediation

参数	参数类型	描述
recommendation	String	推荐处理方法 最小长度：**0** 最大长度：**128**
url	String	链接，指向该事件的一般修复信息。该URL必须可以从公网访问，不需要提供凭证 最小长度：**0** 最大长度：**2048**

表 4-148 malware

参数	参数类型	描述
malware_family	String	恶意家族 最小长度：**0** 最大长度：**64**
malware_class	String	恶意软件分类 最小长度：**0** 最大长度：**64**

表 4-149 process

参数	参数类型	描述
process_name	String	进程名 最小长度：**0** 最大长度：**64**
process_path	String	进程执行文件路径 最小长度：**0** 最大长度：**512**
process_pid	Integer	进程id 最小值：**0** 最大值：**65535**
process_uid	Integer	进程用户id 最小值：**0** 最大值：**655350**

参数	参数类型	描述
process_cmdline	String	进程命令行 最小长度：**0** 最大长度：**128**
process_parent_name	String	父进程名称 最小长度：**0** 最大长度：**64**
process_parent_path	String	父进程执行文件路径 最小长度：**0** 最大长度：**512**
process_parent_pid	Integer	父进程id 最小值：**0** 最大值：**65535**
process_parent_uid	Integer	父进程用户id 最小值：**0** 最大值：**655350**
process_parent_cmdline	String	父进程命令行 最小长度：**0** 最大长度：**128**
process_child_name	String	子进程名称 最小长度：**0** 最大长度：**64**
process_child_path	String	子进程执行文件路径 最小长度：**0** 最大长度：**512**
process_child_pid	Integer	子进程id 最小值：**0** 最大值：**65535**
process_child_uid	Integer	子进程用户id 最小值：**0** 最大值：**655350**
process_child_cmdline	String	子进程命令行 最小长度：**0** 最大长度：**128**

参数	参数类型	描述
process_launche_time	String	进程启动时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
process_terminate_time	String	进程结束时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

表 4-150 user_info

参数	参数类型	描述
user_id	String	用户uid 最小长度：**0** 最大长度：**36**
user_name	String	用户名称 最小长度：**32** 最大长度：**64**

表 4-151 file_info

参数	参数类型	描述
file_path	String	文件路径/名称 最小长度：**0** 最大长度：**128**
file_content	String	文件内容 最小长度：**0** 最大长度：**1024**
file_new_path	String	文件新路径/名称 最小长度：**32** 最大长度：**64**

参数	参数类型	描述
file_hash	String	文件hash 最小长度：**0** 最大长度：**128**
file_md5	String	文件md5 最小长度：**0** 最大长度：**128**
file_sha256	String	文件sha256 最小长度：**0** 最大长度：**128**
file_attr	String	文件属性 最小长度：**0** 最大长度：**1024**

表 4-152 dataclass_ref

参数	参数类型	描述
id	String	数据类唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
name	String	数据类名称 最小长度：**0** 最大长度：**36**

状态码： 400

表 4-153 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-154 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

查询事件列表请求样例，查询2024年1月20号到2024年1月26号，事件等级为中危且处理状态为打开的事件，按照创建时间降序排序，返回第一页，每页10条数据

```
{
  "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"
}
```

响应示例

状态码： 200

搜索事件列表返回body体

```
{
  "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 – 未知，True_Positive – 确认，False_Positive – 误报。默认填写
Unknown",
    "handle_status" : "Open – 打开，Block – 阻塞，Closed – 关闭。默认填写Open",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-
Activity",
    "simulation" : "false",
    "actor" : "刘一博",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "误检;已解决;重复;其他",
    "close_comment" : "误检;已解决;重复;其他",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "恶意占用内存"
    },
    "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 代码示例

SDK代码示例如下。

Java

查询事件列表请求样例，查询2024年1月20号到2024年1月26号，事件等级为中危且处理状态为打开的事件，按照创建时间降序排序，返回第一页，每页10条数据

```
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");

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

```
        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListIncidentsRequest request = new ListIncidentsRequest();
        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

查询事件列表请求样例，查询2024年1月20号到2024年1月26号，事件等级为中危且处理状态为打开的事件，按照创建时间降序排序，返回第一页，每页10条数据

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListIncidentsRequest()
        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

查询事件列表请求样例，查询2024年1月20号到2024年1月26号，事件等级为中危且处理状态为打开的事件，按照创建时间降序排序，返回第一页，每页10条数据

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListIncidentsRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	搜索事件列表返回body体
400	搜索事件列表错误返回body体

错误码

请参见**错误码**。

4.2.2 创建事件

功能介绍

创建事件

调用方法

请参见**如何调用API**。

URI

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

表 4-155 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**

请求参数

表 4-156 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

表 4-157 请求 Body 参数

参数	是否必选	参数类型	描述
data_object	否	**Incident** object	事件实体信息

表 4-158 Incident

参数	是否必选	参数类型	描述
version	否	String	事件对象的版本，该字段的值必须为华为云SSA服务确定的官方发布版本之一 最小长度：**0** 最大长度：**64**
id	否	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
domain_id	否	String	数据投递后，被委托用户的domain_id 最小长度：**0** 最大长度：**36**
region_id	否	String	数据投递后，被委托用户的region_id 最小长度：**0** 最大长度：**36**
workspace_id	否	String	当前的工作空间id 最小长度：**0** 最大长度：**36**
labels	否	String	标签，仅展示 最小长度：**0** 最大长度：**1024**
environment	否	**environment** object	事件产生的环境坐标信息
data_source	否	**data_source** object	首次上报数据源
first_observed_time	否	String	首次发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	是否必选	参数类型	描述
last_observed_time	否	String	最近发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
create_time	否	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
arrive_time	否	String	接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
title	否	String	事件标题 最小长度：**0** 最大长度：**255**
description	否	String	事件描述信息 最小长度：**0** 最大长度：**1024**
source_url	否	String	事件URL链接，指向数据源产品中有关当前事件说明的页面 最小长度：**0** 最大长度：**1024**
count	否	Integer	事件发生次数 最小值：**0** 最大值：**999**

参数	是否必选	参数类型	描述
confidence	否	Integer	事件的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100，0表示置信度为0%，100表示置信度为100% 最小值：**0** 最大值：**100**
severity	否	String	严重性等级，取值范围：Tips | Low | Medium | High | Fatal 说明： 0: Tips – 未发现任何问题。 1: Low – 无需针对问题执行任何操作。 2: Medium – 问题需要处理，但不紧急。 3: High – 问题必须优先处理。 4: Fatal – 问题必须立即处理，以防止产生进一步的损害 最小长度：**3** 最大长度：**6** 枚举值： • **Tips** • **Low** • **Medium** • **High** • **Fatal**
criticality	否	Integer	关键性，是指事件涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源 最小值：**0** 最大值：**100**
incident_type	否	**incident_type** object	事件分类，详细定义参考《告警事件类型定义》
network_list	否	Array of **network_list** objects	网络信息 数组长度：**0 - 999**
resource_list	否	Array of **resource_list** objects	受影响资源 数组长度：**0 - 999**
remediation	否	**remediation** object	补救措施

参数	是否必选	参数类型	描述
verification_state	否	String	验证状态，标识事件的准确性。可选类型如下： Unknown – 未知 True_Positive – 确认 False_Positive – 误报 默认填写 Unknown 最小长度：**32** 最大长度：**64** 枚举值： • **Unknown** • **True_Positive** • **False_Positive**
handle_status	否	String	事件处理状态，可选类型如下：Open – 打开，默认 Block – 阻塞 Closed – 关闭 默认填写 Open 最小长度：**4** 最大长度：**5** 枚举值： • **Open** • **Block** • **Closed**
sla	否	Integer	约束闭环时间：设置风险接受持续时间。单位：小时 最小值：**0** 最大值：**999**
update_time	否	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
close_time	否	String	关闭时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	是否必选	参数类型	描述
ipdrr_phase	否	String	周期/处置阶段编号 Prepartion| Detection and Analysis| Containm，Eradication& Recovery|Post-Incident-Activity 最小长度：**0** 最大长度：**64** 枚举值： • **Prepartion** • **Detection and Analysis** • **Containm，Eradication& Recovery** • **Post-Incident-Activity**
simulation	否	String	调试字段 最小长度：**0** 最大长度：**64**
actor	否	String	事件调查员 最小长度：**0** 最大长度：**64**
owner	否	String	责任人、服务责任人 最小长度：**0** 最大长度：**64**
creator	否	String	创建人 最小长度：**0** 最大长度：**64**
close_reason	否	String	关闭原因: 误检 - False detection 已解决 - Resolved 重复 - Repeated 其他 - Other 最小长度：**0** 最大长度：**64** 枚举值： • **False detection** • **Resolved** • **Repeated** • **Other**
close_comment	否	String	关闭评论 最小长度：**0** 最大长度：**1024**

参数	是否必选	参数类型	描述
malware	否	**malware** object	恶意软件
system_info	否	Object	系统信息
process	否	Array of **process** objects	进程信息 数组长度：**0 - 999**
user_info	否	Array of **user_info** objects	用户信息 数组长度：**0 - 999**
file_info	否	Array of **file_info** objects	文件信息 数组长度：**0 - 999**
system_alert_table	否	Object	事件管理列表的布局字段

表 4-159 environment

参数	是否必选	参数类型	描述
vendor_type	否	String	环境供应商：HWCP/HWC/AWS/Azure/GCP 最小长度：**0** 最大长度：**64**
domain_id	否	String	租户id 最小长度：**0** 最大长度：**64**
region_id	否	String	区域id，全局服务global 最小长度：**0** 最大长度：**64**
cross_workspace_id	否	String	数据投递前的源工作空间id，在源空间下值为null，投递后为被委托用户的id 最小长度：**0** 最大长度：**64**
project_id	否	String	项目id， 全局服务默认null 最小长度：**0** 最大长度：**64**

表 4-160 data_source

参数	是否必选	参数类型	描述
source_type	否	Integer	数据源类型，取值范围如下： 1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**1** 最大值：**3** 枚举值： • **1** • **2** • **3**
domain_id	否	String	数据源产品所属账号的id 最小长度：**0** 最大长度：**36**
project_id	否	String	数据源产品所属项目的id 最小长度：**0** 最大长度：**64**
region_id	否	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义，例如cn-north-1 最小长度：**0** 最大长度：**64**
company_name	否	String	数据源产品所属公司的名称 最小长度：**0** 最大长度：**16**
product_name	否	String	数据源产品的名称 最小长度：**0** 最大长度：**24**
product_feature	否	String	产品功能特性名称，用来指明检测到当前事件的产品的功能特性 最小长度：**0** 最大长度：**24**
product_module	否	String	检测模块列表 最小长度：**0** 最大长度：**1024**

表 4-161 incident_type

参数	是否必选	参数类型	描述
category	否	String	类别 最小长度：**0** 最大长度：**1024**
incident_type	否	String	事件类型 最小长度：**0** 最大长度：**1024**

表 4-162 network_list

参数	是否必选	参数类型	描述
direction	否	String	方向，取值范围：IN | OUT 最小长度：**0** 最大长度：**3** 枚举值： • **IN** • **OUT**
protocol	否	String	协议，包含7层和4层的协议 参考：IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml 最小长度：**0** 最大长度：**64**
src_ip	否	String	源IP地址 最小长度：**0** 最大长度：**64**
src_port	否	Integer	源端口，0–65535 最小值：**0** 最大值：**65535**
src_domain	否	String	源域名 最小长度：**0** 最大长度：**128**
src_geo	否	**src_geo** object	源IP的地理位置信息

参数	是否必选	参数类型	描述
dest_ip	否	String	目的IP地址 最小长度：**32** 最大长度：**64**
dest_port	否	String	目的端口，0–65535 最小长度：**0** 最大长度：**65535**
dest_domain	否	String	目的域名 最小长度：**0** 最大长度：**128**
dest_geo	否	**dest_geo** object	目标IP的地理位置信息

表 4-163 src_geo

参数	是否必选	参数类型	描述
latitude	否	Number	纬度 最小值：**0** 最大值：**90**
longitude	否	Number	经度 最小值：**0** 最大值：**180**
city_code	否	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	否	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-164 dest_geo

参数	是否必选	参数类型	描述
latitude	否	Number	纬度 最小值：**0** 最大值：**90**

参数	是否必选	参数类型	描述
longitude	否	Number	经度 最小值：**0** 最大值：**180**
city_code	否	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	否	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-165 resource_list

参数	是否必选	参数类型	描述
id	否	String	云服务资源id 最小长度：**0** 最大长度：**36**
name	否	String	资源名称 最小长度：**0** 最大长度：**255**
type	否	String	资源类型；引用华为云RMS type字段 最小长度：**0** 最大长度：**64**
provider	否	String	云服务名称；引用华为云RMS provider字段 最小长度：**0** 最大长度：**64**
region_id	否	String	区域；按照华为云regionId填写，如cn-north-1等 最小长度：**0** 最大长度：**36**
domain_id	否	String	资源所属账号ID，UUID格式 最小长度：**0** 最大长度：**36**

参数	是否必选	参数类型	描述
project_id	否	String	资源所属项目ID，UUID格式 最小长度：**0** 最大长度：**36**
ep_id	否	String	企业项目id 最小长度：**0** 最大长度：**128**
ep_name	否	String	企业项目名称 最小长度：**0** 最大长度：**128**
tags	否	String	资源标签 1、最多50个key/values对 2、values：最大255字符，取值范围：字母数字,空格,+, -, =, ., _, :, /,@ 最小长度：**0** 最大长度：**2048**

表 4-166 remediation

参数	是否必选	参数类型	描述
recommendation	否	String	推荐处理方法 最小长度：**0** 最大长度：**128**
url	否	String	链接，指向该事件的一般修复信息。该URL必须可以从公网访问，不需要提供凭证 最小长度：**0** 最大长度：**2048**

表 4-167 malware

参数	是否必选	参数类型	描述
malware_family	否	String	恶意家族 最小长度：**0** 最大长度：**64**
malware_class	否	String	恶意软件分类 最小长度：**0** 最大长度：**64**

表 4-168 process

参数	是否必选	参数类型	描述
process_name	否	String	进程名 最小长度：**0** 最大长度：**64**
process_path	否	String	进程执行文件路径 最小长度：**0** 最大长度：**512**
process_pid	否	Integer	进程id 最小值：**0** 最大值：**65535**
process_uid	否	Integer	进程用户id 最小值：**0** 最大值：**655350**
process_cmdline	否	String	进程命令行 最小长度：**0** 最大长度：**128**
process_parent_name	否	String	父进程名称 最小长度：**0** 最大长度：**64**
process_parent_path	否	String	父进程执行文件路径 最小长度：**0** 最大长度：**512**
process_parent_pid	否	Integer	父进程id 最小值：**0** 最大值：**65535**
process_parent_uid	否	Integer	父进程用户id 最小值：**0** 最大值：**655350**
process_parent_cmdline	否	String	父进程命令行 最小长度：**0** 最大长度：**128**
process_child_name	否	String	子进程名称 最小长度：**0** 最大长度：**64**

参数	是否必选	参数类型	描述
process_child_path	否	String	子进程执行文件路径 最小长度：**0** 最大长度：**512**
process_child_pid	否	Integer	子进程id 最小值：**0** 最大值：**65535**
process_child_uid	否	Integer	子进程用户id 最小值：**0** 最大值：**655350**
process_child_cmdline	否	String	子进程命令行 最小长度：**0** 最大长度：**128**
process_launche_time	否	String	进程启动时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
process_terminate_time	否	String	进程结束时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

表 4-169 user_info

参数	是否必选	参数类型	描述
user_id	否	String	用户uid 最小长度：**0** 最大长度：**36**
user_name	否	String	用户名称 最小长度：**32** 最大长度：**64**

表 4-170 file_info

参数	是否必选	参数类型	描述
file_path	否	String	文件路径/名称 最小长度：**0** 最大长度：**128**
file_content	否	String	文件内容 最小长度：**0** 最大长度：**1024**
file_new_path	否	String	文件新路径/名称 最小长度：**32** 最大长度：**64**
file_hash	否	String	文件hash 最小长度：**0** 最大长度：**128**
file_md5	否	String	文件md5 最小长度：**0** 最大长度：**128**
file_sha256	否	String	文件sha256 最小长度：**0** 最大长度：**128**
file_attr	否	String	文件属性 最小长度：**0** 最大长度：**1024**

响应参数

状态码： 200

表 4-171 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-172 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误信息 最小长度：**0** 最大长度：**1024**
data	**IncidentDetail** object	

表 4-173 IncidentDetail

参数	参数类型	描述
create_time	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
data_object	**Incident** object	事件实体信息
dataclass_ref	**dataclass_ref** object	数据类对象
format_version	Integer	格式版本 最小值：**0** 最大值：**999**
id	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
project_id	String	当前项目的id 最小长度：**0** 最大长度：**64**
update_time	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为告警发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	参数类型	描述
version	Integer	版本 最小值：**0** 最大值：**999**
workspace_id	String	当前的工作空间id 最小长度：**0** 最大长度：**36**

表 4-174 Incident

参数	参数类型	描述
version	String	事件对象的版本，该字段的值必须为华为云SSA服务确定的官方发布版本之一 最小长度：**0** 最大长度：**64**
id	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
domain_id	String	数据投递后，被委托用户的domain_id 最小长度：**0** 最大长度：**36**
region_id	String	数据投递后，被委托用户的region_id 最小长度：**0** 最大长度：**36**
workspace_id	String	当前的工作空间id 最小长度：**0** 最大长度：**36**
labels	String	标签，仅展示 最小长度：**0** 最大长度：**1024**
environment	**environment** object	事件产生的环境坐标信息
data_source	**data_source** object	首次上报数据源

参数	参数类型	描述
first_observed_time	String	首次发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
last_observed_time	String	最近发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
create_time	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
arrive_time	String	接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
title	String	事件标题 最小长度：**0** 最大长度：**255**
description	String	事件描述信息 最小长度：**0** 最大长度：**1024**
source_url	String	事件URL链接，指向数据源产品中有关当前事件说明的页面 最小长度：**0** 最大长度：**1024**
count	Integer	事件发生次数 最小值：**0** 最大值：**999**

参数	参数类型	描述
confidence	Integer	事件的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100，0表示置信度为0%，100表示置信度为100% 最小值：**0** 最大值：**100**
severity	String	严重性等级，取值范围：Tips | Low | Medium | High | Fatal 说明： 0: Tips – 未发现任何问题。 1: Low – 无需针对问题执行任何操作。 2: Medium – 问题需要处理，但不紧急。 3: High – 问题必须优先处理。 4: Fatal – 问题必须立即处理，以防止产生进一步的损害 最小长度：**3** 最大长度：**6** 枚举值： • **Tips** • **Low** • **Medium** • **High** • **Fatal**
criticality	Integer	关键性，是指事件涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源 最小值：**0** 最大值：**100**
incident_type	**incident_type** object	事件分类，详细定义参考《告警事件类型定义》
network_list	Array of **network_list** objects	网络信息 数组长度：**0 - 999**
resource_list	Array of **resource_list** objects	受影响资源 数组长度：**0 - 999**
remediation	**remediation** object	补救措施

参数	参数类型	描述
verification_state	String	验证状态，标识事件的准确性。可选类型如下：Unknown – 未知 True_Positive – 确认 False_Positive – 误报 默认填写Unknown 最小长度：**32** 最大长度：**64** 枚举值： • **Unknown** • **True_Positive** • **False_Positive**
handle_status	String	事件处理状态，可选类型如下： Open – 打开，默认 Block – 阻塞 Closed – 关闭 默认填写Open 最小长度：**4** 最大长度：**5** 枚举值： • **Open** • **Block** • **Closed**
sla	Integer	约束闭环时间：设置风险接受持续时间。单位：小时 最小值：**0** 最大值：**999**
update_time	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
close_time	String	关闭时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	参数类型	描述
ipdrr_phase	String	周期/处置阶段编号 Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-Activity 最小长度：**0** 最大长度：**64** 枚举值： • **Prepartion** • **Detection and Analysis** • **Containm，Eradication& Recovery** • **Post-Incident-Activity**
simulation	String	调试字段 最小长度：**0** 最大长度：**64**
actor	String	事件调查员 最小长度：**0** 最大长度：**64**
owner	String	责任人、服务责任人 最小长度：**0** 最大长度：**64**
creator	String	创建人 最小长度：**0** 最大长度：**64**
close_reason	String	关闭原因: 误检 - False detection 已解决 - Resolved 重复 - Repeated 其他 - Other 最小长度：**0** 最大长度：**64** 枚举值： • **False detection** • **Resolved** • **Repeated** • **Other**
close_comment	String	关闭评论 最小长度：**0** 最大长度：**1024**
malware	**malware** object	恶意软件
system_info	Object	系统信息

参数	参数类型	描述
process	Array of **process** objects	进程信息 数组长度：**0 - 999**
user_info	Array of **user_info** objects	用户信息 数组长度：**0 - 999**
file_info	Array of **file_info** objects	文件信息 数组长度：**0 - 999**
system_alert_table	Object	事件管理列表的布局字段

表 4-175 environment

参数	参数类型	描述
vendor_type	String	环境供应商：HWCP/HWC/AWS/Azure/GCP 最小长度：**0** 最大长度：**64**
domain_id	String	租户id 最小长度：**0** 最大长度：**64**
region_id	String	区域id，全局服务global 最小长度：**0** 最大长度：**64**
cross_workspace_id	String	数据投递前的源工作空间id，在源空间下值为null，投递后为被委托用户的id 最小长度：**0** 最大长度：**64**
project_id	String	项目id， 全局服务默认null 最小长度：**0** 最大长度：**64**

表 4-176 data_source

参数	参数类型	描述
source_type	Integer	数据源类型，取值范围如下： 1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**1** 最大值：**3** 枚举值： • **1** • **2** • **3**
domain_id	String	数据源产品所属账号的id 最小长度：**0** 最大长度：**36**
project_id	String	数据源产品所属项目的id 最小长度：**0** 最大长度：**64**
region_id	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义，例如cn-north-1 最小长度：**0** 最大长度：**64**
company_name	String	数据源产品所属公司的名称 最小长度：**0** 最大长度：**16**
product_name	String	数据源产品的名称 最小长度：**0** 最大长度：**24**
product_feature	String	产品功能特性名称，用来指明检测到当前事件的产品的功能特性 最小长度：**0** 最大长度：**24**
product_module	String	检测模块列表 最小长度：**0** 最大长度：**1024**

表 4-177 incident_type

参数	参数类型	描述
category	String	类别 最小长度：**0** 最大长度：**1024**
incident_type	String	事件类型 最小长度：**0** 最大长度：**1024**

表 4-178 network_list

参数	参数类型	描述
direction	String	方向，取值范围：IN | OUT 最小长度：**0** 最大长度：**3** 枚举值： • **IN** • **OUT**
protocol	String	协议，包含7层和4层的协议 参考：IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml 最小长度：**0** 最大长度：**64**
src_ip	String	源IP地址 最小长度：**0** 最大长度：**64**
src_port	Integer	源端口，0–65535 最小值：**0** 最大值：**65535**
src_domain	String	源域名 最小长度：**0** 最大长度：**128**
src_geo	**src_geo** object	源IP的地理位置信息

参数	参数类型	描述
dest_ip	String	目的IP地址 最小长度：**32** 最大长度：**64**
dest_port	String	目的端口，0–65535 最小长度：**0** 最大长度：**65535**
dest_domain	String	目的域名 最小长度：**0** 最大长度：**128**
dest_geo	**dest_geo** object	目标IP的地理位置信息

表 4-179 src_geo

参数	参数类型	描述
latitude	Number	纬度 最小值：**0** 最大值：**90**
longitude	Number	经度 最小值：**0** 最大值：**180**
city_code	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-180 dest_geo

参数	参数类型	描述
latitude	Number	纬度 最小值：**0** 最大值：**90**

参数	参数类型	描述
longitude	Number	经度 最小值：**0** 最大值：**180**
city_code	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-181 resource_list

参数	参数类型	描述
id	String	云服务资源id 最小长度：**0** 最大长度：**36**
name	String	资源名称 最小长度：**0** 最大长度：**255**
type	String	资源类型；引用华为云RMS type字段 最小长度：**0** 最大长度：**64**
provider	String	云服务名称；引用华为云RMS provider字段 最小长度：**0** 最大长度：**64**
region_id	String	区域；按照华为云regionId填写，如cn-north-1等 最小长度：**0** 最大长度：**36**
domain_id	String	资源所属账号ID，UUID格式 最小长度：**0** 最大长度：**36**
project_id	String	资源所属项目ID，UUID格式 最小长度：**0** 最大长度：**36**

参数	参数类型	描述
ep_id	String	企业项目id 最小长度：**0** 最大长度：**128**
ep_name	String	企业项目名称 最小长度：**0** 最大长度：**128**
tags	String	资源标签 1、最多50个key/values对 2、values：最大255字符，取值范围：字母数字,空格,+, -, =, ., _, :, /,@ 最小长度：**0** 最大长度：**2048**

表 4-182 remediation

参数	参数类型	描述
recommendation	String	推荐处理方法 最小长度：**0** 最大长度：**128**
url	String	链接，指向该事件的一般修复信息。该URL必须可以从公网访问，不需要提供凭证 最小长度：**0** 最大长度：**2048**

表 4-183 malware

参数	参数类型	描述
malware_family	String	恶意家族 最小长度：**0** 最大长度：**64**
malware_class	String	恶意软件分类 最小长度：**0** 最大长度：**64**

表 4-184 process

参数	参数类型	描述
process_name	String	进程名 最小长度：**0** 最大长度：**64**
process_path	String	进程执行文件路径 最小长度：**0** 最大长度：**512**
process_pid	Integer	进程id 最小值：**0** 最大值：**65535**
process_uid	Integer	进程用户id 最小值：**0** 最大值：**655350**
process_cmdline	String	进程命令行 最小长度：**0** 最大长度：**128**
process_parent_name	String	父进程名称 最小长度：**0** 最大长度：**64**
process_parent_path	String	父进程执行文件路径 最小长度：**0** 最大长度：**512**
process_parent_pid	Integer	父进程id 最小值：**0** 最大值：**65535**
process_parent_uid	Integer	父进程用户id 最小值：**0** 最大值：**655350**
process_parent_cmdline	String	父进程命令行 最小长度：**0** 最大长度：**128**
process_child_name	String	子进程名称 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
process_child_path	String	子进程执行文件路径 最小长度：**0** 最大长度：**512**
process_child_pid	Integer	子进程id 最小值：**0** 最大值：**65535**
process_child_uid	Integer	子进程用户id 最小值：**0** 最大值：**655350**
process_child_cmdline	String	子进程命令行 最小长度：**0** 最大长度：**128**
process_launche_time	String	进程启动时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
process_terminate_time	String	进程结束时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

表 4-185 user_info

参数	参数类型	描述
user_id	String	用户uid 最小长度：**0** 最大长度：**36**
user_name	String	用户名称 最小长度：**32** 最大长度：**64**

表 4-186 file_info

参数	参数类型	描述
file_path	String	文件路径/名称 最小长度：**0** 最大长度：**128**
file_content	String	文件内容 最小长度：**0** 最大长度：**1024**
file_new_path	String	文件新路径/名称 最小长度：**32** 最大长度：**64**
file_hash	String	文件hash 最小长度：**0** 最大长度：**128**
file_md5	String	文件md5 最小长度：**0** 最大长度：**128**
file_sha256	String	文件sha256 最小长度：**0** 最大长度：**128**
file_attr	String	文件属性 最小长度：**0** 最大长度：**1024**

表 4-187 dataclass_ref

参数	参数类型	描述
id	String	数据类唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
name	String	数据类名称 最小长度：**0** 最大长度：**36**

状态码： 400

表 4-188 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-189 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

创建一条事件，事件标题为MyXXX，标签为MyXXX，严重级别为tips，发生次数为4次。

```
{
  "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 – 未知，True_Positive – 确认，False_Positive – 误报。默认填写Unknown",
  "handle_status" : "Open – 打开，Block – 阻塞，Closed – 关闭。默认填写Open",
  "sla" : 60000,
  "update_time" : "2021-01-30T23:00:00Z+0800",
  "close_time" : "2021-01-30T23:00:00Z+0800",
  "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-
Activity",
  "simulation" : "false",
  "actor" : "刘一博",
  "owner" : "MyXXX",
  "creator" : "MyXXX",
  "close_reason" : "误检;已解决;重复;其他",
  "close_comment" : "误检;已解决;重复;其他",
  "malware" : {
    "malware_family" : "family",
    "malware_class" : "恶意占用内存"
  },
  "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"
  }
}
```

响应示例

状态码： 200

创建事件返回body体

```
{
  "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 – 未知，True_Positive – 确认，False_Positive – 误报。默认填写
Unknown",
    "handle_status" : "Open – 打开，Block – 阻塞，Closed – 关闭。默认填写Open",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-
Activity",
    "simulation" : "false",
    "actor" : "刘一博",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "误检;已解决;重复;其他",
    "close_comment" : "误检;已解决;重复;其他",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "恶意占用内存"
    },
    "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 代码示例

SDK代码示例如下。

Java

创建一条事件，事件标题为MyXXX，标签为MyXXX，严重级别为tips，发生次数为4次。

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateIncidentRequest request = new CreateIncidentRequest();
        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("恶意占用内存");
        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 – 未知,True_Positive – 确
```

```
认,False_Positive – 误报。默认填写Unknown"))
            .withHandleStatus(Incident.HandleStatusEnum.fromValue("Open – 打开,Block – 阻塞,Closed – 关闭。默认填写Open"))
            .withSla(60000)
            .withUpdateTime("2021-01-30T23:00:00Z+0800")
            .withCloseTime("2021-01-30T23:00:00Z+0800")
            .withIpdrrPhase(Incident.IpdrrPhaseEnum.fromValue("Prepartion|Detection and Analysis|Containm,Eradication& Recovery| Post-Incident-Activity"))
            .withSimulation("false")
            .withActor("刘一博")
            .withOwner("MyXXX")
            .withCreator("MyXXX")
            .withCloseReason(Incident.CloseReasonEnum.fromValue("误检;已解决;重复;其他"))
            .withCloseComment("误检;已解决;重复;其他")
            .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

创建一条事件，事件标题为MyXXX，标签为MyXXX，严重级别为tips，发生次数为4次。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = CreateIncidentRequest()
        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="恶意占用内存"
)
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 – 未知,True_Positive – 确认,False_Positive – 误报。默认填写Unknown",
            handle_status="Open – 打开,Block – 阻塞,Closed – 关闭。默认填写Open",
            sla=60000,
            update_time="2021-01-30T23:00:00Z+0800",
            close_time="2021-01-30T23:00:00Z+0800",
            ipdrr_phase="Prepartion|Detection and Analysis|Containm,Eradication& Recovery| Post-Incident-
Activity",
            simulation="false",
            actor="刘一博",
            owner="MyXXX",
            creator="MyXXX",
            close_reason="误检;已解决;重复;其他",
            close_comment="误检;已解决;重复;其他",
            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

创建一条事件，事件标题为MyXXX，标签为MyXXX，严重级别为tips，发生次数为4次。

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateIncidentRequest{}
    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:= "恶意占用内存"
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_-_未
知,TRUE_POSITIVE_-_确认,FALSE_POSITIVE_-_误报。默认填写UNKNOWN
    handleStatusDataObject:= model.GetIncidentHandleStatusEnum().OPEN_-_打开,BLOCK_-_阻塞,CLOSED_-
_关闭。默认填写OPEN
    slaDataObject:= int32(60000)
    updateTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    closeTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    ipdrrPhaseDataObject:= model.GetIncidentIpdrrPhaseEnum().PREPARTION|DETECTION_AND_ANALYSIS|
CONTAINM,ERADICATION&_RECOVERY|_POST_INCIDENT_ACTIVITY
    simulationDataObject:= "false"
    actorDataObject:= "刘一博"
    ownerDataObject:= "MyXXX"
    creatorDataObject:= "MyXXX"
    closeReasonDataObject:= model.GetIncidentCloseReasonEnum().误检;已解决;重复;其他
    closeCommentDataObject:= "误检;已解决;重复;其他"
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	创建事件返回body体
400	创建事件错误返回body体

错误码

请参见**错误码**。

4.2.3 删除事件

功能介绍

删除事件

调用方法

请参见**如何调用API**。

URI

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

表 4-190 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**

请求参数

表 4-191 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

表 4-192 请求 Body 参数

参数	是否必选	参数类型	描述
batch_ids	否	Array of strings	删除事件的ID列表 最小长度：**0** 最大长度：**100** 数组长度：**0 - 999**

响应参数

状态码： 200

表 4-193 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-194 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误信息 最小长度：**0** 最大长度：**1024**
data	**data** object	批量删除事件返回对象

表 4-195 data

参数	参数类型	描述
error_ids	Array of strings	失败id 最小长度：**0** 最大长度：**100** 数组长度：**0 - 100**

参数	参数类型	描述
success_ids	Array of strings	成功id 最小长度：**0** 最大长度：**100** 数组长度：**0 - 100**

状态码： 400

表 4-196 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-197 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

删除id为909494e3-558e-46b6-a9eb-07a8e18ca621的事件

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

响应示例

状态码： 200

事件删除结果

```
{
  "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 代码示例

SDK代码示例如下。

Java

删除id为909494e3-558e-46b6-a9eb-07a8e18ca621的事件

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteIncidentRequest request = new DeleteIncidentRequest();
        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

删除id为909494e3-558e-46b6-a9eb-07a8e18ca621的事件

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = DeleteIncidentRequest()
        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

删除id为909494e3-558e-46b6-a9eb-07a8e18ca621的事件

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
```

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

    request := &model.DeleteIncidentRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	事件删除结果
400	删除事件错误返回body体

错误码

请参见**错误码**。

4.2.4 获取事件详情

功能介绍

获取事件详情

调用方法

请参见**如何调用API**。

URI

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

表 4-198 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**
incident_id	是	String	事件ID 最小长度：**32** 最大长度：**36**

请求参数

表 4-199 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

响应参数

状态码： 200

表 4-200 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
message	String	错误信息 最小长度：**0** 最大长度：**1024**
data	**IncidentDetail** object	

表 4-201 IncidentDetail

参数	参数类型	描述
create_time	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
data_object	**Incident** object	事件实体信息
dataclass_ref	**dataclass_ref** object	数据类对象
format_version	Integer	格式版本 最小值：**0** 最大值：**999**
id	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
project_id	String	当前项目的id 最小长度：**0** 最大长度：**64**
update_time	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为告警发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
version	Integer	版本 最小值：**0** 最大值：**999**

参数	参数类型	描述
workspace_id	String	当前的工作空间id 最小长度：**0** 最大长度：**36**

表 4-202 Incident

参数	参数类型	描述
version	String	事件对象的版本，该字段的值必须为华为云SSA服务确定的官方发布版本之一 最小长度：**0** 最大长度：**64**
id	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
domain_id	String	数据投递后，被委托用户的domain_id 最小长度：**0** 最大长度：**36**
region_id	String	数据投递后，被委托用户的region_id 最小长度：**0** 最大长度：**36**
workspace_id	String	当前的工作空间id 最小长度：**0** 最大长度：**36**
labels	String	标签，仅展示 最小长度：**0** 最大长度：**1024**
environment	**environment** object	事件产生的环境坐标信息
data_source	**data_source** object	首次上报数据源
first_observed_time	String	首次发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	参数类型	描述
last_observed_time	String	最近发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
create_time	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
arrive_time	String	接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
title	String	事件标题 最小长度：**0** 最大长度：**255**
description	String	事件描述信息 最小长度：**0** 最大长度：**1024**
source_url	String	事件URL链接，指向数据源产品中有关当前事件说明的页面 最小长度：**0** 最大长度：**1024**
count	Integer	事件发生次数 最小值：**0** 最大值：**999**
confidence	Integer	事件的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100，0表示置信度为0%，100表示置信度为100% 最小值：**0** 最大值：**100**

参数	参数类型	描述
severity	String	严重性等级，取值范围：Tips | Low | Medium | High | Fatal 说明： 0: Tips – 未发现任何问题。 1: Low – 无需针对问题执行任何操作。 2: Medium – 问题需要处理，但不紧急。 3: High – 问题必须优先处理。 4: Fatal – 问题必须立即处理，以防止产生进一步的损害 最小长度：**3** 最大长度：**6** 枚举值： • **Tips** • **Low** • **Medium** • **High** • **Fatal**
criticality	Integer	关键性，是指事件涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源 最小值：**0** 最大值：**100**
incident_type	**incident_type** object	事件分类，详细定义参考《 告警事件类型定义 》
network_list	Array of **network_list** objects	网络信息 数组长度：**0 - 999**
resource_list	Array of **resource_list** objects	受影响资源 数组长度：**0 - 999**
remediation	**remediation** object	补救措施
verification_state	String	验证状态，标识事件的准确性。可选类型如下：Unknown – 未知 True_Positive – 确认 False_Positive – 误报 默认填写Unknown 最小长度：**32** 最大长度：**64** 枚举值： • **Unknown** • **True_Positive** • **False_Positive**

参数	参数类型	描述
handle_status	String	事件处理状态，可选类型如下： Open – 打开，默认 Block – 阻塞 Closed – 关闭 默认填写Open 最小长度：**4** 最大长度：**5** 枚举值： • **Open** • **Block** • **Closed**
sla	Integer	约束闭环时间：设置风险接受持续时间。单位：小时 最小值：**0** 最大值：**999**
update_time	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
close_time	String	关闭时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
ipdrr_phase	String	周期/处置阶段编号 Prepartion|Detection and Analysis|Containm，Eradication& Recovery|Post-Incident-Activity 最小长度：**0** 最大长度：**64** 枚举值： • **Prepartion** • **Detection and Analysis** • **Containm，Eradication& Recovery** • **Post-Incident-Activity**
simulation	String	调试字段 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
actor	String	事件调查员 最小长度：**0** 最大长度：**64**
owner	String	责任人、服务责任人 最小长度：**0** 最大长度：**64**
creator	String	创建人 最小长度：**0** 最大长度：**64**
close_reason	String	关闭原因: 误检 - False detection 已解决 - Resolved 重复 - Repeated 其他 - Other 最小长度：**0** 最大长度：**64** 枚举值： • **False detection** • **Resolved** • **Repeated** • **Other**
close_comment	String	关闭评论 最小长度：**0** 最大长度：**1024**
malware	**malware** object	恶意软件
system_info	Object	系统信息
process	Array of **process** objects	进程信息 数组长度：**0 - 999**
user_info	Array of **user_info** objects	用户信息 数组长度：**0 - 999**
file_info	Array of **file_info** objects	文件信息 数组长度：**0 - 999**
system_alert_table	Object	事件管理列表的布局字段

表 4-203 environment

参数	参数类型	描述
vendor_type	String	环境供应商：HWCP/HWC/AWS/Azure/GCP 最小长度：**0** 最大长度：**64**
domain_id	String	租户id 最小长度：**0** 最大长度：**64**
region_id	String	区域id，全局服务global 最小长度：**0** 最大长度：**64**
cross_workspace_id	String	数据投递前的源工作空间id，在源空间下值为null，投递后为被委托用户的id 最小长度：**0** 最大长度：**64**
project_id	String	项目id， 全局服务默认null 最小长度：**0** 最大长度：**64**

表 4-204 data_source

参数	参数类型	描述
source_type	Integer	数据源类型，取值范围如下： 1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**1** 最大值：**3** 枚举值： • **1** • **2** • **3**
domain_id	String	数据源产品所属账号的id 最小长度：**0** 最大长度：**36**
project_id	String	数据源产品所属项目的id 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
region_id	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义，例如cn-north-1 最小长度：**0** 最大长度：**64**
company_name	String	数据源产品所属公司的名称 最小长度：**0** 最大长度：**16**
product_name	String	数据源产品的名称 最小长度：**0** 最大长度：**24**
product_feature	String	产品功能特性名称，用来指明检测到当前事件的产品的功能特性 最小长度：**0** 最大长度：**24**
product_module	String	检测模块列表 最小长度：**0** 最大长度：**1024**

表 4-205 incident_type

参数	参数类型	描述
category	String	类别 最小长度：**0** 最大长度：**1024**
incident_type	String	事件类型 最小长度：**0** 最大长度：**1024**

表 4-206 network_list

参数	参数类型	描述
direction	String	方向，取值范围：IN | OUT 最小长度：**0** 最大长度：**3** 枚举值： • **IN** • **OUT**
protocol	String	协议，包含7层和4层的协议 参考：IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml 最小长度：**0** 最大长度：**64**
src_ip	String	源IP地址 最小长度：**0** 最大长度：**64**
src_port	Integer	源端口，0–65535 最小值：**0** 最大值：**65535**
src_domain	String	源域名 最小长度：**0** 最大长度：**128**
src_geo	**src_geo** object	源IP的地理位置信息
dest_ip	String	目的IP地址 最小长度：**32** 最大长度：**64**
dest_port	String	目的端口，0–65535 最小长度：**0** 最大长度：**65535**
dest_domain	String	目的域名 最小长度：**0** 最大长度：**128**
dest_geo	**dest_geo** object	目标IP的地理位置信息

表 4-207 src_geo

参数	参数类型	描述
latitude	Number	纬度 最小值：**0** 最大值：**90**
longitude	Number	经度 最小值：**0** 最大值：**180**
city_code	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-208 dest_geo

参数	参数类型	描述
latitude	Number	纬度 最小值：**0** 最大值：**90**
longitude	Number	经度 最小值：**0** 最大值：**180**
city_code	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-209 resource_list

参数	参数类型	描述
id	String	云服务资源id 最小长度：**0** 最大长度：**36**
name	String	资源名称 最小长度：**0** 最大长度：**255**
type	String	资源类型；引用华为云RMS type字段 最小长度：**0** 最大长度：**64**
provider	String	云服务名称；引用华为云RMS provider字段 最小长度：**0** 最大长度：**64**
region_id	String	区域；按照华为云regionId填写，如cn-north-1等 最小长度：**0** 最大长度：**36**
domain_id	String	资源所属账号ID，UUID格式 最小长度：**0** 最大长度：**36**
project_id	String	资源所属项目ID，UUID格式 最小长度：**0** 最大长度：**36**
ep_id	String	企业项目id 最小长度：**0** 最大长度：**128**
ep_name	String	企业项目名称 最小长度：**0** 最大长度：**128**
tags	String	资源标签 1、最多50个key/values对 2、values：最大255字符，取值范围：字母数字,空格,+, -, =, ., _, :, /,@ 最小长度：**0** 最大长度：**2048**

表 4-210 remediation

参数	参数类型	描述
recommendation	String	推荐处理方法 最小长度：**0** 最大长度：**128**
url	String	链接，指向该事件的一般修复信息。该URL必须可以从公网访问，不需要提供凭证 最小长度：**0** 最大长度：**2048**

表 4-211 malware

参数	参数类型	描述
malware_family	String	恶意家族 最小长度：**0** 最大长度：**64**
malware_class	String	恶意软件分类 最小长度：**0** 最大长度：**64**

表 4-212 process

参数	参数类型	描述
process_name	String	进程名 最小长度：**0** 最大长度：**64**
process_path	String	进程执行文件路径 最小长度：**0** 最大长度：**512**
process_pid	Integer	进程id 最小值：**0** 最大值：**65535**
process_uid	Integer	进程用户id 最小值：**0** 最大值：**655350**

参数	参数类型	描述
process_cmdline	String	进程命令行 最小长度：**0** 最大长度：**128**
process_parent_name	String	父进程名称 最小长度：**0** 最大长度：**64**
process_parent_path	String	父进程执行文件路径 最小长度：**0** 最大长度：**512**
process_parent_pid	Integer	父进程id 最小值：**0** 最大值：**65535**
process_parent_uid	Integer	父进程用户id 最小值：**0** 最大值：**655350**
process_parent_cmdline	String	父进程命令行 最小长度：**0** 最大长度：**128**
process_child_name	String	子进程名称 最小长度：**0** 最大长度：**64**
process_child_path	String	子进程执行文件路径 最小长度：**0** 最大长度：**512**
process_child_pid	Integer	子进程id 最小值：**0** 最大值：**65535**
process_child_uid	Integer	子进程用户id 最小值：**0** 最大值：**655350**
process_child_cmdline	String	子进程命令行 最小长度：**0** 最大长度：**128**

参数	参数类型	描述
process_launche_time	String	进程启动时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
process_terminate_time	String	进程结束时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

表 4-213 user_info

参数	参数类型	描述
user_id	String	用户uid 最小长度：**0** 最大长度：**36**
user_name	String	用户名称 最小长度：**32** 最大长度：**64**

表 4-214 file_info

参数	参数类型	描述
file_path	String	文件路径/名称 最小长度：**0** 最大长度：**128**
file_content	String	文件内容 最小长度：**0** 最大长度：**1024**
file_new_path	String	文件新路径/名称 最小长度：**32** 最大长度：**64**

参数	参数类型	描述
file_hash	String	文件hash 最小长度：**0** 最大长度：**128**
file_md5	String	文件md5 最小长度：**0** 最大长度：**128**
file_sha256	String	文件sha256 最小长度：**0** 最大长度：**128**
file_attr	String	文件属性 最小长度：**0** 最大长度：**1024**

表 4-215 dataclass_ref

参数	参数类型	描述
id	String	数据类唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
name	String	数据类名称 最小长度：**0** 最大长度：**36**

状态码： 400

表 4-216 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

获取事件详情返回body体


```
{
  "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 – 未知，True_Positive – 确认，False_Positive – 误报。默认填写
Unknown",
    "handle_status" : "Open – 打开，Block – 阻塞，Closed – 关闭。默认填写Open",
    "sla" : 60000,
    "update_time" : "2021-01-30T23:00:00Z+0800",
    "close_time" : "2021-01-30T23:00:00Z+0800",
    "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-
Activity",
    "simulation" : "false",
    "actor" : "刘一博",
    "owner" : "MyXXX",
    "creator" : "MyXXX",
    "close_reason" : "误检;已解决;重复;其他",
    "close_comment" : "误检;已解决;重复;其他",
    "malware" : {
      "malware_family" : "family",
      "malware_class" : "恶意占用内存"
    },
    "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 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowIncidentRequest request = new ShowIncidentRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
```



```
        request = ShowIncidentRequest()
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	获取事件详情返回body体
400	获取事件详情错误返回body体

错误码

请参见**错误码**。

4.2.5 更新事件

功能介绍

编辑事件，根据实际修改的属性更新，未修改的列不更新

调用方法

请参见**如何调用API**。

URI

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

表 4-217 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**
incident_id	是	String	事件ID 最小长度：**32** 最大长度：**36**

请求参数

表 4-218 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**

参数	是否必选	参数类型	描述
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

表 4-219 请求 Body 参数

参数	是否必选	参数类型	描述
batch_ids	否	Array of strings	更新事件的ID列表 最小长度：**0** 最大长度：**100** 数组长度：**0 - 999**
data_object	否	**Incident** object	事件实体信息

表 4-220 Incident

参数	是否必选	参数类型	描述
version	否	String	事件对象的版本，该字段的值必须为华为云SSA服务确定的官方发布版本之一 最小长度：**0** 最大长度：**64**
id	否	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
domain_id	否	String	数据投递后，被委托用户的domain_id 最小长度：**0** 最大长度：**36**
region_id	否	String	数据投递后，被委托用户的region_id 最小长度：**0** 最大长度：**36**

参数	是否必选	参数类型	描述
workspace_id	否	String	当前的工作空间id 最小长度：**0** 最大长度：**36**
labels	否	String	标签，仅展示 最小长度：**0** 最大长度：**1024**
environment	否	**environment** object	事件产生的环境坐标信息
data_source	否	**data_source** object	首次上报数据源
first_observed_time	否	String	首次发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
last_observed_time	否	String	最近发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
create_time	否	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
arrive_time	否	String	接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	是否必选	参数类型	描述
title	否	String	事件标题 最小长度：**0** 最大长度：**255**
description	否	String	事件描述信息 最小长度：**0** 最大长度：**1024**
source_url	否	String	事件URL链接，指向数据源产品中有关当前事件说明的页面 最小长度：**0** 最大长度：**1024**
count	否	Integer	事件发生次数 最小值：**0** 最大值：**999**
confidence	否	Integer	事件的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100，0表示置信度为0%，100表示置信度为100% 最小值：**0** 最大值：**100**
severity	否	String	严重性等级，取值范围：Tips | Low | Medium | High | Fatal 说明： 0: Tips – 未发现任何问题。 1: Low – 无需针对问题执行任何操作。 2: Medium – 问题需要处理，但不紧急。 3: High – 问题必须优先处理。 4: Fatal – 问题必须立即处理，以防止产生进一步的损害 最小长度：**3** 最大长度：**6** 枚举值： • **Tips** • **Low** • **Medium** • **High** • **Fatal**

参数	是否必选	参数类型	描述
criticality	否	Integer	关键性，是指事件涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源 最小值：**0** 最大值：**100**
incident_type	否	**incident_type** object	事件分类，详细定义参考《告警事件类型定义》
network_list	否	Array of **network_list** objects	网络信息 数组长度：**0 - 999**
resource_list	否	Array of **resource_list** objects	受影响资源 数组长度：**0 - 999**
remediation	否	**remediation** object	补救措施
verification_state	否	String	验证状态，标识事件的准确性。可选类型如下： Unknown – 未知 True_Positive – 确认 False_Positive – 误报 默认填写 Unknown 最小长度：**32** 最大长度：**64** 枚举值： • **Unknown** • **True_Positive** • **False_Positive**
handle_status	否	String	事件处理状态，可选类型如下：Open – 打开，默认 Block – 阻塞 Closed – 关闭 默认填写 Open 最小长度：**4** 最大长度：**5** 枚举值： • **Open** • **Block** • **Closed**

参数	是否必选	参数类型	描述
sla	否	Integer	约束闭环时间：设置风险接受持续时间。单位：小时 最小值：**0** 最大值：**999**
update_time	否	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
close_time	否	String	关闭时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
ipdrr_phase	否	String	周期/处置阶段编号 Prepartion|Detection and Analysis|Containm，Eradication&Recovery|Post-Incident-Activity 最小长度：**0** 最大长度：**64** 枚举值： • **Prepartion** • **Detection and Analysis** • **Containm，Eradication&Recovery** • **Post-Incident-Activity**
simulation	否	String	调试字段 最小长度：**0** 最大长度：**64**
actor	否	String	事件调查员 最小长度：**0** 最大长度：**64**
owner	否	String	责任人、服务责任人 最小长度：**0** 最大长度：**64**

参数	是否必选	参数类型	描述
creator	否	String	创建人 最小长度：**0** 最大长度：**64**
close_reason	否	String	关闭原因: 误检 - False detection 已解决 - Resolved 重复 - Repeated 其他 - Other 最小长度：**0** 最大长度：**64** 枚举值： • **False detection** • **Resolved** • **Repeated** • **Other**
close_comment	否	String	关闭评论 最小长度：**0** 最大长度：**1024**
malware	否	**malware** object	恶意软件
system_info	否	Object	系统信息
process	否	Array of **process** objects	进程信息 数组长度：**0 - 999**
user_info	否	Array of **user_info** objects	用户信息 数组长度：**0 - 999**
file_info	否	Array of **file_info** objects	文件信息 数组长度：**0 - 999**
system_alert_table	否	Object	事件管理列表的布局字段

表 4-221 environment

参数	是否必选	参数类型	描述
vendor_type	否	String	环境供应商：HWCP/HWC/AWS/Azure/GCP 最小长度：**0** 最大长度：**64**

参数	是否必选	参数类型	描述
domain_id	否	String	租户id 最小长度：**0** 最大长度：**64**
region_id	否	String	区域id，全局服务global 最小长度：**0** 最大长度：**64**
cross_workspace_id	否	String	数据投递前的源工作空间id，在源空间下值为null，投递后为被委托用户的id 最小长度：**0** 最大长度：**64**
project_id	否	String	项目id， 全局服务默认null 最小长度：**0** 最大长度：**64**

表 4-222 data_source

参数	是否必选	参数类型	描述
source_type	否	Integer	数据源类型，取值范围如下： 1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**1** 最大值：**3** 枚举值： • **1** • **2** • **3**
domain_id	否	String	数据源产品所属账号的id 最小长度：**0** 最大长度：**36**
project_id	否	String	数据源产品所属项目的id 最小长度：**0** 最大长度：**64**

参数	是否必选	参数类型	描述
region_id	否	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义，例如cn-north-1 最小长度：**0** 最大长度：**64**
company_name	否	String	数据源产品所属公司的名称 最小长度：**0** 最大长度：**16**
product_name	否	String	数据源产品的名称 最小长度：**0** 最大长度：**24**
product_feature	否	String	产品功能特性名称，用来指明检测到当前事件的产品的功能特性 最小长度：**0** 最大长度：**24**
product_module	否	String	检测模块列表 最小长度：**0** 最大长度：**1024**

表 4-223 incident_type

参数	是否必选	参数类型	描述
category	否	String	类别 最小长度：**0** 最大长度：**1024**
incident_type	否	String	事件类型 最小长度：**0** 最大长度：**1024**

表 4-224 network_list

参数	是否必选	参数类型	描述
direction	否	String	方向，取值范围：IN | OUT 最小长度：**0** 最大长度：**3** 枚举值： • **IN** • **OUT**
protocol	否	String	协议，包含7层和4层的协议 参考：IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml 最小长度：**0** 最大长度：**64**
src_ip	否	String	源IP地址 最小长度：**0** 最大长度：**64**
src_port	否	Integer	源端口，0–65535 最小值：**0** 最大值：**65535**
src_domain	否	String	源域名 最小长度：**0** 最大长度：**128**
src_geo	否	**src_geo** object	源IP的地理位置信息
dest_ip	否	String	目的IP地址 最小长度：**32** 最大长度：**64**
dest_port	否	String	目的端口，0–65535 最小长度：**0** 最大长度：**65535**
dest_domain	否	String	目的域名 最小长度：**0** 最大长度：**128**
dest_geo	否	**dest_geo** object	目标IP的地理位置信息

表 4-225 src_geo

参数	是否必选	参数类型	描述
latitude	否	Number	纬度 最小值：**0** 最大值：**90**
longitude	否	Number	经度 最小值：**0** 最大值：**180**
city_code	否	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	否	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-226 dest_geo

参数	是否必选	参数类型	描述
latitude	否	Number	纬度 最小值：**0** 最大值：**90**
longitude	否	Number	经度 最小值：**0** 最大值：**180**
city_code	否	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	否	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-227 resource_list

参数	是否必选	参数类型	描述
id	否	String	云服务资源id 最小长度：**0** 最大长度：**36**
name	否	String	资源名称 最小长度：**0** 最大长度：**255**
type	否	String	资源类型；引用华为云RMS type字段 最小长度：**0** 最大长度：**64**
provider	否	String	云服务名称；引用华为云RMS provider字段 最小长度：**0** 最大长度：**64**
region_id	否	String	区域；按照华为云regionId填写，如cn-north-1等 最小长度：**0** 最大长度：**36**
domain_id	否	String	资源所属账号ID，UUID格式 最小长度：**0** 最大长度：**36**
project_id	否	String	资源所属项目ID，UUID格式 最小长度：**0** 最大长度：**36**
ep_id	否	String	企业项目id 最小长度：**0** 最大长度：**128**
ep_name	否	String	企业项目名称 最小长度：**0** 最大长度：**128**
tags	否	String	资源标签 1、最多50个key/values对 2、values：最大255字符，取值范围：字母数字,空格,+, -, =, ., _, :, /,@ 最小长度：**0** 最大长度：**2048**

表 4-228 remediation

参数	是否必选	参数类型	描述
recommendation	否	String	推荐处理方法 最小长度：**0** 最大长度：**128**
url	否	String	链接，指向该事件的一般修复信息。该URL必须可以从公网访问，不需要提供凭证 最小长度：**0** 最大长度：**2048**

表 4-229 malware

参数	是否必选	参数类型	描述
malware_family	否	String	恶意家族 最小长度：**0** 最大长度：**64**
malware_class	否	String	恶意软件分类 最小长度：**0** 最大长度：**64**

表 4-230 process

参数	是否必选	参数类型	描述
process_name	否	String	进程名 最小长度：**0** 最大长度：**64**
process_path	否	String	进程执行文件路径 最小长度：**0** 最大长度：**512**
process_pid	否	Integer	进程id 最小值：**0** 最大值：**65535**

参数	是否必选	参数类型	描述
process_uid	否	Integer	进程用户id 最小值：**0** 最大值：**655350**
process_cmdline	否	String	进程命令行 最小长度：**0** 最大长度：**128**
process_parent_name	否	String	父进程名称 最小长度：**0** 最大长度：**64**
process_parent_path	否	String	父进程执行文件路径 最小长度：**0** 最大长度：**512**
process_parent_pid	否	Integer	父进程id 最小值：**0** 最大值：**65535**
process_parent_uid	否	Integer	父进程用户id 最小值：**0** 最大值：**655350**
process_parent_cmdline	否	String	父进程命令行 最小长度：**0** 最大长度：**128**
process_child_name	否	String	子进程名称 最小长度：**0** 最大长度：**64**
process_child_path	否	String	子进程执行文件路径 最小长度：**0** 最大长度：**512**
process_child_pid	否	Integer	子进程id 最小值：**0** 最大值：**65535**
process_child_uid	否	Integer	子进程用户id 最小值：**0** 最大值：**655350**

参数	是否必选	参数类型	描述
process_child_cmdline	否	String	子进程命令行 最小长度：**0** 最大长度：**128**
process_launche_time	否	String	进程启动时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
process_terminate_time	否	String	进程结束时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

表 4-231 user_info

参数	是否必选	参数类型	描述
user_id	否	String	用户uid 最小长度：**0** 最大长度：**36**
user_name	否	String	用户名称 最小长度：**32** 最大长度：**64**

表 4-232 file_info

参数	是否必选	参数类型	描述
file_path	否	String	文件路径/名称 最小长度：**0** 最大长度：**128**
file_content	否	String	文件内容 最小长度：**0** 最大长度：**1024**

参数	是否必选	参数类型	描述
file_new_path	否	String	文件新路径/名称 最小长度：**32** 最大长度：**64**
file_hash	否	String	文件hash 最小长度：**0** 最大长度：**128**
file_md5	否	String	文件md5 最小长度：**0** 最大长度：**128**
file_sha256	否	String	文件sha256 最小长度：**0** 最大长度：**128**
file_attr	否	String	文件属性 最小长度：**0** 最大长度：**1024**

响应参数

状态码： 200

表 4-233 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-234 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误信息 最小长度：**0** 最大长度：**1024**

参数	参数类型	描述
data	IncidentDetail object	

表 4-235 IncidentDetail

参数	参数类型	描述
create_time	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
data_object	Incident object	事件实体信息
dataclass_ref	dataclass_ref object	数据类对象
format_version	Integer	格式版本 最小值：**0** 最大值：**999**
id	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
project_id	String	当前项目的id 最小长度：**0** 最大长度：**64**
update_time	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为告警发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
version	Integer	版本 最小值：**0** 最大值：**999**
workspace_id	String	当前的工作空间id 最小长度：**0** 最大长度：**36**

表 4-236 Incident

参数	参数类型	描述
version	String	事件对象的版本，该字段的值必须为华为云SSA服务确定的官方发布版本之一 最小长度：**0** 最大长度：**64**
id	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
domain_id	String	数据投递后，被委托用户的domain_id 最小长度：**0** 最大长度：**36**
region_id	String	数据投递后，被委托用户的region_id 最小长度：**0** 最大长度：**36**
workspace_id	String	当前的工作空间id 最小长度：**0** 最大长度：**36**
labels	String	标签，仅展示 最小长度：**0** 最大长度：**1024**
environment	**environment** object	事件产生的环境坐标信息
data_source	**data_source** object	首次上报数据源
first_observed_time	String	首次发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
last_observed_time	String	最近发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	参数类型	描述
create_time	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
arrive_time	String	接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
title	String	事件标题 最小长度：**0** 最大长度：**255**
description	String	事件描述信息 最小长度：**0** 最大长度：**1024**
source_url	String	事件URL链接，指向数据源产品中有关当前事件说明的页面 最小长度：**0** 最大长度：**1024**
count	Integer	事件发生次数 最小值：**0** 最大值：**999**
confidence	Integer	事件的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100，0表示置信度为0%，100表示置信度为100% 最小值：**0** 最大值：**100**

参数	参数类型	描述
severity	String	严重性等级，取值范围：Tips | Low | Medium | High | Fatal 说明： 0: Tips – 未发现任何问题。 1: Low – 无需针对问题执行任何操作。 2: Medium – 问题需要处理，但不紧急。 3: High – 问题必须优先处理。 4: Fatal – 问题必须立即处理，以防止产生进一步的损害 最小长度：**3** 最大长度：**6** 枚举值： • **Tips** • **Low** • **Medium** • **High** • **Fatal**
criticality	Integer	关键性，是指事件涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源 最小值：**0** 最大值：**100**
incident_type	**incident_type** object	事件分类，详细定义参考《 告警事件类型定义 》
network_list	Array of **network_list** objects	网络信息 数组长度：**0 - 999**
resource_list	Array of **resource_list** objects	受影响资源 数组长度：**0 - 999**
remediation	**remediation** object	补救措施
verification_state	String	验证状态，标识事件的准确性。可选类型如下：Unknown – 未知 True_Positive – 确认 False_Positive – 误报 默认填写Unknown 最小长度：**32** 最大长度：**64** 枚举值： • **Unknown** • **True_Positive** • **False_Positive**

参数	参数类型	描述
handle_status	String	事件处理状态，可选类型如下： Open – 打开，默认 Block – 阻塞 Closed – 关闭 默认填写Open 最小长度：**4** 最大长度：**5** 枚举值： • **Open** • **Block** • **Closed**
sla	Integer	约束闭环时间：设置风险接受持续时间。单位：小时 最小值：**0** 最大值：**999**
update_time	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
close_time	String	关闭时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
ipdrr_phase	String	周期/处置阶段编号 Prepartion|Detection and Analysis|Containm，Eradication& Recovery|Post-Incident-Activity 最小长度：**0** 最大长度：**64** 枚举值： • **Prepartion** • **Detection and Analysis** • **Containm，Eradication& Recovery** • **Post-Incident-Activity**
simulation	String	调试字段 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
actor	String	事件调查员 最小长度：**0** 最大长度：**64**
owner	String	责任人、服务责任人 最小长度：**0** 最大长度：**64**
creator	String	创建人 最小长度：**0** 最大长度：**64**
close_reason	String	关闭原因: 误检 - False detection 已解决 - Resolved 重复 - Repeated 其他 - Other 最小长度：**0** 最大长度：**64** 枚举值： • **False detection** • **Resolved** • **Repeated** • **Other**
close_comment	String	关闭评论 最小长度：**0** 最大长度：**1024**
malware	**malware** object	恶意软件
system_info	Object	系统信息
process	Array of **process** objects	进程信息 数组长度：**0 - 999**
user_info	Array of **user_info** objects	用户信息 数组长度：**0 - 999**
file_info	Array of **file_info** objects	文件信息 数组长度：**0 - 999**
system_alert_table	Object	事件管理列表的布局字段

表 4-237 environment

参数	参数类型	描述
vendor_type	String	环境供应商：HWCP/HWC/AWS/Azure/GCP 最小长度：**0** 最大长度：**64**
domain_id	String	租户id 最小长度：**0** 最大长度：**64**
region_id	String	区域id，全局服务global 最小长度：**0** 最大长度：**64**
cross_workspace_id	String	数据投递前的源工作空间id，在源空间下值为null，投递后为被委托用户的id 最小长度：**0** 最大长度：**64**
project_id	String	项目id， 全局服务默认null 最小长度：**0** 最大长度：**64**

表 4-238 data_source

参数	参数类型	描述
source_type	Integer	数据源类型，取值范围如下： 1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**1** 最大值：**3** 枚举值： • **1** • **2** • **3**
domain_id	String	数据源产品所属账号的id 最小长度：**0** 最大长度：**36**
project_id	String	数据源产品所属项目的id 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
region_id	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义，例如cn-north-1 最小长度：**0** 最大长度：**64**
company_name	String	数据源产品所属公司的名称 最小长度：**0** 最大长度：**16**
product_name	String	数据源产品的名称 最小长度：**0** 最大长度：**24**
product_feature	String	产品功能特性名称，用来指明检测到当前事件的产品的功能特性 最小长度：**0** 最大长度：**24**
product_module	String	检测模块列表 最小长度：**0** 最大长度：**1024**

表 4-239 incident_type

参数	参数类型	描述
category	String	类别 最小长度：**0** 最大长度：**1024**
incident_type	String	事件类型 最小长度：**0** 最大长度：**1024**

表 4-240 network_list

参数	参数类型	描述
direction	String	方向，取值范围：IN | OUT 最小长度：**0** 最大长度：**3** 枚举值： • **IN** • **OUT**
protocol	String	协议，包含7层和4层的协议 参考：IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml 最小长度：**0** 最大长度：**64**
src_ip	String	源IP地址 最小长度：**0** 最大长度：**64**
src_port	Integer	源端口，0–65535 最小值：**0** 最大值：**65535**
src_domain	String	源域名 最小长度：**0** 最大长度：**128**
src_geo	**src_geo** object	源IP的地理位置信息
dest_ip	String	目的IP地址 最小长度：**32** 最大长度：**64**
dest_port	String	目的端口，0–65535 最小长度：**0** 最大长度：**65535**
dest_domain	String	目的域名 最小长度：**0** 最大长度：**128**
dest_geo	**dest_geo** object	目标IP的地理位置信息

表 4-241 src_geo

参数	参数类型	描述
latitude	Number	纬度 最小值：**0** 最大值：**90**
longitude	Number	经度 最小值：**0** 最大值：**180**
city_code	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-242 dest_geo

参数	参数类型	描述
latitude	Number	纬度 最小值：**0** 最大值：**90**
longitude	Number	经度 最小值：**0** 最大值：**180**
city_code	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-243 resource_list

参数	参数类型	描述
id	String	云服务资源id 最小长度：**0** 最大长度：**36**
name	String	资源名称 最小长度：**0** 最大长度：**255**
type	String	资源类型；引用华为云RMS type字段 最小长度：**0** 最大长度：**64**
provider	String	云服务名称；引用华为云RMS provider字段 最小长度：**0** 最大长度：**64**
region_id	String	区域；按照华为云regionId填写，如cn-north-1等 最小长度：**0** 最大长度：**36**
domain_id	String	资源所属账号ID，UUID格式 最小长度：**0** 最大长度：**36**
project_id	String	资源所属项目ID，UUID格式 最小长度：**0** 最大长度：**36**
ep_id	String	企业项目id 最小长度：**0** 最大长度：**128**
ep_name	String	企业项目名称 最小长度：**0** 最大长度：**128**
tags	String	资源标签 1、最多50个key/values对 2、values：最大255字符，取值范围：字母数字,空格,+, -, =, ., _, :, /,@ 最小长度：**0** 最大长度：**2048**

表 4-244 remediation

参数	参数类型	描述
recommendation	String	推荐处理方法 最小长度：**0** 最大长度：**128**
url	String	链接，指向该事件的一般修复信息。该URL必须可以从公网访问，不需要提供凭证 最小长度：**0** 最大长度：**2048**

表 4-245 malware

参数	参数类型	描述
malware_family	String	恶意家族 最小长度：**0** 最大长度：**64**
malware_class	String	恶意软件分类 最小长度：**0** 最大长度：**64**

表 4-246 process

参数	参数类型	描述
process_name	String	进程名 最小长度：**0** 最大长度：**64**
process_path	String	进程执行文件路径 最小长度：**0** 最大长度：**512**
process_pid	Integer	进程id 最小值：**0** 最大值：**65535**
process_uid	Integer	进程用户id 最小值：**0** 最大值：**655350**

参数	参数类型	描述
process_cmdline	String	进程命令行 最小长度：**0** 最大长度：**128**
process_parent_name	String	父进程名称 最小长度：**0** 最大长度：**64**
process_parent_path	String	父进程执行文件路径 最小长度：**0** 最大长度：**512**
process_parent_pid	Integer	父进程id 最小值：**0** 最大值：**65535**
process_parent_uid	Integer	父进程用户id 最小值：**0** 最大值：**655350**
process_parent_cmdline	String	父进程命令行 最小长度：**0** 最大长度：**128**
process_child_name	String	子进程名称 最小长度：**0** 最大长度：**64**
process_child_path	String	子进程执行文件路径 最小长度：**0** 最大长度：**512**
process_child_pid	Integer	子进程id 最小值：**0** 最大值：**65535**
process_child_uid	Integer	子进程用户id 最小值：**0** 最大值：**655350**
process_child_cmdline	String	子进程命令行 最小长度：**0** 最大长度：**128**

参数	参数类型	描述
process_launche_time	String	进程启动时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
process_terminate_time	String	进程结束时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

表 4-247 user_info

参数	参数类型	描述
user_id	String	用户uid 最小长度：**0** 最大长度：**36**
user_name	String	用户名称 最小长度：**32** 最大长度：**64**

表 4-248 file_info

参数	参数类型	描述
file_path	String	文件路径/名称 最小长度：**0** 最大长度：**128**
file_content	String	文件内容 最小长度：**0** 最大长度：**1024**
file_new_path	String	文件新路径/名称 最小长度：**32** 最大长度：**64**

参数	参数类型	描述
file_hash	String	文件hash 最小长度：**0** 最大长度：**128**
file_md5	String	文件md5 最小长度：**0** 最大长度：**128**
file_sha256	String	文件sha256 最小长度：**0** 最大长度：**128**
file_attr	String	文件属性 最小长度：**0** 最大长度：**1024**

表 4-249 dataclass_ref

参数	参数类型	描述
id	String	数据类唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
name	String	数据类名称 最小长度：**0** 最大长度：**36**

状态码： 400

表 4-250 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-251 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

更新一条事件，事件标题为MyXXX，URL链接为http://xxx，发生次数为4次，置信度为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 – 未知，True_Positive – 确认，False_Positive – 误报。默认填写Unknown",
   "handle_status" : "Open – 打开，Block – 阻塞，Closed – 关闭。默认填写Open",
   "sla" : 60000,
   "update_time" : "2021-01-30T23:00:00Z+0800",
   "close_time" : "2021-01-30T23:00:00Z+0800",
   "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-
Activity",
   "simulation" : "false",
   "actor" : "刘一博",
   "owner" : "MyXXX",
   "creator" : "MyXXX",
   "close_reason" : "误检;已解决;重复;其他",
   "close_comment" : "误检;已解决;重复;其他",
   "malware" : {
    "malware_family" : "family",
    "malware_class" : "恶意占用内存"
   },
   "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"
  }
}
```

响应示例

状态码： 200

更新事件返回body体

```
{
  "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 – 未知，True_Positive – 确认，False_Positive – 误报。默认填写
Unknown",
     "handle_status" : "Open – 打开，Block – 阻塞，Closed – 关闭。默认填写Open",
     "sla" : 60000,
     "update_time" : "2021-01-30T23:00:00Z+0800",
     "close_time" : "2021-01-30T23:00:00Z+0800",
     "ipdrr_phase" : "Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-
```

```
Activity",
      "simulation" : "false",
      "actor" : "刘一博",
      "owner" : "MyXXX",
      "creator" : "MyXXX",
      "close_reason" : "误检;已解决;重复;其他",
      "close_comment" : "误检;已解决;重复;其他",
      "malware" : {
        "malware_family" : "family",
        "malware_class" : "恶意占用内存"
      },
      "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 代码示例

SDK代码示例如下。

Java

更新一条事件，事件标题为MyXXX，URL链接为http://xxx，发生次数为4次，置信度为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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ChangeIncidentRequest request = new ChangeIncidentRequest();
        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("恶意占用内存");
        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 – 未知,True_Positive – 确
认,False_Positive – 误报。默认填写Unknown"))
            .withHandleStatus(Incident.HandleStatusEnum.fromValue("Open – 打开,Block – 阻塞,Closed – 关
闭。默认填写Open"))
            .withSla(60000)
            .withUpdateTime("2021-01-30T23:00:00Z+0800")
            .withCloseTime("2021-01-30T23:00:00Z+0800")
            .withIpdrrPhase(Incident.IpdrrPhaseEnum.fromValue("Prepartion|Detection and Analysis|
Containm,Eradication& Recovery| Post-Incident-Activity"))
            .withSimulation("false")
            .withActor("刘一博")
            .withOwner("MyXXX")
            .withCreator("MyXXX")
            .withCloseReason(Incident.CloseReasonEnum.fromValue("误检;已解决;重复;其他"))
            .withCloseComment("误检;已解决;重复;其他")
            .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

更新一条事件，事件标题为MyXXX，URL链接为http://xxx，发生次数为4次，置信度为4。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ChangeIncidentRequest()
        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="恶意占用内存"
)
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 – 未知,True_Positive – 确认,False_Positive – 误报。默认填写Unknown",
            handle_status="Open – 打开,Block – 阻塞,Closed – 关闭。默认填写Open",
            sla=60000,
            update_time="2021-01-30T23:00:00Z+0800",
            close_time="2021-01-30T23:00:00Z+0800",
            ipdrr_phase="Prepartion|Detection and Analysis|Containm,Eradication& Recovery| Post-Incident-
Activity",
            simulation="false",
            actor="刘一博",
            owner="MyXXX",
            creator="MyXXX",
            close_reason="误检;已解决;重复;其他",
            close_comment="误检;已解决;重复;其他",
            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

更新一条事件，事件标题为MyXXX，URL链接为http://xxx，发生次数为4次，置信度为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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
```

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

request := &model.ChangeIncidentRequest{}
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:= "恶意占用内存"
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_-_未
知,TRUE_POSITIVE_-_确认,FALSE_POSITIVE_-_误报。默认填写UNKNOWN
    handleStatusDataObject:= model.GetIncidentHandleStatusEnum().OPEN_-_打开,BLOCK_-_阻塞,CLOSED_-
_关闭。默认填写OPEN
    slaDataObject:= int32(60000)
    updateTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    closeTimeDataObject:= "2021-01-30T23:00:00Z+0800"
    ipdrrPhaseDataObject:= model.GetIncidentIpdrrPhaseEnum().PREPARTION|DETECTION_AND_ANALYSIS|
CONTAINM,ERADICATION&_RECOVERY|_POST_INCIDENT_ACTIVITY
    simulationDataObject:= "false"
    actorDataObject:= "刘一博"
    ownerDataObject:= "MyXXX"
    creatorDataObject:= "MyXXX"
    closeReasonDataObject:= model.GetIncidentCloseReasonEnum().误检;已解决;重复;其他
    closeCommentDataObject:= "误检;已解决;重复;其他"
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	更新事件返回body体
400	更新事件错误返回body体

错误码

请参见**错误码**。

4.3 情报指标管理

4.3.1 查询指标列表

功能介绍

查询指标列表

调用方法

请参见**如何调用API**。

URI

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

表 4-252 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**64**
workspace_id	是	String	工作空间ID 最小长度：**1** 最大长度：**1024**

请求参数

表 4-253 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	租户的Token 最小长度：**32** 最大长度：**65535**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

表 4-254 请求 Body 参数

参数	是否必选	参数类型	描述
ids	否	Array of strings	指标ID列表 最小长度：**32** 最大长度：**64** 数组长度：**0 - 999**
name	否	String	指标名称 最小长度：**0** 最大长度：**64**
dataclass_id	否	String	数据类ID 最小长度：**32** 最大长度：**64**
condition	是	**condition** object	搜索条件表达式
offset	是	Integer	request offset, from 0 最小值：**0** 最大值：**999999** 缺省值：**0**
limit	是	Integer	request limit size 最小值：**1** 最大值：**999999**

参数	是否必选	参数类型	描述
sort_by	否	String	sort by property, create_time. 最小长度：**1** 最大长度：**64**
from_date	否	String	查询起始时间，例如：2024-01-20T00:00:00.000Z +0800 最小长度：**0** 最大长度：**64**
to_date	否	String	查询截止时间，例如：2024-01-26T23:59:59.999Z +0800 最小长度：**0** 最大长度：**64**

表 4-255 condition

参数	是否必选	参数类型	描述
conditions	否	Array of **conditions** objects	表达式列表 数组长度：**0 - 999**
logics	否	Array of strings	表达式名称列表 最小长度：**0** 最大长度：**100** 数组长度：**0 - 999**

表 4-256 conditions

参数	是否必选	参数类型	描述
name	否	String	表达式名称 最小长度：**0** 最大长度：**64**
data	否	Array of strings	表达式内容列表 最小长度：**0** 最大长度：**100** 数组长度：**0 - 999**

响应参数

状态码： 200

表 4-257 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为:request_uuid-timestamp-hostname.

表 4-258 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**32** 最大长度：**64**
message	String	错误信息 最小长度：**1** 最大长度：**32**
total	Integer	总数 最小值：**0** 最大值：**99999**
data	Array of **IndicatorDetail** objects	指标列表数据 数组长度：**0 - 100**

表 4-259 IndicatorDetail

参数	参数类型	描述
id	String	指标ID 最小长度：**32** 最大长度：**64**
name	String	指标名称 最小长度：**0** 最大长度：**64**
data_object	**IndicatorDataObjectDetail** object	情报详情

参数	参数类型	描述
workspace_id	String	工作空间ID 最小长度：**32** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
dataclass_ref	**DataClassRefPojo** object	数据类对象信息
create_time	String	创建时间 最小长度：**0** 最大长度：**64**
update_time	String	更新时间 最小长度：**0** 最大长度：**64**

表 4-260 IndicatorDataObjectDetail

参数	参数类型	描述
indicator_type	**indicator_type** object	情报类型对象
value	String	值，如：ip url domain等 最小长度：**0** 最大长度：**256**
update_time	String	更新时间 最小长度：**0** 最大长度：**64**
create_time	String	创建时间 最小长度：**0** 最大长度：**64**
environment	**environment** object	环境信息
data_source	**data_source** object	数据源信息
first_report_time	String	首次发生时间 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
is_deleted	Boolean	是否删除
last_report_time	String	最近发生时间 最小长度：**0** 最大长度：**64**
granular_marking	Integer	粒度（保密等级），由高到低：1（首次发现）、2（自产数据）、3（需购买）、4（外网直接查询） 最小值：**1** 最大值：**4**
name	String	名称 最小长度：**1** 最大长度：**64**
id	String	情报ID 最小长度：**1** 最大长度：**64**
project_id	String	项目ID 最小长度：**1** 最大长度：**64**
revoked	Boolean	是否作废
status	String	状态， Open--打开，Closed--关闭, Revoked--作废 最小长度：**1** 最大长度：**64**
verdict	String	威胁度， Black--黑,White--白，Gray--灰 最小长度：**1** 最大长度：**64**
workspace_id	String	工作空间ID 最小长度：**1** 最大长度：**64**
confidence	Integer	置信度，取值范围是80-100 最小值：**80** 最大值：**100**

表 4-261 indicator_type

参数	参数类型	描述
indicator_type	String	情报类型 最小长度：**1** 最大长度：**32**
id	String	情报类型ID 最小长度：**1** 最大长度：**64**
category	String	目录 最小长度：**1** 最大长度：**64**
layout_id	String	布局ID 最小长度：**1** 最大长度：**64**

表 4-262 environment

参数	参数类型	描述
vendor_type	String	环境供应商（如HWC,AWS,Azure等） 最小长度：**0** 最大长度：**1024**
domain_id	String	租户ID 最小长度：**32** 最大长度：**64**
region_id	String	区域ID 最小长度：**1** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**

表 4-263 data_source

参数	参数类型	描述
source_type	Integer	数据源类型，取值范围如下：1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**0** 最大值：**9999**
domain_id	String	租户ID 最小长度：**32** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
region_id	String	区域ID 最小长度：**1** 最大长度：**64**

表 4-264 DataClassRefPojo

参数	参数类型	描述
id	String	数据类ID 最小长度：**32** 最大长度：**64**
name	String	数据类名称 最小长度：**0** 最大长度：**64**

状态码： 400

表 4-265 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-266 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

查询id为id1、id2，名称为指标名称，类型为DATA_SOURCE，数据类id为28f61af50fc9452aa0ed5ea25c3cc3d3的指标列表，偏移量为0，查询上限10条，根据create_time排序

```
{
  "ids" : [ "id1", "id2" ],
  "name" : "指标名称",
  "dataclass_id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
  "condition" : {
    "conditions" : [ {
      "name" : "title",
      "data" : [ "title", "=", "事件" ]
    } ],
    "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"
}
```

响应示例

状态码： 200

请求成功响应信息

```
{
  "code" : "00000000",
  "data" : [ {
    "create_time" : "2023-07-24T20:54:19Z+0800",
    "data_object" : {
      "indicator_type" : {
        "layout_id" : "20e45c85-8192-3142-bfc8-54b784a80c69",
        "indicator_type" : "ipv6",
        "id" : "ac794b2dfab9fe8c0676587301a636d3",
        "category" : "ipv6"
      },
      "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" : "cn-XXX-7",
      "source_type" : 1
    },
    "environment" : {
      "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
      "project_id" : "15645222e8744afa985c93dab6341da6",
      "region_id" : "cn-xxx-7",
      "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 代码示例

SDK代码示例如下。

Java

查询id为id1、id2，名称为指标名称，类型为DATA_SOURCE，数据类id为28f61af50fc9452aa0ed5ea25c3cc3d3的指标列表，偏移量为0，查询上限10条，根据create_time排序

```
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");

        ICredential auth = new BasicCredentials()
                .withAk(ak)
```

```
            .withSk(sk);

    SecMasterClient client = SecMasterClient.newBuilder()
            .withCredential(auth)
            .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
            .build();
    ListIndicatorsRequest request = new ListIndicatorsRequest();
    IndicatorListSearchRequest body = new IndicatorListSearchRequest();
    List<String> listConditionLogics = new ArrayList<>();
    listConditionLogics.add("title");
    List<String> listConditionsData = new ArrayList<>();
    listConditionsData.add("title");
    listConditionsData.add("=");
    listConditionsData.add("事件");
    List<IndicatorListSearchRequestConditionConditions> listConditionConditions = new ArrayList<>();
    listConditionConditions.add(
        new IndicatorListSearchRequestConditionConditions()
            .withName("title")
            .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.withName("指标名称");
    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

查询id为id1、id2，名称为指标名称，类型为DATA_SOURCE，数据类id为28f61af50fc9452aa0ed5ea25c3cc3d3的指标列表，偏移量为0，查询上限10条，根据create_time排序

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListIndicatorsRequest()
        listLogicsCondition = [
            "title"
        ]
        listDataConditions = [
            "title",
            "=",
            "事件"
        ]
        listConditionsCondition = [
            IndicatorListSearchRequestConditionConditions(
                name="title",
                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",
            name="指标名称",
            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

查询id为id1、id2，名称为指标名称，类型为DATA_SOURCE，数据类id为28f61af50fc9452aa0ed5ea25c3cc3d3的指标列表，偏移量为0，查询上限10条，根据create_time排序

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListIndicatorsRequest{}
    var listLogicsCondition = []string{
        "title",
    }
    var listDataConditions = []string{
        "title",
        "=",
        "事件",
    }
    nameConditions:= "title"
    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"
    nameIndicatorListSearchRequest:= "指标名称"
    request.Body = &model.IndicatorListSearchRequest{
        ToDate: &toDateIndicatorListSearchRequest,
        FromDate: &fromDateIndicatorListSearchRequest,
        SortBy: &sortByIndicatorListSearchRequest,
        Limit: int32(10),
        Offset: int32(0),
        Condition: conditionbody,
        DataclassId: &dataclassIdIndicatorListSearchRequest,
        Name: &nameIndicatorListSearchRequest,
        Ids: &listIdsbody,
    }
    response, err := client.ListIndicators(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
```



```
        fmt.Println(err)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.3.2 创建指标

功能介绍

创建指标

调用方法

请参见**如何调用API**。

URI

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

表 4-267 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**64**
workspace_id	是	String	工作空间ID 最小长度：**1** 最大长度：**1024**

请求参数

表 4-268 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	租户的Token 最小长度：**32** 最大长度：**65535**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

表 4-269 请求 Body 参数

参数	是否必选	参数类型	描述
data_object	是	**CreateIndicatorDetail** object	情报详情信息

表 4-270 CreateIndicatorDetail

参数	是否必选	参数类型	描述
data_source	是	**data_source** object	数据源信息
verdict	是	String	威胁度 最小长度：**1** 最大长度：**64**
confidence	否	Integer	置信度 最小值：**0** 最大值：**99**
status	否	String	状态 最小长度：**1** 最大长度：**64**
labels	否	String	标签 最小长度：**1** 最大长度：**64**

参数	是否必选	参数类型	描述
value	是	String	值 最小长度：**1** 最大长度：**128**
granular_marking	是	String	粒度（保密等级），由高到低：1（首次发现）、2（自产数据）、3（需购买）、4（外网直接查询） 最小长度：**1** 最大长度：**64**
environment	是	**environment** object	环境信息
defanged	是	Boolean	是否失效 缺省值：**false** 枚举值： • **true** • **false**
first_report_time	是	String	首次发生时间 最小长度：**0** 最大长度：**64**
last_report_time	否	String	最近发生时间 最小长度：**0** 最大长度：**64**
id	否	String	指标ID 最小长度：**32** 最大长度：**64**
indicator_type	是	**indicator_type** object	指标类型统计数据
name	是	String	指标名称 最小长度：**0** 最大长度：**64**
dataclass_id	否	String	数据类ID 最小长度：**32** 最大长度：**64**
data_object	否	**IndicatorDataObjectDetail** object	情报详情

参数	是否必选	参数类型	描述
workspace_id	是	String	workspace id 最小长度：**32** 最大长度：**64**
project_id	否	String	Project id value 最小长度：**32** 最大长度：**64**
layout_id	否	String	布局ID 最小长度：**0** 最大长度：**64**
dataclass	否	**DataClassRefPojo** object	数据类对象信息
create_time	否	String	Create time 最小长度：**0** 最大长度：**64**
update_time	否	String	Update time 最小长度：**0** 最大长度：**64**

表 4-271 data_source

参数	是否必选	参数类型	描述
source_type	是	Integer	current page count 最小值：**0** 最大值：**9999**
domain_id	是	String	Id value 最小长度：**32** 最大长度：**64**
project_id	是	String	Id value 最小长度：**32** 最大长度：**64**
region_id	是	String	Id value 最小长度：**1** 最大长度：**64**

参数	是否必选	参数类型	描述
product_name	是	String	Id value 最小长度：**1** 最大长度：**64**
product_feature	是	String	Id value 最小长度：**1** 最大长度：**64**

表 4-272 environment

参数	是否必选	参数类型	描述
vendor_type	是	String	环境供应商，如：HWC/AWS等 最小长度：**0** 最大长度：**1024**
domain_id	是	String	租户ID 最小长度：**32** 最大长度：**64**
region_id	是	String	区域ID 最小长度：**1** 最大长度：**64**
project_id	是	String	项目ID 最小长度：**32** 最大长度：**64**

表 4-273 indicator_type

参数	是否必选	参数类型	描述
indicator_type	是	String	指标类型 最小长度：**1** 最大长度：**32**
id	是	String	情报类型ID 最小长度：**1** 最大长度：**64**
category	是	String	目录 最小长度：**1** 最大长度：**64**

参数	是否必选	参数类型	描述
layout_id	是	String	布局ID 最小长度：**1** 最大长度：**64**

表 4-274 IndicatorDataObjectDetail

参数	是否必选	参数类型	描述
indicator_type	否	**indicator_type** object	情报类型对象
value	否	String	值，如：ip url domain等 最小长度：**0** 最大长度：**256**
update_time	否	String	更新时间 最小长度：**0** 最大长度：**64**
create_time	否	String	创建时间 最小长度：**0** 最大长度：**64**
environment	否	**environment** object	环境信息
data_source	否	**data_source** object	数据源信息
first_report_time	否	String	首次发生时间 最小长度：**0** 最大长度：**64**
is_deleted	否	Boolean	是否删除
last_report_time	否	String	最近发生时间 最小长度：**0** 最大长度：**64**
granular_marking	否	Integer	粒度（保密等级），由高到低：1（首次发现）、2（自产数据）、3（需购买）、4（外网直接查询） 最小值：**1** 最大值：**4**

参数	是否必选	参数类型	描述
name	否	String	名称 最小长度：**1** 最大长度：**64**
id	否	String	情报ID 最小长度：**1** 最大长度：**64**
project_id	否	String	项目ID 最小长度：**1** 最大长度：**64**
revoked	否	Boolean	是否作废
status	否	String	状态， Open--打开，Closed--关闭, Revoked--作废 最小长度：**1** 最大长度：**64**
verdict	否	String	威胁度， Black--黑,White--白，Gray--灰 最小长度：**1** 最大长度：**64**
workspace_id	否	String	工作空间ID 最小长度：**1** 最大长度：**64**
confidence	否	Integer	置信度，取值范围是80-100 最小值：**80** 最大值：**100**

表 4-275 indicator_type

参数	是否必选	参数类型	描述
indicator_type	否	String	情报类型 最小长度：**1** 最大长度：**32**
id	否	String	情报类型ID 最小长度：**1** 最大长度：**64**

参数	是否必选	参数类型	描述
category	否	String	目录 最小长度：**1** 最大长度：**64**
layout_id	否	String	布局ID 最小长度：**1** 最大长度：**64**

表 4-276 environment

参数	是否必选	参数类型	描述
vendor_type	否	String	环境供应商（如HWC,AWS,Azure等） 最小长度：**0** 最大长度：**1024**
domain_id	否	String	租户ID 最小长度：**32** 最大长度：**64**
region_id	否	String	区域ID 最小长度：**1** 最大长度：**64**
project_id	否	String	项目ID 最小长度：**32** 最大长度：**64**

表 4-277 data_source

参数	是否必选	参数类型	描述
source_type	否	Integer	数据源类型，取值范围如下：1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**0** 最大值：**9999**
domain_id	否	String	租户ID 最小长度：**32** 最大长度：**64**

参数	是否必选	参数类型	描述
project_id	否	String	项目ID 最小长度：**32** 最大长度：**64**
region_id	否	String	区域ID 最小长度：**1** 最大长度：**64**

表 4-278 DataClassRefPojo

参数	是否必选	参数类型	描述
id	是	String	数据类ID 最小长度：**32** 最大长度：**64**
name	否	String	数据类名称 最小长度：**0** 最大长度：**64**

响应参数

状态码： 200

表 4-279 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-280 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**32** 最大长度：**64**
message	String	错误信息 最小长度：**1** 最大长度：**32**

参数	参数类型	描述
data	**IndicatorDetail** object	情报详情信息

表 4-281 IndicatorDetail

参数	参数类型	描述
id	String	指标ID 最小长度：**32** 最大长度：**64**
name	String	指标名称 最小长度：**0** 最大长度：**64**
data_object	**IndicatorDataObjectDetail** object	情报详情
workspace_id	String	工作空间ID 最小长度：**32** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
dataclass_ref	**DataClassRefPojo** object	数据类对象信息
create_time	String	创建时间 最小长度：**0** 最大长度：**64**
update_time	String	更新时间 最小长度：**0** 最大长度：**64**

表 4-282 IndicatorDataObjectDetail

参数	参数类型	描述
indicator_type	**indicator_type** object	情报类型对象

参数	参数类型	描述
value	String	值，如：ip url domain等 最小长度：**0** 最大长度：**256**
update_time	String	更新时间 最小长度：**0** 最大长度：**64**
create_time	String	创建时间 最小长度：**0** 最大长度：**64**
environment	**environment** object	环境信息
data_source	**data_source** object	数据源信息
first_report_time	String	首次发生时间 最小长度：**0** 最大长度：**64**
is_deleted	Boolean	是否删除
last_report_time	String	最近发生时间 最小长度：**0** 最大长度：**64**
granular_marking	Integer	粒度（保密等级），由高到低：1（首次发现）、2（自产数据）、3（需购买）、4（外网直接查询） 最小值：**1** 最大值：**4**
name	String	名称 最小长度：**1** 最大长度：**64**
id	String	情报ID 最小长度：**1** 最大长度：**64**
project_id	String	项目ID 最小长度：**1** 最大长度：**64**
revoked	Boolean	是否作废

参数	参数类型	描述
status	String	状态， Open--打开，Closed--关闭, Revoked--作废 最小长度：**1** 最大长度：**64**
verdict	String	威胁度， Black--黑,White--白，Gray--灰 最小长度：**1** 最大长度：**64**
workspace_id	String	工作空间ID 最小长度：**1** 最大长度：**64**
confidence	Integer	置信度，取值范围是80-100 最小值：**80** 最大值：**100**

表 4-283 indicator_type

参数	参数类型	描述
indicator_type	String	情报类型 最小长度：**1** 最大长度：**32**
id	String	情报类型ID 最小长度：**1** 最大长度：**64**
category	String	目录 最小长度：**1** 最大长度：**64**
layout_id	String	布局ID 最小长度：**1** 最大长度：**64**

表 4-284 environment

参数	参数类型	描述
vendor_type	String	环境供应商（如HWC,AWS,Azure等） 最小长度：**0** 最大长度：**1024**
domain_id	String	租户ID 最小长度：**32** 最大长度：**64**
region_id	String	区域ID 最小长度：**1** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**

表 4-285 data_source

参数	参数类型	描述
source_type	Integer	数据源类型，取值范围如下：1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**0** 最大值：**9999**
domain_id	String	租户ID 最小长度：**32** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
region_id	String	区域ID 最小长度：**1** 最大长度：**64**

表 4-286 DataClassRefPojo

参数	参数类型	描述
id	String	数据类ID 最小长度：**32** 最大长度：**64**
name	String	数据类名称 最小长度：**0** 最大长度：**64**

状态码： 400

表 4-287 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-288 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

创建一条指标，指标名称为“指标名称”，指标版本为1，指标类型为DATA_SOURCE，触发标志为否。

```
{
  "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",
    "layout_id" : "909494e3-558e-xxxxxx-07a8e18ca62f",
    "indicator_type" : "ipv6",
    "category" : "ipv6"
  },
  "name" : "指标名称",
  "dataclass_id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
  "workspace_id" : "909494e3-558e-46b6-a9eb-07a8e18ca620",
  "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "layout_id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
  "dataclass" : {
    "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
    "name" : "名称"
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800"
 }
}
```

响应示例

状态码： 200

请求成功响应信息

```
{
 "code" : 0,
 "message" : "Error message",
 "data" : {
  "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
  "name" : "指标名称",
  "data_object" : {
   "indicator_type" : {
    "layout_id" : "4e2d7f64-a66d-3236-a8c1-704636ced9a7",
    "indicator_type" : "ipv6",
    "id" : "ac794b2dfab9fe8c0676587301a636d3",
    "category" : "ipv6"
   },
   "value" : "ip",
   "data_source" : {
    "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
    "project_id" : "5b8bb3c888db498f9eeaf1023f7ba597",
    "region_id" : "cn-xxx-7",
    "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" : "名称"
  },
```

```
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800"
  }
}
```

SDK 代码示例

SDK代码示例如下。

Java

创建一条指标，指标名称为“指标名称”，指标版本为1，指标类型为DATA_SOURCE，触发标志为否。

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateIndicatorRequest request = new CreateIndicatorRequest();
        IndicatorCreateRequest body = new IndicatorCreateRequest();
        DataClassRefPojo dataclassDataObject = new DataClassRefPojo();
        dataclassDataObject.withId("28f61af50fc9452aa0ed5ea25c3cc3d3")
            .withName("名称");
        CreateIndicatorDetailIndicatorType indicatorTypeDataObject = new CreateIndicatorDetailIndicatorType();
        indicatorTypeDataObject.withIndicatorType("ipv6")
            .withId("909494e3-558e-xxxxxx-07a8e18ca6xxx")
            .withCategory("ipv6")
            .withLayoutId("909494e3-558e-xxxxxx-07a8e18ca62f");
        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("指标名称")
            .withDataclassId("28f61af50fc9452aa0ed5ea25c3cc3d3")
            .withWorkspaceId("909494e3-558e-46b6-a9eb-07a8e18ca620")
            .withProjectId("909494e3-558e-46b6-a9eb-07a8e18ca62f")
            .withLayoutId("28f61af50fc9452aa0ed5ea25c3cc3d3")
            .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

创建一条指标，指标名称为“指标名称”，指标版本为1，指标类型为DATA_SOURCE，触发标志为否。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

```
try:
    request = CreateIndicatorRequest()
    dataclassDataObject = DataClassRefPojo(
        id="28f61af50fc9452aa0ed5ea25c3cc3d3",
        name="名称"
    )
    indicatorTypeDataObject = CreateIndicatorDetailIndicatorType(
        indicator_type="ipv6",
        id="909494e3-558e-xxxxxx-07a8e18ca6xxx",
        category="ipv6",
        layout_id="909494e3-558e-xxxxxx-07a8e18ca62f"
    )
    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="指标名称",
        dataclass_id="28f61af50fc9452aa0ed5ea25c3cc3d3",
        workspace_id="909494e3-558e-46b6-a9eb-07a8e18ca620",
        project_id="909494e3-558e-46b6-a9eb-07a8e18ca62f",
        layout_id="28f61af50fc9452aa0ed5ea25c3cc3d3",
        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

创建一条指标，指标名称为“指标名称”，指标版本为1，指标类型为DATA_SOURCE，触发标志为否。

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateIndicatorRequest{}
    nameDataclass:= "名称"
    dataclassDataObject := &model.DataClassRefPojo{
        Id: "28f61af50fc9452aa0ed5ea25c3cc3d3",
        Name: &nameDataclass,
    }
    indicatorTypeDataObject := &model.CreateIndicatorDetailIndicatorType{
        IndicatorType: "ipv6",
        Id: "909494e3-558e-xxxxxx-07a8e18ca6xxx",
        Category: "ipv6",
        LayoutId: "909494e3-558e-xxxxxx-07a8e18ca62f",
    }
    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"
    layoutIdDataObject:= "28f61af50fc9452aa0ed5ea25c3cc3d3"
    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: "指标名称",
        DataclassId: &dataclassIdDataObject,
        WorkspaceId: "909494e3-558e-46b6-a9eb-07a8e18ca620",
        ProjectId: &projectIdDataObject,
        LayoutId: &layoutIdDataObject,
        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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.3.3 删除指标

功能介绍

删除指标

调用方法

请参见**如何调用API**。

URI

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

表 4-289 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**64**
workspace_id	是	String	工作空间ID 最小长度：**1** 最大长度：**1024**

请求参数

表 4-290 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	租户的Token 最小长度：**32** 最大长度：**65535**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

表 4-291 请求 Body 参数

参数	是否必选	参数类型	描述
batch_ids	否	Array of strings	指标ID列表 最小长度：**32** 最大长度：**64** 数组长度：**0 - 999**

响应参数

状态码： 200

表 4-292 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-293 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**32** 最大长度：**64**
message	String	错误信息 最小长度：**1** 最大长度：**32**
data	**IndicatorBatchOperateResponse** object	情报响应参数

表 4-294 IndicatorBatchOperateResponse

参数	参数类型	描述
success_ids	Array of strings	成功ID列表 最小长度：**32** 最大长度：**64** 数组长度：**0 - 999**
error_ids	Array of strings	失败ID列表 最小长度：**32** 最大长度：**64** 数组长度：**0 - 999**

状态码： 400

表 4-295 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-296 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

删除一条指标，指标批次ID为909494e3-558e-46b6-a9eb-07a8e18ca62f。

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

响应示例

状态码： 200

请求成功响应

```
{
  "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 代码示例

SDK代码示例如下。

Java

删除一条指标，指标批次ID为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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteIndicatorRequest request = new DeleteIndicatorRequest();
        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

删除一条指标，指标批次ID为909494e3-558e-46b6-a9eb-07a8e18ca62f。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = DeleteIndicatorRequest()
```

```
        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

删除一条指标，指标批次ID为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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteIndicatorRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应
400	请求失败响应

错误码

请参见**错误码**。

4.3.4 查询指标详情

功能介绍

查询指标详情

调用方法

请参见**如何调用API**。

URI

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

表 4-297 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**64**
workspace_id	是	String	工作空间ID 最小长度：**1** 最大长度：**1024**
indicator_id	是	String	情报指标ID 最小长度：**32** 最大长度：**64**

请求参数

表 4-298 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	租户的Token 最小长度：**32** 最大长度：**65535**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-299 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-300 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**32** 最大长度：**64**
message	String	错误信息 最小长度：**1** 最大长度：**32**
data	**IndicatorDetail** object	情报详情信息

表 4-301 IndicatorDetail

参数	参数类型	描述
id	String	指标ID 最小长度：**32** 最大长度：**64**
name	String	指标名称 最小长度：**0** 最大长度：**64**
data_object	**IndicatorDataObjectDetail** object	情报详情
workspace_id	String	工作空间ID 最小长度：**32** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
dataclass_ref	**DataClassRefPojo** object	数据类对象信息
create_time	String	创建时间 最小长度：**0** 最大长度：**64**
update_time	String	更新时间 最小长度：**0** 最大长度：**64**

表 4-302 IndicatorDataObjectDetail

参数	参数类型	描述
indicator_type	**indicator_type** object	情报类型对象
value	String	值，如：ip url domain等 最小长度：**0** 最大长度：**256**
update_time	String	更新时间 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
create_time	String	创建时间 最小长度：**0** 最大长度：**64**
environment	**environment** object	环境信息
data_source	**data_source** object	数据源信息
first_report_time	String	首次发生时间 最小长度：**0** 最大长度：**64**
is_deleted	Boolean	是否删除
last_report_time	String	最近发生时间 最小长度：**0** 最大长度：**64**
granular_marking	Integer	粒度（保密等级），由高到低：1（首次发现）、2（自产数据）、3（需购买）、4（外网直接查询） 最小值：**1** 最大值：**4**
name	String	名称 最小长度：**1** 最大长度：**64**
id	String	情报ID 最小长度：**1** 最大长度：**64**
project_id	String	项目ID 最小长度：**1** 最大长度：**64**
revoked	Boolean	是否作废
status	String	状态， Open--打开，Closed--关闭, Revoked--作废 最小长度：**1** 最大长度：**64**
verdict	String	威胁度， Black--黑,White--白，Gray--灰 最小长度：**1** 最大长度：**64**

参数	参数类型	描述
workspace_id	String	工作空间ID 最小长度：**1** 最大长度：**64**
confidence	Integer	置信度，取值范围是80-100 最小值：**80** 最大值：**100**

表 4-303 indicator_type

参数	参数类型	描述
indicator_type	String	情报类型 最小长度：**1** 最大长度：**32**
id	String	情报类型ID 最小长度：**1** 最大长度：**64**
category	String	目录 最小长度：**1** 最大长度：**64**
layout_id	String	布局ID 最小长度：**1** 最大长度：**64**

表 4-304 environment

参数	参数类型	描述
vendor_type	String	环境供应商（如HWC,AWS,Azure等） 最小长度：**0** 最大长度：**1024**
domain_id	String	租户ID 最小长度：**32** 最大长度：**64**
region_id	String	区域ID 最小长度：**1** 最大长度：**64**

参数	参数类型	描述
project_id	String	项目ID 最小长度：**32** 最大长度：**64**

表 4-305 data_source

参数	参数类型	描述
source_type	Integer	数据源类型，取值范围如下：1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**0** 最大值：**9999**
domain_id	String	租户ID 最小长度：**32** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
region_id	String	区域ID 最小长度：**1** 最大长度：**64**

表 4-306 DataClassRefPojo

参数	参数类型	描述
id	String	数据类ID 最小长度：**32** 最大长度：**64**
name	String	数据类名称 最小长度：**0** 最大长度：**64**

状态码： 400

表 4-307 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-308 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

请求成功响应信息

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
    "name" : "指标名称",
    "data_object" : {
      "indicator_type" : {
        "layout_id" : "4e2d7f64-a66d-3236-a8c1-704636ced9a7",
        "indicator_type" : "ipv6",
        "id" : "ac794b2dfab9fe8c0676587301a636d3",
        "category" : "ipv6"
      },
      "value" : "ip",
      "data_source" : {
        "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
        "project_id" : "5b8bb3c888db498f9eeaf1023f7ba597",
        "region_id" : "cn-xxx-7",
        "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" : "名称"
  },
  "create_time" : "2021-01-30T23:00:00Z+0800",
  "update_time" : "2021-01-30T23:00:00Z+0800"
 }
}
```

SDK 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowIndicatorDetailRequest request = new ShowIndicatorDetailRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ShowIndicatorDetailRequest()
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

```
  }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.3.5 更新指标

功能介绍

更新指标

调用方法

请参见**如何调用API**。

URI

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

表 4-309 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**64**
workspace_id	是	String	工作空间ID 最小长度：**1** 最大长度：**1024**
indicator_id	是	String	情报ID 最小长度：**32** 最大长度：**64**

请求参数

表 4-310 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	租户的Token 最小长度：**32** 最大长度：**65535**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

表 4-311 请求 Body 参数

参数	是否必选	参数类型	描述
data_object	否	**IndicatorDataObjectDetail** object	情报详情

表 4-312 IndicatorDataObjectDetail

参数	是否必选	参数类型	描述
indicator_type	否	**indicator_type** object	情报类型对象
value	否	String	值，如：ip url domain等 最小长度：**0** 最大长度：**256**
update_time	否	String	更新时间 最小长度：**0** 最大长度：**64**
create_time	否	String	创建时间 最小长度：**0** 最大长度：**64**
environment	否	**environment** object	环境信息

参数	是否必选	参数类型	描述
data_source	否	data_source object	数据源信息
first_report_time	否	String	首次发生时间 最小长度：**0** 最大长度：**64**
is_deleted	否	Boolean	是否删除
last_report_time	否	String	最近发生时间 最小长度：**0** 最大长度：**64**
granular_marking	否	Integer	粒度（保密等级），由高到低：1（首次发现）、2（自产数据）、3（需购买）、4（外网直接查询） 最小值：**1** 最大值：**4**
name	否	String	名称 最小长度：**1** 最大长度：**64**
id	否	String	情报ID 最小长度：**1** 最大长度：**64**
project_id	否	String	项目ID 最小长度：**1** 最大长度：**64**
revoked	否	Boolean	是否作废
status	否	String	状态， Open--打开，Closed--关闭, Revoked--作废 最小长度：**1** 最大长度：**64**
verdict	否	String	威胁度， Black--黑,White--白，Gray--灰 最小长度：**1** 最大长度：**64**
workspace_id	否	String	工作空间ID 最小长度：**1** 最大长度：**64**

参数	是否必选	参数类型	描述
confidence	否	Integer	置信度，取值范围是80-100 最小值：**80** 最大值：**100**

表 4-313 indicator_type

参数	是否必选	参数类型	描述
indicator_type	否	String	情报类型 最小长度：**1** 最大长度：**32**
id	否	String	情报类型ID 最小长度：**1** 最大长度：**64**
category	否	String	目录 最小长度：**1** 最大长度：**64**
layout_id	否	String	布局ID 最小长度：**1** 最大长度：**64**

表 4-314 environment

参数	是否必选	参数类型	描述
vendor_type	否	String	环境供应商（如HWC,AWS,Azure等） 最小长度：**0** 最大长度：**1024**
domain_id	否	String	租户ID 最小长度：**32** 最大长度：**64**
region_id	否	String	区域ID 最小长度：**1** 最大长度：**64**

参数	是否必选	参数类型	描述
project_id	否	String	项目ID 最小长度：**32** 最大长度：**64**

表 4-315 data_source

参数	是否必选	参数类型	描述
source_type	否	Integer	数据源类型，取值范围如下：1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**0** 最大值：**9999**
domain_id	否	String	租户ID 最小长度：**32** 最大长度：**64**
project_id	否	String	项目ID 最小长度：**32** 最大长度：**64**
region_id	否	String	区域ID 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-316 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-317 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**32** 最大长度：**64**
message	String	错误信息 最小长度：**1** 最大长度：**32**
data	**IndicatorDetail** object	情报详情信息

表 4-318 IndicatorDetail

参数	参数类型	描述
id	String	指标ID 最小长度：**32** 最大长度：**64**
name	String	指标名称 最小长度：**0** 最大长度：**64**
data_object	**IndicatorDataObjectDetail** object	情报详情
workspace_id	String	工作空间ID 最小长度：**32** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
dataclass_ref	**DataClassRefPojo** object	数据类对象信息
create_time	String	创建时间 最小长度：**0** 最大长度：**64**
update_time	String	更新时间 最小长度：**0** 最大长度：**64**

表 4-319 IndicatorDataObjectDetail

参数	参数类型	描述
indicator_type	**indicator_type** object	情报类型对象
value	String	值，如：ip url domain等 最小长度：**0** 最大长度：**256**
update_time	String	更新时间 最小长度：**0** 最大长度：**64**
create_time	String	创建时间 最小长度：**0** 最大长度：**64**
environment	**environment** object	环境信息
data_source	**data_source** object	数据源信息
first_report_time	String	首次发生时间 最小长度：**0** 最大长度：**64**
is_deleted	Boolean	是否删除
last_report_time	String	最近发生时间 最小长度：**0** 最大长度：**64**
granular_marking	Integer	粒度（保密等级），由高到低：1（首次发现）、2（自产数据）、3（需购买）、4（外网直接查询） 最小值：**1** 最大值：**4**
name	String	名称 最小长度：**1** 最大长度：**64**
id	String	情报ID 最小长度：**1** 最大长度：**64**

参数	参数类型	描述
project_id	String	项目ID 最小长度：**1** 最大长度：**64**
revoked	Boolean	是否作废
status	String	状态， Open--打开，Closed--关闭, Revoked--作废 最小长度：**1** 最大长度：**64**
verdict	String	威胁度， Black--黑,White--白，Gray--灰 最小长度：**1** 最大长度：**64**
workspace_id	String	工作空间ID 最小长度：**1** 最大长度：**64**
confidence	Integer	置信度，取值范围是80-100 最小值：**80** 最大值：**100**

表 4-320 indicator_type

参数	参数类型	描述
indicator_type	String	情报类型 最小长度：**1** 最大长度：**32**
id	String	情报类型ID 最小长度：**1** 最大长度：**64**
category	String	目录 最小长度：**1** 最大长度：**64**
layout_id	String	布局ID 最小长度：**1** 最大长度：**64**

表 4-321 environment

参数	参数类型	描述
vendor_type	String	环境供应商（如HWC,AWS,Azure等） 最小长度：**0** 最大长度：**1024**
domain_id	String	租户ID 最小长度：**32** 最大长度：**64**
region_id	String	区域ID 最小长度：**1** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**

表 4-322 data_source

参数	参数类型	描述
source_type	Integer	数据源类型，取值范围如下：1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**0** 最大值：**9999**
domain_id	String	租户ID 最小长度：**32** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
region_id	String	区域ID 最小长度：**1** 最大长度：**64**

表 4-323 DataClassRefPojo

参数	参数类型	描述
id	String	数据类ID 最小长度：**32** 最大长度：**64**
name	String	数据类名称 最小长度：**0** 最大长度：**64**

状态码： 400

表 4-324 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-325 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

更新一条指标，指标触发标志为否，值为ip。

```
{
  "data_object" : {
    "indicator_type" : {
      "layout_id" : "4e2d7f64-a66d-3236-a8c1-704636ced9a7",
      "indicator_type" : "ipv6",
      "id" : "ac794b2dfab9fe8c0676587301a636d3",
      "category" : "ipv6"
    },
    "value" : "ip",
    "data_source" : {
      "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
      "project_id" : "5b8bb3c888db498f9eeaf1023f7ba597",
      "region_id" : "cn-xxx-7",
```

```
    "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"
  }
}
```

响应示例

状态码： 200

请求成功响应信息

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "data" : {
    "id" : "28f61af50fc9452aa0ed5ea25c3cc3d3",
    "name" : "指标名称",
    "data_object" : {
      "indicator_type" : {
        "layout_id" : "4e2d7f64-a66d-3236-a8c1-704636ced9a7",
        "indicator_type" : "ipv6",
        "id" : "ac794b2dfab9fe8c0676587301a636d3",
        "category" : "ipv6"
      },
      "value" : "ip",
      "data_source" : {
        "domain_id" : "ac7438b990ef4a37b741004eb45e8bf4",
        "project_id" : "5b8bb3c888db498f9eeaf1023f7ba597",
        "region_id" : "cn-xxx-7",
        "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" : "名称"
    },
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800"
  }
}
```

SDK 代码示例

SDK代码示例如下。

Java

更新一条指标，指标触发标志为否，值为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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateIndicatorRequest request = new UpdateIndicatorRequest();
        UpdateIndicatorRequestBody body = new UpdateIndicatorRequestBody();
        IndicatorDataObjectDetailDataSource dataSourceDataObject = new IndicatorDataObjectDetailDataSource();
        dataSourceDataObject.withSourceType(1)
            .withDomainId("ac7438b990ef4a37b741004eb45e8bf4")
            .withProjectId("5b8bb3c888db498f9eeaf1023f7ba597")
            .withRegionId("cn-xxx-7");
        IndicatorDataObjectDetailIndicatorType indicatorTypeDataObject = new IndicatorDataObjectDetailIndicatorType();
        indicatorTypeDataObject.withIndicatorType("ipv6")
            .withId("ac794b2dfab9fe8c0676587301a636d3")
            .withCategory("ipv6")
            .withLayoutId("4e2d7f64-a66d-3236-a8c1-704636ced9a7");
        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

更新一条指标，指标触发标志为否，值为ip。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = UpdateIndicatorRequest()
        dataSourceDataObject = IndicatorDataObjectDetailDataSource(
            source_type=1,
            domain_id="ac7438b990ef4a37b741004eb45e8bf4",
            project_id="5b8bb3c888db498f9eeaf1023f7ba597",
            region_id="cn-xxx-7"
        )
        indicatorTypeDataObject = IndicatorDataObjectDetailIndicatorType(
            indicator_type="ipv6",
            id="ac794b2dfab9fe8c0676587301a636d3",
            category="ipv6",
            layout_id="4e2d7f64-a66d-3236-a8c1-704636ced9a7"
        )
        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

更新一条指标，指标触发标志为否，值为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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateIndicatorRequest{}
    sourceTypeDataSource:= int32(1)
    domainIdDataSource:= "ac7438b990ef4a37b741004eb45e8bf4"
    projectIdDataSource:= "5b8bb3c888db498f9eeaf1023f7ba597"
    regionIdDataSource:= "cn-xxx-7"
    dataSourceDataObject := &model.IndicatorDataObjectDetailDataSource{
        SourceType: &sourceTypeDataSource,
        DomainId: &domainIdDataSource,
        ProjectId: &projectIdDataSource,
        RegionId: &regionIdDataSource,
    }
    indicatorTypeIndicatorType:= "ipv6"
    idIndicatorType:= "ac794b2dfab9fe8c0676587301a636d3"
    categoryIndicatorType:= "ipv6"
    layoutIdIndicatorType:= "4e2d7f64-a66d-3236-a8c1-704636ced9a7"
    indicatorTypeDataObject := &model.IndicatorDataObjectDetailIndicatorType{
        IndicatorType: &indicatorTypeIndicatorType,
        Id: &idIndicatorType,
        Category: &categoryIndicatorType,
        LayoutId: &layoutIdIndicatorType,
    }
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求错误响应信息

错误码

请参见**错误码**。

4.4 剧本管理

4.4.1 剧本运行监控

功能介绍

剧本运行监控

调用方法

请参见**如何调用API**。

URI

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

表 4-326 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**

参数	是否必选	参数类型	描述
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
playbook_id	是	String	剧本ID 最小长度：**32** 最大长度：**64**

表 4-327 Query 参数

参数	是否必选	参数类型	描述
start_time	是	String	开始时间。格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。例如：2021-01-30T23:00:00Z+0800。时区信息为剧本实例产生的时区，无法解析时区的时间，默认时区填东八区。 最小长度：**18** 最大长度：**64**
version_query_type	是	String	统计剧本版本类型（ALL:全部，VALID:有效的，DELETED:已删除） 最小长度：**1** 最大长度：**20** 枚举值： • **ALL:全部，VALID:有效的，DELETED:已删除**
end_time	是	String	结束时间。格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。例如：2021-01-30T23:00:00Z+0800。时区信息为剧本实例产生的时区，无法解析时区的时间，默认时区填东八区。 最小长度：**18** 最大长度：**64**

请求参数

表 4-328 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-329 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-330 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	错误信息 最小长度：**1** 最大长度：**32**
data	**PlaybookInstanceMonitorDetail** object	剧本运行监控详情

表 4-331 PlaybookInstanceMonitorDetail

参数	参数类型	描述
total_instance_run_num	Integer	运行总次数 最小值：**0** 最大值：**99999999**
schedule_instance_run_num	Integer	定时触发执行次数 最小值：**0** 最大值：**99999999**
event_instance_run_num	Integer	时间触发执行次数 最小值：**0** 最大值：**99999999**
average_run_time	Number	平均运行时间 最小值：**0** 最大值：**9999999999**
min_run_time_instance	**PlaybookInstanceRunStatistics** object	最短运行时间流程实例信息
max_run_time_instance	**PlaybookInstanceRunStatistics** object	最长运行时间流程实例信息
total_instance_num	Integer	剧本实例总数 最小值：**0** 最大值：**99999999**
success_instance_num	Integer	运行成功实例数量 最小值：**0** 最大值：**99999999**
fail_instance_num	Integer	运行失败实例数量 最小值：**0** 最大值：**99999999**
terminate_instance_num	Integer	运行终止实例数量 最小值：**0** 最大值：**99999999**
running_instance_num	Integer	运行中实例数量 最小值：**0** 最大值：**99999999**

表 4-332 PlaybookInstanceRunStatistics

参数	参数类型	描述
playbook_instance_id	String	剧本实例ID 最小长度：**0** 最大长度：**64**
playbook_instance_name	String	剧本实例名称 最小长度：**0** 最大长度：**64**
playbook_instance_run_time	Number	剧本实例运行时间 最小值：**0** 最大值：**9999999999**

状态码： 400

表 4-333 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-334 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

请求成功响应信息

```
{
  "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 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookMonitorsRequest request = new ShowPlaybookMonitorsRequest();
        request.withStartTime("<start_time>");

request.withVersionQueryType(ShowPlaybookMonitorsRequest.VersionQueryTypeEnum.fromValue("<version_query_type>"));
```

```
        request.withEndTime("<end_time>");
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ShowPlaybookMonitorsRequest()
        request.start_time = "<start_time>"
        request.version_query_type = "<version_query_type>"
        request.end_time = "<end_time>"
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowPlaybookMonitorsRequest{}
    request.StartTime = "<start_time>"
    request.VersionQueryType = model.GetShowPlaybookMonitorsRequestVersionQueryTypeEnum().<VERSION_QUERY_TYPE>
    request.EndTime = "<end_time>"
    response, err := client.ShowPlaybookMonitors(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.4.2 剧本数据统计

功能介绍

剧本统计数据

调用方法

请参见**如何调用API**。

URI

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

表 4-335 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**

请求参数

表 4-336 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-337 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-338 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	错误信息 最小长度：**1** 最大长度：**32**
data	**PlaybookStatisticDetail** object	剧本状态统计信息

表 4-339 PlaybookStatisticDetail

参数	参数类型	描述
unapproved_num	Integer	未审核剧本数量 最小值：**0** 最大值：**99999999**
disabled_num	Integer	未启用剧本数量 最小值：**0** 最大值：**99999999**
enabled_num	Integer	已启用剧本数量 最小值：**0** 最大值：**99999999**

状态码： 400

表 4-340 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-341 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

请求成功响应信息

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

SDK 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookStatisticsRequest request = new ShowPlaybookStatisticsRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ShowPlaybookStatisticsRequest()
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.4.3 查询剧本列表

功能介绍

查询剧本列表

调用方法

请参见**如何调用API**。

URI

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

表 4-342 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**

表 4-343 Query 参数

参数	是否必选	参数类型	描述
search_txt	否	String	搜索关键字 最小长度：**32** 最大长度：**36**
enabled	否	Boolean	是否启用
offset	是	Integer	分页查询参数。用于指定查询结果的起始位置，从0开始 最小值：**0** 最大值：**999999** 缺省值：**0**
limit	是	Integer	分页查询参数，用于指定一次查询最多的结果数，从1开始 最小值：**1** 最大值：**999999**
description	否	String	剧本描述 最小长度：**0** 最大长度：**64**
dataclass_name	否	String	数据类名称 最小长度：**0** 最大长度：**64**

参数	是否必选	参数类型	描述
name	否	String	剧本名称 最小长度：**0** 最大长度：**64**

请求参数

表 4-344 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-345 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-346 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**

参数	参数类型	描述
message	String	响应消息信息 最小长度：**1** 最大长度：**32**
total	Integer	总条数 最小值：**0** 最大值：**99999**
size	Integer	分页查询数据大小 最小值：**0** 最大值：**9999**
page	Integer	当前页码 最小值：**0** 最大值：**100**
data	Array of **PlaybookInfo** objects	剧本列表信息 数组长度：**0 - 100000000**

表 4-347 PlaybookInfo

参数	参数类型	描述
id	String	剧本ID 最小长度：**32** 最大长度：**64**
name	String	剧本名称 最小长度：**0** 最大长度：**1024**
description	String	描述信息 最小长度：**0** 最大长度：**1024**
create_time	String	剧本创建时间 最小长度：**0** 最大长度：**64**
update_time	String	剧本更新时间 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
version_id	String	剧本版本ID 最小长度：**32** 最大长度：**64**
enabled	Boolean	是否启用
workspace_id	String	工作空间ID 最小长度：**32** 最大长度：**64**
approve_role	String	审核用户角色 最小长度：**0** 最大长度：**64**
user_role	String	用户角色 最小长度：**0** 最大长度：**64**
edit_role	String	编辑用户角色 最小长度：**0** 最大长度：**64**
owner_id	String	所有者ID 最小长度：**32** 最大长度：**64**
version	String	版本号 最小长度：**32** 最大长度：**64**
dataclass_name	String	数据类名称 最小长度：**0** 最大长度：**64**
dataclass_id	String	数据类ID 最小长度：**1** 最大长度：**64**
unaudited_version_id	String	待审核剧本版本ID 最小长度：**1** 最大长度：**64**

参数	参数类型	描述
reject_version_id	String	已驳回剧本版本ID 最小长度：**1** 最大长度：**64**

状态码： 400

表 4-348 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-349 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

剧本列表查询成功响应参数

```
{
  "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 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybooksRequest request = new ListPlaybooksRequest();
        request.withSearchTxt("<search_txt>");
        request.withEnabled(<enabled>);
        request.withOffset(<offset>);
        request.withLimit(<limit>);
        request.withDescription("<description>");
        request.withDataclassName("<dataclass_name>");
        request.withName("<name>");
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListPlaybooksRequest()
        request.search_txt = "<search_txt>"
        request.enabled = <Enabled>
        request.offset = <offset>
        request.limit = <limit>
        request.description = "<description>"
        request.dataclass_name = "<dataclass_name>"
        request.name = "<name>"
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPlaybooksRequest{}
    searchTxtRequest:= "<search_txt>"
    request.SearchTxt = &searchTxtRequest
    enabledRequest:= <enabled>
    request.Enabled = &enabledRequest
    request.Offset = int32(<offset>)
    request.Limit = int32(<limit>)
    descriptionRequest:= "<description>"
    request.Description = &descriptionRequest
    dataclassNameRequest:= "<dataclass_name>"
    request.DataclassName = &dataclassNameRequest
    nameRequest:= "<name>"
    request.Name = &nameRequest
    response, err := client.ListPlaybooks(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	剧本列表查询成功响应参数
400	查询失败响应参数

错误码

请参见**错误码**。

4.4.4 创建剧本

功能介绍

创建剧本

调用方法

请参见**如何调用API**。

URI

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

表 4-350 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**

请求参数

表 4-351 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

表 4-352 请求 Body 参数

参数	是否必选	参数类型	描述
name	是	String	剧本名称 最小长度：**0** 最大长度：**1024**

参数	是否必选	参数类型	描述
description	否	String	描述 最小长度：**0** 最大长度：**1024**
workspace_id	是	String	工作空间ID 最小长度：**0** 最大长度：**2097152**
enabled	否	Boolean	是否启用，默认传false

响应参数

状态码： 200

表 4-353 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-354 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	错误信息 最小长度：**1** 最大长度：**32**
data	**PlaybookInfo** object	剧本详情信息

表 4-355 PlaybookInfo

参数	参数类型	描述
id	String	剧本ID 最小长度：**32** 最大长度：**64**

参数	参数类型	描述
name	String	剧本名称 最小长度：**0** 最大长度：**1024**
description	String	描述信息 最小长度：**0** 最大长度：**1024**
create_time	String	剧本创建时间 最小长度：**0** 最大长度：**64**
update_time	String	剧本更新时间 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
version_id	String	剧本版本ID 最小长度：**32** 最大长度：**64**
enabled	Boolean	是否启用
workspace_id	String	工作空间ID 最小长度：**32** 最大长度：**64**
approve_role	String	审核用户角色 最小长度：**0** 最大长度：**64**
user_role	String	用户角色 最小长度：**0** 最大长度：**64**
edit_role	String	编辑用户角色 最小长度：**0** 最大长度：**64**
owner_id	String	所有者ID 最小长度：**32** 最大长度：**64**

参数	参数类型	描述
version	String	版本号 最小长度：**32** 最大长度：**64**
dataclass_name	String	数据类名称 最小长度：**0** 最大长度：**64**
dataclass_id	String	数据类ID 最小长度：**1** 最大长度：**64**
unaudited_version_id	String	待审核剧本版本ID 最小长度：**1** 最大长度：**64**
reject_version_id	String	已驳回剧本版本ID 最小长度：**1** 最大长度：**64**

状态码： 400

表 4-356 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-357 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

创建一个剧本，剧本名称为MyXXX，工作空间ID为string，审批人为approve，启用状态为开启。

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

响应示例

状态码： 200

请求成功响应信息

```
{
  "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 代码示例

SDK代码示例如下。

Java

创建一个剧本，剧本名称为MyXXX，工作空间ID为string，审批人为approve，启用状态为开启。

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePlaybookRequest request = new CreatePlaybookRequest();
        CreatePlaybookInfo body = new CreatePlaybookInfo();
        body.withEnabled(true);
        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

创建一个剧本，剧本名称为MyXXX，工作空间ID为string，审批人为approve，启用状态为开启。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

```
    try:
        request = CreatePlaybookRequest()
        request.body = CreatePlaybookInfo(
            enabled=True,
            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

创建一个剧本，剧本名称为MyXXX，工作空间ID为string，审批人为approve，启用状态为开启。

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePlaybookRequest{}
    enabledCreatePlaybookInfo:= true
    descriptionCreatePlaybookInfo:= "This my XXXX"
    request.Body = &model.CreatePlaybookInfo{
        Enabled: &enabledCreatePlaybookInfo,
        WorkspaceId: "string",
        Description: &descriptionCreatePlaybookInfo,
        Name: "MyXXX",
    }
    response, err := client.CreatePlaybook(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.4.5 查询剧本详情

功能介绍

查询剧本详情

调用方法

请参见**如何调用API**。

URI

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

表 4-358 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
playbook_id	是	String	ID of playbook 最小长度：**32** 最大长度：**64**

请求参数

表 4-359 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-360 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-361 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	错误信息 最小长度：**1** 最大长度：**32**
data	**PlaybookInfo** object	剧本详情信息

表 4-362 PlaybookInfo

参数	参数类型	描述
id	String	剧本ID 最小长度：**32** 最大长度：**64**
name	String	剧本名称 最小长度：**0** 最大长度：**1024**
description	String	描述信息 最小长度：**0** 最大长度：**1024**
create_time	String	剧本创建时间 最小长度：**0** 最大长度：**64**
update_time	String	剧本更新时间 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
version_id	String	剧本版本ID 最小长度：**32** 最大长度：**64**
enabled	Boolean	是否启用
workspace_id	String	工作空间ID 最小长度：**32** 最大长度：**64**
approve_role	String	审核用户角色 最小长度：**0** 最大长度：**64**
user_role	String	用户角色 最小长度：**0** 最大长度：**64**
edit_role	String	编辑用户角色 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
owner_id	String	所有者ID 最小长度：**32** 最大长度：**64**
version	String	版本号 最小长度：**32** 最大长度：**64**
dataclass_name	String	数据类名称 最小长度：**0** 最大长度：**64**
dataclass_id	String	数据类ID 最小长度：**1** 最大长度：**64**
unaudited_version_id	String	待审核剧本版本ID 最小长度：**1** 最大长度：**64**
reject_version_id	String	已驳回剧本版本ID 最小长度：**1** 最大长度：**64**

状态码： 400

表 4-363 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-364 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

请求成功响应信息

```
{
  "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 代码示例

SDK代码示例如下。

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");
```

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookRequest request = new ShowPlaybookRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ShowPlaybookRequest()
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.4.6 删除剧本

功能介绍

删除剧本

调用方法

请参见**如何调用API**。

URI

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

表 4-365 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
playbook_id	是	String	ID of playbook 最小长度：**32** 最大长度：**64**

请求参数

表 4-366 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-367 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-368 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	错误信息 最小长度：**1** 最大长度：**32**
data	**PlaybookInfo** object	剧本详情信息

表 4-369 PlaybookInfo

参数	参数类型	描述
id	String	剧本ID 最小长度：**32** 最大长度：**64**
name	String	剧本名称 最小长度：**0** 最大长度：**1024**
description	String	描述信息 最小长度：**0** 最大长度：**1024**
create_time	String	剧本创建时间 最小长度：**0** 最大长度：**64**
update_time	String	剧本更新时间 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
version_id	String	剧本版本ID 最小长度：**32** 最大长度：**64**
enabled	Boolean	是否启用
workspace_id	String	工作空间ID 最小长度：**32** 最大长度：**64**
approve_role	String	审核用户角色 最小长度：**0** 最大长度：**64**
user_role	String	用户角色 最小长度：**0** 最大长度：**64**
edit_role	String	编辑用户角色 最小长度：**0** 最大长度：**64**
owner_id	String	所有者ID 最小长度：**32** 最大长度：**64**
version	String	版本号 最小长度：**32** 最大长度：**64**
dataclass_name	String	数据类名称 最小长度：**0** 最大长度：**64**
dataclass_id	String	数据类ID 最小长度：**1** 最大长度：**64**
unaudited_version_id	String	待审核剧本版本ID 最小长度：**1** 最大长度：**64**

参数	参数类型	描述
reject_version_id	String	已驳回剧本版本ID 最小长度：**1** 最大长度：**64**

状态码： 400

表 4-370 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-371 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

请求成功响应信息

```
{
  "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 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeletePlaybookRequest request = new DeletePlaybookRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = DeletePlaybookRequest()
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeletePlaybookRequest{}
    response, err := client.DeletePlaybook(request)
```

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.4.7 修改剧本

功能介绍

修改剧本

调用方法

请参见**如何调用API**。

URI

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

表 4-372 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**

参数	是否必选	参数类型	描述
playbook_id	是	String	剧本ID 最小长度：**32** 最大长度：**64**

请求参数

表 4-373 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

表 4-374 请求 Body 参数

参数	是否必选	参数类型	描述
name	否	String	剧本名称 最小长度：**0** 最大长度：**1024**
description	否	String	描述 最小长度：**0** 最大长度：**1024**
enabled	否	Boolean	是否启用
active_version_id	否	String	启用的剧本版本ID 最小长度：**32** 最大长度：**64**

响应参数

状态码： 200

表 4-375 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-376 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	错误信息 最小长度：**1** 最大长度：**32**
data	**PlaybookInfo** object	剧本详情信息

表 4-377 PlaybookInfo

参数	参数类型	描述
id	String	剧本ID 最小长度：**32** 最大长度：**64**
name	String	剧本名称 最小长度：**0** 最大长度：**1024**
description	String	描述信息 最小长度：**0** 最大长度：**1024**
create_time	String	剧本创建时间 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
update_time	String	剧本更新时间 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
version_id	String	剧本版本ID 最小长度：**32** 最大长度：**64**
enabled	Boolean	是否启用
workspace_id	String	工作空间ID 最小长度：**32** 最大长度：**64**
approve_role	String	审核用户角色 最小长度：**0** 最大长度：**64**
user_role	String	用户角色 最小长度：**0** 最大长度：**64**
edit_role	String	编辑用户角色 最小长度：**0** 最大长度：**64**
owner_id	String	所有者ID 最小长度：**32** 最大长度：**64**
version	String	版本号 最小长度：**32** 最大长度：**64**
dataclass_name	String	数据类名称 最小长度：**0** 最大长度：**64**
dataclass_id	String	数据类ID 最小长度：**1** 最大长度：**64**

参数	参数类型	描述
unaudited_version_id	String	待审核剧本版本ID 最小长度：**1** 最大长度：**64**
reject_version_id	String	已驳回剧本版本ID 最小长度：**1** 最大长度：**64**

状态码： 400

表 4-378 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-379 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

修改一个剧本，剧本名称为MyXXX，描述信息为This my XXXX，开启状态为已开启，启用剧本ID为active_version_id。

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

响应示例

状态码： 200

请求成功响应信息

```
{
  "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 代码示例

SDK代码示例如下。

Java

修改一个剧本，剧本名称为MyXXX，描述信息为This my XXXX，开启状态为已开启，启用剧本ID为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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdatePlaybookRequest request = new UpdatePlaybookRequest();
        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

修改一个剧本，剧本名称为MyXXX，描述信息为This my XXXX，开启状态为已开启，启用剧本ID为active_version_id。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = UpdatePlaybookRequest()
        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

修改一个剧本，剧本名称为MyXXX，描述信息为This my XXXX，开启状态为已开启，启用剧本ID为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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdatePlaybookRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息

状态码	描述
400	请求失败响应信息

错误码

请参见**错误码**。

4.5 告警规则管理

4.5.1 列出告警规则

功能介绍

List alert rules

调用方法

请参见**如何调用API**。

URI

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

表 4-380 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目 ID。Project ID. 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间 ID。Workspace ID. 最小长度：**32** 最大长度：**36**

表 4-381 Query 参数

参数	是否必选	参数类型	描述
offset	是	Long	偏移量。Offset. 最小值：**0** 最大值：**9223372036854775807**

参数	是否必选	参数类型	描述
limit	是	Long	条数。Limit. 最小值：**10** 最大值：**50**
sort_key	否	String	排序字段。Sort key 最小长度：**1** 最大长度：**256**
sort_dir	否	String	排序顺序，顺序、逆序。Sort direction, asc, desc。 枚举值： • **asc** • **desc**
pipe_id	否	String	数据管道 ID。Pipe ID. 最小长度：**36** 最大长度：**36**
rule_name	否	String	告警规则名称。Alert rule name. 最小长度：**1** 最大长度：**256**
rule_id	否	String	告警规则 ID。Alert rule ID. 最小长度：**36** 最大长度：**36**
status	否	Array	启用状态，启用、停用。Status, enabled, disabled. 最小长度：**1** 最大长度：**256** 数组长度：**1 - 2** 枚举值： • **ENABLED** • **DISABLED**

参数	是否必选	参数类型	描述
severity	否	Array	严重程度，提示、低危、中危、高危、致命。Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 数组长度：**1 - 5** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**

请求参数

表 4-382 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取。 IAM user token, fetch from IAM api. 最小长度：**1** 最大长度：**2097152**

响应参数

状态码： 200

表 4-383 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

表 4-384 响应 Body 参数

参数	参数类型	描述
count	Long	总数量。Total count. 最小值：**0** 最大值：**9223372036854775807**
records	Array of **AlertRule** objects	告警模型。Alert rules. 数组长度：**0 - 100**

表 4-385 AlertRule

参数	参数类型	描述
rule_id	String	告警规则 ID。Alert rule ID. 最小长度：**36** 最大长度：**36**
pipe_id	String	数据管道 ID。Pipe ID. 最小长度：**36** 最大长度：**36**
pipe_name	String	数据管道名称。Pipe name. 最小长度：**5** 最大长度：**63**
create_by	String	创建人。Create by. 最小长度：**1** 最大长度：**255**
create_time	Long	创建时间。Create time. 最小值：**0** 最大值：**9223372036854775807**
update_by	String	更新人。Update by. 最小长度：**1** 最大长度：**255**
update_time	Long	更新时间。Update time. 最小值：**0** 最大值：**9223372036854775807**
delete_time	Long	删除时间。Delete time. 最小值：**0** 最大值：**9223372036854775807**

参数	参数类型	描述
rule_name	String	告警规则名称。Alert rule name. 最小长度：**1** 最大长度：**255**
query	String	查询语句。Query. 最小长度：**1** 最大长度：**1024**
query_type	String	查询语法，SQL。Query type. SQL. 缺省值：**SQL** 最小长度：**1** 最大长度：**255** 枚举值： • **SQL**
status	String	启用状态，启用、停用。Status, enabled, disabled. 缺省值：**ENABLED** 最小长度：**1** 最大长度：**255** 枚举值： • **ENABLED** • **DISABLED**
severity	String	严重程度，提示、低危、中危、高危、致命。Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 缺省值：**TIPS** 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**
custom_properties	Map<String,String>	自定义扩展信息。Custom properties.
event_grouping	Boolean	告警分组。Event grouping. 缺省值：**true**
schedule	**Schedule** object	

参数	参数类型	描述
triggers	Array of **AlertRuleTrigger** objects	告警触发规则。Alert triggers. 数组长度：**1 - 5**

表 4-386 Schedule

参数	参数类型	描述
frequency_interval	Integer	调度间隔。Frequency interval. 最小值：**1** 最大值：**60**
frequency_unit	String	调度间隔单位，分钟、小时、天。Frequency unit. MINUTE, HOUR, DAY. 最小长度：**1** 最大长度：**255** 枚举值： • **MINUTE** • **HOUR** • **DAY**
period_interval	Integer	时间窗口间隔。Period interval. 最小值：**1** 最大值：**60**
period_unit	String	时间窗口单位，分钟、小时、天。Period unit. MINUTE, HOUR, DAY. 最小长度：**1** 最大长度：**255** 枚举值： • **MINUTE** • **HOUR** • **DAY**
delay_interval	Integer	延迟间隔。Delay interval 最小值：**0** 最大值：**10** 缺省值：**0**
overtime_interval	Integer	超时间隔。Overtime interval 最小值：**0** 最大值：**10** 缺省值：**10**

表 4-387 AlertRuleTrigger

参数	参数类型	描述
mode	String	模式，数量。Mode. COUNT. 缺省值：**COUNT** 最小长度：**1** 最大长度：**255** 枚举值： • **COUNT**
operator	String	操作符，等于、不等于、大于、小于。 operator. EQ equal, NE not equal, GT greater than, LT less than. 缺省值：**GT** 最小长度：**1** 最大长度：**255** 枚举值： • **EQ** • **NE** • **GT** • **LT**
expression	String	expression 最小长度：**1** 最大长度：**255**
severity	String	严重程度，提示、低危、中危、高危、致命。 Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**
accumulated_times	Integer	accumulated_times 最小值：**1** 最大值：**1000** 缺省值：**1**

状态码： 400

表 4-388 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

请求示例

无

响应示例

状态码： 200

Success

```
{
  "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 代码示例

SDK代码示例如下。

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 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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListAlertRulesRequest request = new ListAlertRulesRequest();
        request.withOffset(<offset>L);
        request.withLimit(<limit>L);
        request.withSortKey("<sort_key>");
        request.withSortDir(ListAlertRulesRequest.SortDirEnum.fromValue("<sort_dir>"));
        request.withPipeId("<pipe_id>");
        request.withRuleName("<rule_name>");
        request.withRuleId("<rule_id>");
        request.withStatus();
        request.withSeverity();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListAlertRulesRequest()
        request.offset = <offset>
        request.limit = <limit>
        request.sort_key = "<sort_key>"
        request.sort_dir = "<sort_dir>"
        request.pipe_id = "<pipe_id>"
        request.rule_name = "<rule_name>"
        request.rule_id = "<rule_id>"
        request.status =
        request.severity =
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAlertRulesRequest{}
    request.Offset = int64(<offset>)
    request.Limit = int64(<limit>)
    sortKeyRequest:= "<sort_key>"
```

```
    request.SortKey = &sortKeyRequest
    sortDirRequest:= model.GetListAlertRulesRequestSortDirEnum().<SORT_DIR>
    request.SortDir = &sortDirRequest
    pipeIdRequest:= "<pipe_id>"
    request.PipeId = &pipeIdRequest
    ruleNameRequest:= "<rule_name>"
    request.RuleName = &ruleNameRequest
    ruleIdRequest:= "<rule_id>"
    request.RuleId = &ruleIdRequest
    response, err := client.ListAlertRules(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	Success
400	Bad Request

错误码

请参见**错误码**。

4.5.2 创建告警规则

功能介绍

Create alert rule

调用方法

请参见**如何调用API**。

URI

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

表 4-389 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目 ID。Project ID. 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间 ID。Workspace ID. 最小长度：**32** 最大长度：**36**

请求参数

表 4-390 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取。 IAM user token, fetch from IAM api. 最小长度：**1** 最大长度：**2097152**

表 4-391 请求 Body 参数

参数	是否必选	参数类型	描述
pipe_id	是	String	数据管道 ID。Pipe ID. 最小长度：**36** 最大长度：**36**
rule_name	是	String	告警规则名称。Alert rule name. 最小长度：**1** 最大长度：**255**
description	否	String	描述。Description. 最小长度：**0** 最大长度：**1024**
query	是	String	查询语句。Query. 最小长度：**1** 最大长度：**1024**

参数	是否必选	参数类型	描述
query_type	否	String	查询语法，SQL。Query type. SQL. 缺省值：**SQL** 最小长度：**1** 最大长度：**255** 枚举值： • **SQL**
status	否	String	启用状态，启用、停用。Status, enabled, disabled. 缺省值：**ENABLED** 最小长度：**1** 最大长度：**255** 枚举值： • **ENABLED** • **DISABLED**
severity	否	String	严重程度，提示、低危、中危、高危、致命。Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 缺省值：**TIPS** 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**
custom_properties	否	Map<String,String>	自定义扩展信息。Custom properties.
alert_type	否	Map<String,String>	告警类型。Alert type.
event_grouping	否	Boolean	告警分组。Event grouping. 缺省值：**true**
suspression	否	Boolean	告警抑制。Suspression. 缺省值：**true**
simulation	否	Boolean	模拟告警。Simulation. 缺省值：**true**

参数	是否必选	参数类型	描述
schedule	是	**Schedule** object	
triggers	是	Array of **AlertRuleTrigger** objects	告警触发规则。Alert triggers. 数组长度：**1 - 5**

表 4-392 Schedule

参数	是否必选	参数类型	描述
frequency_interval	是	Integer	调度间隔。Frequency interval. 最小值：**1** 最大值：**60**
frequency_unit	是	String	调度间隔单位，分钟、小时、天。Frequency unit. MINUTE, HOUR, DAY. 最小长度：**1** 最大长度：**255** 枚举值： • **MINUTE** • **HOUR** • **DAY**
period_interval	是	Integer	时间窗口间隔。Period interval. 最小值：**1** 最大值：**60**
period_unit	是	String	时间窗口单位，分钟、小时、天。Period unit. MINUTE, HOUR, DAY. 最小长度：**1** 最大长度：**255** 枚举值： • **MINUTE** • **HOUR** • **DAY**
delay_interval	否	Integer	延迟间隔。Delay interval 最小值：**0** 最大值：**10** 缺省值：**0**

参数	是否必选	参数类型	描述
overtime_interval	否	Integer	超时间隔。Overtime interval 最小值：**0** 最大值：**10** 缺省值：**10**

表 4-393 AlertRuleTrigger

参数	是否必选	参数类型	描述
mode	否	String	模式，数量。Mode. COUNT. 缺省值：**COUNT** 最小长度：**1** 最大长度：**255** 枚举值： • **COUNT**
operator	否	String	操作符，等于、不等于、大于、小于。 operator. EQ equal, NE not equal, GT greater than, LT less than. 缺省值：**GT** 最小长度：**1** 最大长度：**255** 枚举值： • **EQ** • **NE** • **GT** • **LT**
expression	是	String	expression 最小长度：**1** 最大长度：**255**

参数	是否必选	参数类型	描述
severity	否	String	严重程度，提示、低危、中危、高危、致命。Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**
accumulated_times	否	Integer	accumulated_times 最小值：**1** 最大值：**1000** 缺省值：**1**

响应参数

状态码： 200

表 4-394 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

表 4-395 响应 Body 参数

参数	参数类型	描述
rule_id	String	告警规则 ID。Alert rule ID. 最小长度：**36** 最大长度：**36**
pipe_id	String	数据管道 ID。Pipe ID. 最小长度：**36** 最大长度：**36**

参数	参数类型	描述
pipe_name	String	数据管道名称。Pipe name. 最小长度：**5** 最大长度：**63**
create_by	String	创建人。Create by. 最小长度：**1** 最大长度：**255**
create_time	Long	创建时间。Create time. 最小值：**0** 最大值：**9223372036854775807**
update_by	String	更新人。Update by. 最小长度：**1** 最大长度：**255**
update_time	Long	更新时间。Update time. 最小值：**0** 最大值：**9223372036854775807**
delete_time	Long	删除时间。Delete time. 最小值：**0** 最大值：**9223372036854775807**
rule_name	String	告警规则名称。Alert rule name. 最小长度：**1** 最大长度：**255**
query	String	查询语句。Query. 最小长度：**1** 最大长度：**1024**
query_type	String	查询语法，SQL。Query type. SQL. 缺省值：**SQL** 最小长度：**1** 最大长度：**255** 枚举值： • **SQL**

参数	参数类型	描述
status	String	启用状态，启用、停用。Status, enabled, disabled. 缺省值：**ENABLED** 最小长度：**1** 最大长度：**255** 枚举值： • **ENABLED** • **DISABLED**
severity	String	严重程度，提示、低危、中危、高危、致命。Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 缺省值：**TIPS** 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**
custom_properties	Map<String,String>	自定义扩展信息。Custom properties.
event_grouping	Boolean	告警分组。Event grouping. 缺省值：**true**
schedule	**Schedule** object	
triggers	Array of **AlertRuleTrigger** objects	告警触发规则。Alert triggers. 数组长度：**1 - 5**

表 4-396 Schedule

参数	参数类型	描述
frequency_interval	Integer	调度间隔。Frequency interval. 最小值：**1** 最大值：**60**

参数	参数类型	描述
frequency_unit	String	调度间隔单位，分钟、小时、天。Frequency unit. MINUTE, HOUR, DAY. 最小长度：**1** 最大长度：**255** 枚举值： • **MINUTE** • **HOUR** • **DAY**
period_interval	Integer	时间窗口间隔。Period interval. 最小值：**1** 最大值：**60**
period_unit	String	时间窗口单位，分钟、小时、天。Period unit. MINUTE, HOUR, DAY. 最小长度：**1** 最大长度：**255** 枚举值： • **MINUTE** • **HOUR** • **DAY**
delay_interval	Integer	延迟间隔。Delay interval 最小值：**0** 最大值：**10** 缺省值：**0**
overtime_interval	Integer	超时间隔。Overtime interval 最小值：**0** 最大值：**10** 缺省值：**10**

表 4-397 AlertRuleTrigger

参数	参数类型	描述
mode	String	模式，数量。Mode. COUNT. 缺省值：**COUNT** 最小长度：**1** 最大长度：**255** 枚举值： • **COUNT**

参数	参数类型	描述
operator	String	操作符，等于、不等于、大于、小于。 operator. EQ equal, NE not equal, GT greater than, LT less than. 缺省值：**GT** 最小长度：**1** 最大长度：**255** 枚举值： • **EQ** • **NE** • **GT** • **LT**
expression	String	expression 最小长度：**1** 最大长度：**255**
severity	String	严重程度，提示、低危、中危、高危、致命。 Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**
accumulated_times	Integer	accumulated_times 最小值：**1** 最大值：**1000** 缺省值：**1**

状态码： 400

表 4-398 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

请求示例

创建一条告警规则，告警规则所属的管道ID为772fb35b-83bc-46c9-a0b1-ebe31070a889，告警规则名称为Alert rule，查询类型为SQL，状态为启用。

```
{
  "pipe_id" : "772fb35b-83bc-46c9-a0b1-ebe31070a889",
  "rule_name" : "Alert rule",
  "description" : "An 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,
  "suspression" : 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"
  } ]
}
```

响应示例

状态码： 200

Success

```
{
  "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 代码示例

SDK代码示例如下。

Java

创建一条告警规则，告警规则所属的管道ID为772fb35b-83bc-46c9-a0b1-ebe31070a889，告警规则名称为Alert rule，查询类型为SQL，状态为启用。

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateAlertRuleRequest request = new CreateAlertRuleRequest();
        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"))
        );
        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.withSuspression(true);
        body.withEventGrouping(true);
        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

创建一条告警规则，告警规则所属的管道ID为772fb35b-83bc-46c9-a0b1-ebe31070a889，告警规则名称为Alert rule，查询类型为SQL，状态为启用。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = CreateAlertRuleRequest()
        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 = CreateAlertRuleRequestBody(
        triggers=listTriggersbody,
        schedule=schedulebody,
        suspression=True,
        event_grouping=True,
        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

创建一条告警规则，告警规则所属的管道ID为772fb35b-83bc-46c9-a0b1-ebe31070a889，告警规则名称为Alert rule，查询类型为SQL，状态为启用。

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
```

```
        WithCredential(auth).
        Build())

    request := &model.CreateAlertRuleRequest{}
    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",
    }
    suspressionCreateAlertRuleRequestBody:= true
    eventGroupingCreateAlertRuleRequestBody:= true
    severityCreateAlertRuleRequestBody:= model.GetCreateAlertRuleRequestBodySeverityEnum().TIPS
    statusCreateAlertRuleRequestBody:= model.GetCreateAlertRuleRequestBodyStatusEnum().ENABLED
    queryTypeCreateAlertRuleRequestBody:= model.GetCreateAlertRuleRequestBodyQueryTypeEnum().SQL
    descriptionCreateAlertRuleRequestBody:= "An alert rule"
    request.Body = &model.CreateAlertRuleRequestBody{
        Triggers: listTriggersbody,
        Schedule: schedulebody,
        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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	Success
400	Bad Request

错误码

请参见**错误码**。

4.5.3 删除告警规则

功能介绍

Delete alert rule

调用方法

请参见**如何调用API**。

URI

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

表 4-399 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目 ID。Project ID. 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间 ID。Workspace ID. 最小长度：**32** 最大长度：**36**

请求参数

表 4-400 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取。 IAM user token, fetch from IAM api. 最小长度：**1** 最大长度：**2097152**

表 4-401 请求 Body 参数

参数	是否必选	参数类型	描述
[数组元素]	是	Array of strings	告警规则ID数组

响应参数

状态码： 200

表 4-402 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

表 4-403 响应 Body 参数

参数	参数类型	描述
rule_id	String	告警规则 ID。Alert rule ID. 最小长度：**36** 最大长度：**36**
delete_time	Long	删除时间。Delete time. 最小值：**0** 最大值：**9223372036854775807**

状态码： 400

表 4-404 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

请求示例

删除告警规则，告警规则请求体为告警规则ID数组。

```
[ "612b7f41-da89-495b-a6a1-fdf14e4cc794" ]
```

响应示例

状态码： 200

Success

```
{
  "rule_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
  "delete_time" : 1665221214
}
```

SDK 代码示例

SDK代码示例如下。

Java

删除告警规则，告警规则请求体为告警规则ID数组。

```
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");

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

```
        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteAlertRuleRequest request = new DeleteAlertRuleRequest();
        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

删除告警规则，告警规则请求体为告警规则ID数组。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = DeleteAlertRuleRequest()
        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

删除告警规则，告警规则请求体为告警规则ID数组。

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteAlertRuleRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	Success
400	Bad Request

错误码

请参见**错误码**。

4.5.4 查看告警规则

功能介绍

查看告警规则 Get alert rule

调用方法

请参见**如何调用API**。

URI

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

表 4-405 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目 ID。Project ID. 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间 ID。Workspace ID. 最小长度：**32** 最大长度：**36**
rule_id	是	String	告警规则 ID。Alert rule ID. 最小长度：**36** 最大长度：**36**

请求参数

表 4-406 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取。 IAM user token, fetch from IAM api. 最小长度：**1** 最大长度：**2097152**

响应参数

状态码： 200

表 4-407 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

表 4-408 响应 Body 参数

参数	参数类型	描述
rule_id	String	告警规则 ID。Alert rule ID. 最小长度：**36** 最大长度：**36**
pipe_id	String	数据管道 ID。Pipe ID. 最小长度：**36** 最大长度：**36**
pipe_name	String	数据管道名称。Pipe name. 最小长度：**5** 最大长度：**63**
create_by	String	创建人。Create by. 最小长度：**1** 最大长度：**255**
create_time	Long	创建时间。Create time. 最小值：**0** 最大值：**9223372036854775807**
update_by	String	更新人。Update by. 最小长度：**1** 最大长度：**255**
update_time	Long	更新时间。Update time. 最小值：**0** 最大值：**9223372036854775807**
delete_time	Long	删除时间。Delete time. 最小值：**0** 最大值：**9223372036854775807**
rule_name	String	告警规则名称。Alert rule name. 最小长度：**1** 最大长度：**255**

参数	参数类型	描述
query	String	查询语句。Query. 最小长度：**1** 最大长度：**1024**
query_type	String	查询语法，SQL。Query type. SQL. 缺省值：**SQL** 最小长度：**1** 最大长度：**255** 枚举值： • **SQL**
status	String	启用状态，启用、停用。Status, enabled, disabled. 缺省值：**ENABLED** 最小长度：**1** 最大长度：**255** 枚举值： • **ENABLED** • **DISABLED**
severity	String	严重程度，提示、低危、中危、高危、致命。Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 缺省值：**TIPS** 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**
custom_properties	Map<String,String>	自定义扩展信息。Custom properties.
event_grouping	Boolean	告警分组。Event grouping. 缺省值：**true**
schedule	**Schedule** object	
triggers	Array of **AlertRuleTrigger** objects	告警触发规则。Alert triggers. 数组长度：**1 - 5**

表 4-409 Schedule

参数	参数类型	描述
frequency_interval	Integer	调度间隔。Frequency interval. 最小值：**1** 最大值：**60**
frequency_unit	String	调度间隔单位，分钟、小时、天。Frequency unit. MINUTE, HOUR, DAY. 最小长度：**1** 最大长度：**255** 枚举值： • **MINUTE** • **HOUR** • **DAY**
period_interval	Integer	时间窗口间隔。Period interval. 最小值：**1** 最大值：**60**
period_unit	String	时间窗口单位，分钟、小时、天。Period unit. MINUTE, HOUR, DAY. 最小长度：**1** 最大长度：**255** 枚举值： • **MINUTE** • **HOUR** • **DAY**
delay_interval	Integer	延迟间隔。Delay interval 最小值：**0** 最大值：**10** 缺省值：**0**
overtime_interval	Integer	超时间隔。Overtime interval 最小值：**0** 最大值：**10** 缺省值：**10**

表 4-410 AlertRuleTrigger

参数	参数类型	描述
mode	String	模式，数量。Mode. COUNT. 缺省值：**COUNT** 最小长度：**1** 最大长度：**255** 枚举值： • **COUNT**
operator	String	操作符，等于、不等于、大于、小于。 operator. EQ equal, NE not equal, GT greater than, LT less than. 缺省值：**GT** 最小长度：**1** 最大长度：**255** 枚举值： • **EQ** • **NE** • **GT** • **LT**
expression	String	expression 最小长度：**1** 最大长度：**255**
severity	String	严重程度，提示、低危、中危、高危、致命。 Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**
accumulated_times	Integer	accumulated_times 最小值：**1** 最大值：**1000** 缺省值：**1**

状态码： 400

表 4-411 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

请求示例

无

响应示例

状态码： 200

Success

```
{
  "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 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowAlertRuleRequest request = new ShowAlertRuleRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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



```
    try:
        request = ShowAlertRuleRequest()
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	Success
400	Bad Request

错误码

请参见**错误码**。

4.5.5 更新告警规则

功能介绍

Update alert rule

调用方法

请参见**如何调用API**。

URI

PUT /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/{rule_id}

表 4-412 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目 ID。Project ID. 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间 ID。Workspace ID. 最小长度：**32** 最大长度：**36**
rule_id	是	String	告警规则 ID。Alert rule ID. 最小长度：**36** 最大长度：**36**

请求参数

表 4-413 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取。 IAM user token, fetch from IAM api. 最小长度：**1** 最大长度：**2097152**

表 4-414 请求 Body 参数

参数	是否必选	参数类型	描述
rule_name	否	String	告警规则名称。Alert rule name. 最小长度：**1** 最大长度：**255**
description	否	String	描述。Description. 最小长度：**0** 最大长度：**1024**
query	否	String	查询语句。Query. 最小长度：**1** 最大长度：**1024**
query_type	否	String	查询语法，SQL。Query type. SQL. 缺省值：**SQL** 最小长度：**1** 最大长度：**255** 枚举值： • **SQL**
status	否	String	启用状态，启用、停用。Status, enabled, disabled. 缺省值：**ENABLED** 最小长度：**1** 最大长度：**255** 枚举值： • **ENABLED** • **DISABLED**
severity	否	String	严重程度，提示、低危、中危、高危、致命。Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 缺省值：**TIPS** 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**

参数	是否必选	参数类型	描述
custom_properties	否	Map<String,String>	自定义扩展信息。Custom properties.
alert_type	否	Map<String,String>	告警类型。Alert type.
event_grouping	否	Boolean	告警分组。Event grouping. 缺省值：**true**
suppression	否	Boolean	告警抑制。Suppression 缺省值：**true**
simulation	否	Boolean	模拟告警。Simulation. 缺省值：**true**
schedule	否	**Schedule** object	
triggers	否	Array of **AlertRuleTrigger** objects	告警触发规则。Alert triggers. 数组长度：**1 - 5**

表 4-415 Schedule

参数	是否必选	参数类型	描述
frequency_interval	是	Integer	调度间隔。Frequency interval. 最小值：**1** 最大值：**60**
frequency_unit	是	String	调度间隔单位，分钟、小时、天。Frequency unit. MINUTE, HOUR, DAY. 最小长度：**1** 最大长度：**255** 枚举值： • **MINUTE** • **HOUR** • **DAY**
period_interval	是	Integer	时间窗口间隔。Period interval. 最小值：**1** 最大值：**60**

参数	是否必选	参数类型	描述
period_unit	是	String	时间窗口单位，分钟、小时、天。Period unit. MINUTE, HOUR, DAY. 最小长度：**1** 最大长度：**255** 枚举值： • **MINUTE** • **HOUR** • **DAY**
delay_interval	否	Integer	延迟间隔。Delay interval 最小值：**0** 最大值：**10** 缺省值：**0**
overtime_interval	否	Integer	超时间隔。Overtime interval 最小值：**0** 最大值：**10** 缺省值：**10**

表 4-416 AlertRuleTrigger

参数	是否必选	参数类型	描述
mode	否	String	模式，数量。Mode. COUNT. 缺省值：**COUNT** 最小长度：**1** 最大长度：**255** 枚举值： • **COUNT**

参数	是否必选	参数类型	描述
operator	否	String	操作符，等于、不等于、大于、小于。 operator. EQ equal, NE not equal, GT greater than, LT less than. 缺省值：**GT** 最小长度：**1** 最大长度：**255** 枚举值： • **EQ** • **NE** • **GT** • **LT**
expression	是	String	expression 最小长度：**1** 最大长度：**255**
severity	否	String	严重程度，提示、低危、中危、高危、致命。Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**
accumulated_times	否	Integer	accumulated_times 最小值：**1** 最大值：**1000** 缺省值：**1**

响应参数

状态码： 200

表 4-417 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

表 4-418 响应 Body 参数

参数	参数类型	描述
rule_id	String	告警规则 ID。Alert rule ID. 最小长度：**36** 最大长度：**36**
pipe_id	String	数据管道 ID。Pipe ID. 最小长度：**36** 最大长度：**36**
pipe_name	String	数据管道名称。Pipe name. 最小长度：**5** 最大长度：**63**
create_by	String	创建人。Create by. 最小长度：**1** 最大长度：**255**
create_time	Long	创建时间。Create time. 最小值：**0** 最大值：**9223372036854775807**
update_by	String	更新人。Update by. 最小长度：**1** 最大长度：**255**
update_time	Long	更新时间。Update time. 最小值：**0** 最大值：**9223372036854775807**
delete_time	Long	删除时间。Delete time. 最小值：**0** 最大值：**9223372036854775807**
rule_name	String	告警规则名称。Alert rule name. 最小长度：**1** 最大长度：**255**

参数	参数类型	描述
query	String	查询语句。Query. 最小长度：**1** 最大长度：**1024**
query_type	String	查询语法，SQL。Query type. SQL. 缺省值：**SQL** 最小长度：**1** 最大长度：**255** 枚举值： • **SQL**
status	String	启用状态，启用、停用。Status, enabled, disabled. 缺省值：**ENABLED** 最小长度：**1** 最大长度：**255** 枚举值： • **ENABLED** • **DISABLED**
severity	String	严重程度，提示、低危、中危、高危、致命。Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 缺省值：**TIPS** 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**
custom_properties	Map<String,String>	自定义扩展信息。Custom properties.
event_grouping	Boolean	告警分组。Event grouping. 缺省值：**true**
schedule	**Schedule** object	
triggers	Array of **AlertRuleTrigger** objects	告警触发规则。Alert triggers. 数组长度：**1 - 5**

表 4-419 Schedule

参数	参数类型	描述
frequency_interval	Integer	调度间隔。Frequency interval. 最小值：**1** 最大值：**60**
frequency_unit	String	调度间隔单位，分钟、小时、天。Frequency unit. MINUTE, HOUR, DAY. 最小长度：**1** 最大长度：**255** 枚举值： • **MINUTE** • **HOUR** • **DAY**
period_interval	Integer	时间窗口间隔。Period interval. 最小值：**1** 最大值：**60**
period_unit	String	时间窗口单位，分钟、小时、天。Period unit. MINUTE, HOUR, DAY. 最小长度：**1** 最大长度：**255** 枚举值： • **MINUTE** • **HOUR** • **DAY**
delay_interval	Integer	延迟间隔。Delay interval 最小值：**0** 最大值：**10** 缺省值：**0**
overtime_interval	Integer	超时间隔。Overtime interval 最小值：**0** 最大值：**10** 缺省值：**10**

表 4-420 AlertRuleTrigger

参数	参数类型	描述
mode	String	模式，数量。Mode. COUNT. 缺省值：**COUNT** 最小长度：**1** 最大长度：**255** 枚举值： • **COUNT**
operator	String	操作符，等于、不等于、大于、小于。 operator. EQ equal, NE not equal, GT greater than, LT less than. 缺省值：**GT** 最小长度：**1** 最大长度：**255** 枚举值： • **EQ** • **NE** • **GT** • **LT**
expression	String	expression 最小长度：**1** 最大长度：**255**
severity	String	严重程度，提示、低危、中危、高危、致命。 Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**
accumulated_times	Integer	accumulated_times 最小值：**1** 最大值：**1000** 缺省值：**1**

状态码： 400

表 4-421 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

请求示例

更新一条告警规则，告警规则名称为Alert rule，查询类型为SQL，状态为启用，严重程度为提示。

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

响应示例

状态码： 200

Success

```
{
  "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 代码示例

SDK代码示例如下。

Java

更新一条告警规则，告警规则名称为Alert rule，查询类型为SQL，状态为启用，严重程度为提示。

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateAlertRuleRequest request = new UpdateAlertRuleRequest();
        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

更新一条告警规则，告警规则名称为Alert rule，查询类型为SQL，状态为启用，严重程度为提示。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

```
    try:
        request = UpdateAlertRuleRequest()
        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

更新一条告警规则，告警规则名称为Alert rule，查询类型为SQL，状态为启用，严重程度为提示。

```
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")

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

```
client := secmaster.NewSecMasterClient(
    secmaster.SecMasterClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.UpdateAlertRuleRequest{}
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)
}
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	Success
400	Bad Request

错误码

请参见**错误码**。

4.5.6 模拟告警规则

功能介绍

Simulate alert rule

调用方法

请参见**如何调用API**。

URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/simulation

表 4-422 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目 ID。Project ID. 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间 ID。Workspace ID. 最小长度：**32** 最大长度：**36**

请求参数

表 4-423 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取。 IAM user token, fetch from IAM api. 最小长度：**1** 最大长度：**2097152**

表 4-424 请求 Body 参数

参数	是否必选	参数类型	描述
pipe_id	是	String	数据管道 ID。Pipe ID. 最小长度：**36** 最大长度：**36**
query	是	String	查询语句。Query. 最小长度：**1** 最大长度：**1024**
query_type	否	String	查询语法，SQL。Query type. SQL. 缺省值：**SQL** 最小长度：**1** 最大长度：**255** 枚举值： • **SQL**
from	是	Long	开始时间。Start time. 最小值：**0** 最大值：**9223372036854775807**
to	是	Long	结束时间。End time. 最小值：**0** 最大值：**9223372036854775807**
event_grouping	否	Boolean	告警分组。Event grouping. 缺省值：**true**

参数	是否必选	参数类型	描述
triggers	是	Array of **AlertRuleTrigger** objects	告警触发规则。Alert triggers. 数组长度：**1 - 5**

表 4-425 AlertRuleTrigger

参数	是否必选	参数类型	描述
mode	否	String	模式，数量。Mode. COUNT. 缺省值：**COUNT** 最小长度：**1** 最大长度：**255** 枚举值： • **COUNT**
operator	否	String	操作符，等于、不等于、大于、小于。 operator. EQ equal, NE not equal, GT greater than, LT less than. 缺省值：**GT** 最小长度：**1** 最大长度：**255** 枚举值： • **EQ** • **NE** • **GT** • **LT**
expression	是	String	expression 最小长度：**1** 最大长度：**255**

参数	是否必选	参数类型	描述
severity	否	String	严重程度，提示、低危、中危、高危、致命。Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**
accumulated_times	否	Integer	accumulated_times 最小值：**1** 最大值：**1000** 缺省值：**1**

响应参数

状态码： 200

表 4-426 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

表 4-427 响应 Body 参数

参数	参数类型	描述
alert_count	Integer	告警数量。Alert count. 最小值：**0** 最大值：**100**
severity	String	严重程度，提示、低危、中危、高危、致命。Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 最小长度：**1** 最大长度：**64**

状态码： 400

表 4-428 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

请求示例

模拟一条告警规则，告警规则所属的管道ID为ead2769b-afb0-45dd-b9fa-a2953e6ac82f，查询类型为SQL，严重程度为提示。

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

响应示例

状态码： 200

Success

```
{
  "alert_count" : 100,
  "severity" : "TIPS"
}
```

SDK 代码示例

SDK代码示例如下。

Java

模拟一条告警规则，告警规则所属的管道ID为ead2769b-afb0-45dd-b9fa-a2953e6ac82f，查询类型为SQL，严重程度为提示。

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateAlertRuleSimulationRequest request = new CreateAlertRuleSimulationRequest();
        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

模拟一条告警规则，告警规则所属的管道ID为ead2769b-afb0-45dd-b9fa-a2953e6ac82f，查询类型为SQL，严重程度为提示。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = CreateAlertRuleSimulationRequest()
        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

模拟一条告警规则，告警规则所属的管道ID为ead2769b-afb0-45dd-b9fa-a2953e6ac82f，查询类型为SQL，严重程度为提示。

```
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")
```

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateAlertRuleSimulationRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	Success
400	Bad Request

错误码

请参见**错误码**。

4.5.7 告警规则总览

功能介绍

List alert rule metrics

调用方法

请参见**如何调用API**。

URI

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

表 4-429 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目 ID。Project ID. 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间 ID。Workspace ID. 最小长度：**32** 最大长度：**36**

请求参数

表 4-430 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取。 IAM user token, fetch from IAM api. 最小长度：**1** 最大长度：**2097152**

响应参数

状态码： 200

表 4-431 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

表 4-432 响应 Body 参数

参数	参数类型	描述
category	String	指标类型，分组数量。Metric category. GROUP_COUNT. 枚举值： • **GROUP_COUNT**
metric	Map<String,Number>	指标值。Metric value.

状态码： 400

表 4-433 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

请求示例

无

响应示例

状态码： 200

Success

- 示例 1

```
{
  "category" : {
    "GROUP_COUNT" : null
  },
  "metric" : null
}
```

- 示例 2

```
{
  "category" : "GROUP_COUNT",
```

```
 "metric" : {
   "ENABLED" : 8,
   "DISABLED" : 2
 }
}
```

SDK 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListAlertRuleMetricsRequest request = new ListAlertRuleMetricsRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListAlertRuleMetricsRequest()
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	Success
400	Bad Request

错误码

请参见**错误码**。

4.5.8 启用告警规则

功能介绍

Enable alert rule

调用方法

请参见**如何调用API**。

URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/enable

表 4-434 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目 ID。Project ID. 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间 ID。Workspace ID. 最小长度：**32** 最大长度：**36**

请求参数

表 4-435 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取。 IAM user token, fetch from IAM api. 最小长度：**1** 最大长度：**2097152**

表 4-436 请求 Body 参数

参数	是否必选	参数类型	描述
[数组元素]	是	Array of strings	EnableAlertRuleRequestBody

响应参数

状态码： 200

表 4-437 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

表 4-438 响应 Body 参数

参数	参数类型	描述
rule_id	String	告警规则 ID。Alert rule ID. 最小长度：**36** 最大长度：**36**

参数	参数类型	描述
status	String	启用状态，启用、停用。Status, enabled, disabled. 最小长度：**1** 最大长度：**255** 枚举值： • **ENABLED** • **DISABLED**

状态码： 400

表 4-439 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

请求示例

启用告警规则,名称为123123

```
[ "123123" ]
```

响应示例

状态码： 200

Success

```
{
  "rule_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
  "status" : "ENABLED"
}
```

SDK 代码示例

SDK代码示例如下。

Java

启用告警规则,名称为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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        EnableAlertRuleRequest request = new EnableAlertRuleRequest();
        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

启用告警规则,名称为123123

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

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



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

    try:
        request = EnableAlertRuleRequest()
        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

启用告警规则,名称为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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.EnableAlertRuleRequest{}
    var listBodybody = []string{
        "123123",
    }
    request.Body = &listBodybody
    response, err := client.EnableAlertRule(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	Success
400	Bad Request

错误码

请参见**错误码**。

4.5.9 停用告警规则

功能介绍

Disable alert rule

调用方法

请参见**如何调用API**。

URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/disable

表 4-440 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目 ID。Project ID. 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间 ID。Workspace ID. 最小长度：**32** 最大长度：**36**

请求参数

表 4-441 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取。 IAM user token, fetch from IAM api. 最小长度：**1** 最大长度：**2097152**

表 4-442 请求 Body 参数

参数	是否必选	参数类型	描述
[数组元素]	是	Array of strings	DisableAlertRuleRequestBody

响应参数

状态码： 200

表 4-443 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

表 4-444 响应 Body 参数

参数	参数类型	描述
rule_id	String	告警规则 ID。Alert rule ID. 最小长度：**36** 最大长度：**36**

参数	参数类型	描述
status	String	启用状态，启用、停用。Status, enabled, disabled. 最小长度：**1** 最大长度：**255** 枚举值： • **ENABLED** • **DISABLED**

状态码： 400

表 4-445 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

请求示例

停用告警规则,名称为123123

```
[ "123123" ]
```

响应示例

状态码： 200

Success

```
{
  "rule_id" : "443a0117-1aa4-4595-ad4a-796fad4d4950",
  "status" : "ENABLED"
}
```

SDK 代码示例

SDK代码示例如下。

Java

停用告警规则,名称为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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DisableAlertRuleRequest request = new DisableAlertRuleRequest();
        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

停用告警规则,名称为123123

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

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

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

    try:
        request = DisableAlertRuleRequest()
        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

停用告警规则,名称为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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DisableAlertRuleRequest{}
    var listBodybody = []string{
        "123123",
    }
    request.Body = &listBodybody
    response, err := client.DisableAlertRule(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	Success
400	Bad Request

错误码

请参见**错误码**。

4.5.10 列出告警规则模板

功能介绍

List alert rule templates

调用方法

请参见**如何调用API**。

URI

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

表 4-446 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目 ID。Project ID. 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间 ID。Workspace ID. 最小长度：**32** 最大长度：**36**

表 4-447 Query 参数

参数	是否必选	参数类型	描述
offset	是	Long	偏移量。Offset. 最小值：**0** 最大值：**9223372036854775807**
limit	是	Long	条数。Limit. 最小值：**10** 最大值：**50**
sort_key	否	String	排序字段。Sort key 最小长度：**1** 最大长度：**256**
sort_dir	否	String	排序顺序，顺序、逆序。Sort direction, asc, desc。 枚举值： • **asc** • **desc**
severity	否	Array	严重程度，提示、低危、中危、高危、致命。Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 数组长度：**1 - 5** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**

请求参数

表 4-448 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取。 IAM user token, fetch from IAM api. 最小长度：**1** 最大长度：**2097152**

响应参数

状态码： 200

表 4-449 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

表 4-450 响应 Body 参数

参数	参数类型	描述
count	Long	总数量。Total count. 最小值：**0** 最大值：**9223372036854775807**
records	Array of **AlertRuleTemplate** objects	告警规则模板。Alert rule templates. 数组长度：**0 - 100**

表 4-451 AlertRuleTemplate

参数	参数类型	描述
template_id	String	告警规则模板 ID。Alert rule template ID. 最小长度：**36** 最大长度：**36**
update_time	Long	更新时间。Update time. 最小值：**0** 最大值：**9223372036854775807**
template_name	String	告警规则模板名称。Alert rule template name. 最小长度：**1** 最大长度：**255**
data_source	String	数据源。Data source. 最小长度：**1** 最大长度：**255**

参数	参数类型	描述
version	String	版本。Version 最小长度：**1** 最大长度：**255**
query	String	查询语句。Query. 最小长度：**1** 最大长度：**1024**
query_type	String	查询语法，SQL。Query type. SQL. 缺省值：**SQL** 最小长度：**1** 最大长度：**255** 枚举值： • **SQL**
severity	String	严重程度，提示、低危、中危、高危、致命。Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 缺省值：**TIPS** 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**
custom_properties	Map<String,String>	自定义扩展信息。Custom properties.
event_grouping	Boolean	告警分组。Event grouping. 缺省值：**true**
schedule	**Schedule** object	
triggers	Array of **AlertRuleTrigger** objects	告警触发规则。Alert triggers. 数组长度：**1 - 5**

表 4-452 Schedule

参数	参数类型	描述
frequency_interval	Integer	调度间隔。Frequency interval. 最小值：**1** 最大值：**60**
frequency_unit	String	调度间隔单位，分钟、小时、天。Frequency unit. MINUTE, HOUR, DAY. 最小长度：**1** 最大长度：**255** 枚举值： • **MINUTE** • **HOUR** • **DAY**
period_interval	Integer	时间窗口间隔。Period interval. 最小值：**1** 最大值：**60**
period_unit	String	时间窗口单位，分钟、小时、天。Period unit. MINUTE, HOUR, DAY. 最小长度：**1** 最大长度：**255** 枚举值： • **MINUTE** • **HOUR** • **DAY**
delay_interval	Integer	延迟间隔。Delay interval 最小值：**0** 最大值：**10** 缺省值：**0**
overtime_interval	Integer	超时间隔。Overtime interval 最小值：**0** 最大值：**10** 缺省值：**10**

表 4-453 AlertRuleTrigger

参数	参数类型	描述
mode	String	模式，数量。Mode. COUNT. 缺省值：**COUNT** 最小长度：**1** 最大长度：**255** 枚举值： • **COUNT**
operator	String	操作符，等于、不等于、大于、小于。 operator. EQ equal, NE not equal, GT greater than, LT less than. 缺省值：**GT** 最小长度：**1** 最大长度：**255** 枚举值： • **EQ** • **NE** • **GT** • **LT**
expression	String	expression 最小长度：**1** 最大长度：**255**
severity	String	严重程度，提示、低危、中危、高危、致命。 Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**
accumulated_times	Integer	accumulated_times 最小值：**1** 最大值：**1000** 缺省值：**1**

状态码： 400

表 4-454 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

请求示例

无

响应示例

状态码： 200

Success

```
{
  "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 代码示例

SDK代码示例如下。

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 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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListAlertRuleTemplatesRequest request = new ListAlertRuleTemplatesRequest();
        request.withOffset(<offset>L);
        request.withLimit(<limit>L);
        request.withSortKey("<sort_key>");
        request.withSortDir(ListAlertRuleTemplatesRequest.SortDirEnum.fromValue("<sort_dir>"));
        request.withSeverity();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")
```

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

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

    try:
        request = ListAlertRuleTemplatesRequest()
        request.offset = <offset>
        request.limit = <limit>
        request.sort_key = "<sort_key>"
        request.sort_dir = "<sort_dir>"
        request.severity =
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAlertRuleTemplatesRequest{}
    request.Offset = int64(<offset>)
    request.Limit = int64(<limit>)
    sortKeyRequest:= "<sort_key>"
    request.SortKey = &sortKeyRequest
    sortDirRequest:= model.GetListAlertRuleTemplatesRequestSortDirEnum().<SORT_DIR>
    request.SortDir = &sortDirRequest
    response, err := client.ListAlertRuleTemplates(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	Success
400	Bad Request

错误码

请参见**错误码**。

4.5.11 查看告警规则模板

功能介绍

List alert rule templates

调用方法

请参见**如何调用API**。

URI

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

表 4-455 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目 ID。Project ID. 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间 ID。Workspace ID. 最小长度：**32** 最大长度：**36**
template_id	是	String	告警规则模板 ID。Alert rule template ID. 最小长度：**36** 最大长度：**36**

请求参数

表 4-456 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取。 IAM user token, fetch from IAM api. 最小长度：**1** 最大长度：**2097152**

响应参数

状态码： 200

表 4-457 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

表 4-458 响应 Body 参数

参数	参数类型	描述
template_id	String	告警规则模板 ID。Alert rule template ID. 最小长度：**36** 最大长度：**36**
update_time	Long	更新时间。Update time. 最小值：**0** 最大值：**9223372036854775807**
template_name	String	告警规则模板名称。Alert rule template name. 最小长度：**1** 最大长度：**255**
data_source	String	数据源。Data source. 最小长度：**1** 最大长度：**255**

参数	参数类型	描述
version	String	版本。Version 最小长度：**1** 最大长度：**255**
query	String	查询语句。Query. 最小长度：**1** 最大长度：**1024**
query_type	String	查询语法，SQL。Query type. SQL. 缺省值：**SQL** 最小长度：**1** 最大长度：**255** 枚举值： • **SQL**
severity	String	严重程度，提示、低危、中危、高危、致命。Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 缺省值：**TIPS** 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**
custom_properties	Map<String,String>	自定义扩展信息。Custom properties.
event_grouping	Boolean	告警分组。Event grouping. 缺省值：**true**
schedule	**Schedule** object	
triggers	Array of **AlertRuleTrigger** objects	告警触发规则。Alert triggers. 数组长度：**1 - 5**

表 4-459 Schedule

参数	参数类型	描述
frequency_interval	Integer	调度间隔。Frequency interval. 最小值：**1** 最大值：**60**
frequency_unit	String	调度间隔单位，分钟、小时、天。Frequency unit. MINUTE, HOUR, DAY. 最小长度：**1** 最大长度：**255** 枚举值： • **MINUTE** • **HOUR** • **DAY**
period_interval	Integer	时间窗口间隔。Period interval. 最小值：**1** 最大值：**60**
period_unit	String	时间窗口单位，分钟、小时、天。Period unit. MINUTE, HOUR, DAY. 最小长度：**1** 最大长度：**255** 枚举值： • **MINUTE** • **HOUR** • **DAY**
delay_interval	Integer	延迟间隔。Delay interval 最小值：**0** 最大值：**10** 缺省值：**0**
overtime_interval	Integer	超时间隔。Overtime interval 最小值：**0** 最大值：**10** 缺省值：**10**

表 4-460 AlertRuleTrigger

参数	参数类型	描述
mode	String	模式，数量。Mode. COUNT. 缺省值：**COUNT** 最小长度：**1** 最大长度：**255** 枚举值： • **COUNT**
operator	String	操作符，等于、不等于、大于、小于。 operator. EQ equal, NE not equal, GT greater than, LT less than. 缺省值：**GT** 最小长度：**1** 最大长度：**255** 枚举值： • **EQ** • **NE** • **GT** • **LT**
expression	String	expression 最小长度：**1** 最大长度：**255**
severity	String	严重程度，提示、低危、中危、高危、致命。 Severity. TIPS, LOW, MEDIUM, HIGH, FATAL 最小长度：**1** 最大长度：**255** 枚举值： • **TIPS** • **LOW** • **MEDIUM** • **HIGH** • **FATAL**
accumulated_times	Integer	accumulated_times 最小值：**1** 最大值：**1000** 缺省值：**1**

状态码： 400

表 4-461 响应 Header 参数

参数	参数类型	描述
X-request-id	String	This field is the request ID number for task tracking. Format is request_uuid-timestamp-hostname.

请求示例

无

响应示例

状态码： 200

Success

```
{
  "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 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowAlertRuleTemplateRequest request = new ShowAlertRuleTemplateRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ShowAlertRuleTemplateRequest()
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	Success
400	Bad Request

错误码

请参见**错误码**。

4.6 剧本版本管理

4.6.1 克隆剧本及版本

功能介绍

克隆剧本及版本

调用方法

请参见**如何调用API**。

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/clone

表 4-462 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
version_id	是	String	剧本版本ID 最小长度：**32** 最大长度：**64**

请求参数

表 4-463 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

表 4-464 请求 Body 参数

参数	是否必选	参数类型	描述
name	否	String	名称 最小长度：**32** 最大长度：**64**

响应参数

状态码： 200

表 4-465 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-466 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	Error message 最小长度：**1** 最大长度：**32**
data	**PlaybookVersionInfo** object	剧本版本详情信息

表 4-467 PlaybookVersionInfo

参数	参数类型	描述
id	String	剧本版本ID 最小长度：**32** 最大长度：**64**
description	String	描述 最小长度：**0** 最大长度：**1024**
create_time	String	创建时间 最小长度：**0** 最大长度：**64**
update_time	String	更新时间 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
creator_id	String	创建者ID 最小长度：**32** 最大长度：**64**
modifier_id	String	修改者ID 最小长度：**32** 最大长度：**64**

参数	参数类型	描述
playbook_id	String	剧本ID 最小长度：**32** 最大长度：**64**
version	String	版本号 最小长度：**32** 最大长度：**64**
enabled	Boolean	是否启用。（ true--已启用，false-未启用 ）
status	String	剧本版本状态，编辑中：EDITING 审核中：APPROVING 不通过：UNPASSED 已发布：PUBLISHED 最小长度：**0** 最大长度：**64**
action_strategy	String	执行策略. 目前仅支持异步并发执行，对应值为ASYNC 最小长度：**0** 最大长度：**64**
actions	Array of **ActionInfo** objects	剧本关联流程列表信息 数组长度：**0 - 99**
rule_enable	Boolean	是否启用触发条件过滤器
rules	**RuleInfo** object	剧本触发规格信息
dataclass_id	String	数据类ID 最小长度：**0** 最大长度：**64**
trigger_type	String	剧本触发方式(EVENT--事件触发，TIMER--定时触发) 最小长度：**0** 最大长度：**64**
dataobject_create	Boolean	标识数据对象是否创建时触发剧本
dataobject_update	Boolean	标识数据对象是否更新时触发剧本
dataobject_delete	Boolean	标识数据对象是否删除时触发剧本

参数	参数类型	描述
version_type	Integer	版本类型（0--草稿版本，1--正式版本) 最小值：**0** 最大值：**1**
rule_id	String	过滤规则ID 最小长度：**0** 最大长度：**64**
dataclass_name	String	数据类名称 最小长度：**0** 最大长度：**64**
approve_name	String	审核者 最小长度：**0** 最大长度：**64**

表 4-468 ActionInfo

参数	参数类型	描述
id	String	剧本流程动作ID 最小长度：**32** 最大长度：**64**
name	String	流程动作名称 最小长度：**0** 最大长度：**1024**
description	String	描述 最小长度：**0** 最大长度：**1024**
action_type	String	流程动作类型 最小长度：**0** 最大长度：**64**
action_id	String	流程ID 最小长度：**32** 最大长度：**64**
playbook_id	String	剧本ID 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
playbook_version_id	String	剧本版本ID 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**0** 最大长度：**64**

表 4-469 RuleInfo

参数	参数类型	描述
id	String	规则ID 最小长度：**32** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
rule	String	触发规则 最小长度：**0** 最大长度：**128**

状态码： 400

表 4-470 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-471 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

克隆一个剧本及其版本，剧本名称为name。

```
{
  "name" : "name"
}
```

响应示例

状态码： 200

请求成功响应参数

```
{
  "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 代码示例

SDK代码示例如下。

Java

克隆一个剧本及其版本，剧本名称为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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CopyPlaybookVersionRequest request = new CopyPlaybookVersionRequest();
        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

克隆一个剧本及其版本，剧本名称为name。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = CopyPlaybookVersionRequest()
        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

克隆一个剧本及其版本，剧本名称为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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CopyPlaybookVersionRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应参数
400	请求失败响应参数

错误码

请参见**错误码**。

4.6.2 查询剧本版本列表

功能介绍

查询剧本版本列表

调用方法

请参见**如何调用API**。

URI

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

表 4-472 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**

参数	是否必选	参数类型	描述
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
playbook_id	是	String	剧本ID 最小长度：**32** 最大长度：**64**

表 4-473 Query 参数

参数	是否必选	参数类型	描述
status	否	String	剧本版本状态，编辑中：EDITING 审核中：APPROVING 不通过：UNPASSED 已发布：PUBLISHED 最小长度：**0** 最大长度：**64**
enabled	否	Integer	启用/禁用 最小值：**0** 最大值：**1**
version_type	否	Integer	版本类型， 草稿版本：0 正式版本：1 最小值：**0** 最大值：**10**
offset	否	Integer	分页查询参数。用于指定查询结果的起始位置，从0开始 最小值：**0** 最大值：**999999**
limit	否	Integer	分页查询参数，用于指定一次查询最多的结果数，从1开始 最小值：**1** 最大值：**999999**

请求参数

表 4-474 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-475 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-476 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	错误信息 最小长度：**1** 最大长度：**32**
size	Integer	分页查询数据大小 最小值：**0** 最大值：**9999**

参数	参数类型	描述
page	Integer	当前页码 最小值：**0** 最大值：**100**
total	Integer	总数 最小值：**0** 最大值：**99999**
data	Array of **PlaybookVersionListEntity** objects	剧本版本列表信息 数组长度：**0 - 100000000**

表 4-477 PlaybookVersionListEntity

参数	参数类型	描述
id	String	剧本版本ID 最小长度：**32** 最大长度：**64**
description	String	描述 最小长度：**0** 最大长度：**1024**
create_time	String	创建时间 最小长度：**0** 最大长度：**64**
update_time	String	更新时间 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
creator_id	String	创建者ID 最小长度：**32** 最大长度：**64**
modifier_id	String	修改者ID 最小长度：**32** 最大长度：**64**

参数	参数类型	描述
playbook_id	String	剧本ID 最小长度：**32** 最大长度：**64**
version	String	版本号 最小长度：**32** 最大长度：**64**
enabled	Boolean	是否激活
status	String	状态. (EDITING--编辑中, APPROVING--审核中, UNPASSED--审核不通过, PUBLISHED--审核通过) 最小长度：**0** 最大长度：**64**
action_strategy	String	执行策略. 目前仅支持异步并发执行，对应值为ASYNC 最小长度：**0** 最大长度：**64**
rule_enable	Boolean	过滤规则是否启用
dataclass_id	String	数据类ID 最小长度：**0** 最大长度：**64**
trigger_type	String	触发方式. EVENT--事件触发, TIMER--定时触发 最小长度：**0** 最大长度：**64**
dataobject_create	Boolean	标识数据对象是否创建时触发剧本
dataobject_update	Boolean	标识数据对象是否更新时触发剧本
dataobject_delete	Boolean	标识数据对象是否删除时触发剧本
version_type	Integer	版本类型 最小值：**0** 最大值：**1**
rule_id	String	过滤规则ID 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
dataclass_name	String	数据类名称 最小长度：**0** 最大长度：**64**
approve_name	String	审核者 最小长度：**0** 最大长度：**64**

状态码： 400

表 4-478 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-479 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

请求成功响应信息

```
{
  "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 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybookVersionsRequest request = new ListPlaybookVersionsRequest();
        request.withStatus("<status>");
        request.withEnabled(<enabled>);
        request.withVersionType(<version_type>);
        request.withOffset(<offset>);
        request.withLimit(<limit>);
```



```
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListPlaybookVersionsRequest()
        request.status = "<status>"
        request.enabled = <enabled>
        request.version_type = <version_type>
        request.offset = <offset>
        request.limit = <limit>
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPlaybookVersionsRequest{}
    statusRequest:= "<status>"
    request.Status = &statusRequest
    enabledRequest:= int32(<enabled>)
    request.Enabled = &enabledRequest
    versionTypeRequest:= int32(<version_type>)
    request.VersionType = &versionTypeRequest
    offsetRequest:= int32(<offset>)
    request.Offset = &offsetRequest
    limitRequest:= int32(<limit>)
    request.Limit = &limitRequest
    response, err := client.ListPlaybookVersions(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.6.3 创建剧本版本

功能介绍

创建剧本版本

调用方法

请参见**如何调用API**。

URI

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

表 4-480 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
playbook_id	是	String	剧本ID 最小长度：**32** 最大长度：**64**

请求参数

表 4-481 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

表 4-482 请求 Body 参数

参数	是否必选	参数类型	描述
description	否	String	描述 最小长度：**0** 最大长度：**1024**
workspace_id	否	String	工作空间ID 最小长度：**0** 最大长度：**2097152**
playbook_id	否	String	剧本ID 最小长度：**32** 最大长度：**64**
actions	否	Array of **ActionInfo** objects	关联流程列表 数组长度：**0 - 99**
dataclass_id	否	String	数据类ID 最小长度：**32** 最大长度：**64**
rule_enable	否	Boolean	过滤规则是否启用
rule_id	否	String	过滤规则ID 最小长度：**0** 最大长度：**64**
trigger_type	否	String	触发方式. EVENT--事件触发, TIMER--定时触发 最小长度：**0** 最大长度：**64**
dataobject_create	否	Boolean	标识数据对象是否创建时触发剧本
dataobject_update	否	Boolean	标识数据对象是否更新时触发剧本
dataobject_delete	否	Boolean	标识数据对象是否删除时触发剧本
action_strategy	否	String	执行策略. 目前仅支持异步并发执行，对应值为ASYNC 最小长度：**1** 最大长度：**64**

表 4-483 ActionInfo

参数	是否必选	参数类型	描述
id	否	String	剧本流程动作ID 最小长度：**32** 最大长度：**64**
name	否	String	流程动作名称 最小长度：**0** 最大长度：**1024**
description	否	String	描述 最小长度：**0** 最大长度：**1024**
action_type	否	String	流程动作类型 最小长度：**0** 最大长度：**64**
action_id	否	String	流程ID 最小长度：**32** 最大长度：**64**
playbook_id	否	String	剧本ID 最小长度：**0** 最大长度：**64**
playbook_version_id	否	String	剧本版本ID 最小长度：**0** 最大长度：**64**
project_id	否	String	项目ID 最小长度：**0** 最大长度：**64**

响应参数

状态码： 200

表 4-484 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-485 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	Error message 最小长度：**1** 最大长度：**32**
data	**PlaybookVersionInfo** object	剧本版本详情信息

表 4-486 PlaybookVersionInfo

参数	参数类型	描述
id	String	剧本版本ID 最小长度：**32** 最大长度：**64**
description	String	描述 最小长度：**0** 最大长度：**1024**
create_time	String	创建时间 最小长度：**0** 最大长度：**64**
update_time	String	更新时间 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
creator_id	String	创建者ID 最小长度：**32** 最大长度：**64**
modifier_id	String	修改者ID 最小长度：**32** 最大长度：**64**

参数	参数类型	描述
playbook_id	String	剧本ID 最小长度：**32** 最大长度：**64**
version	String	版本号 最小长度：**32** 最大长度：**64**
enabled	Boolean	是否启用。（ true--已启用，false-未启用 ）
status	String	剧本版本状态，编辑中：EDITING 审核中：APPROVING 不通过：UNPASSED 已发布：PUBLISHED 最小长度：**0** 最大长度：**64**
action_strategy	String	执行策略. 目前仅支持异步并发执行，对应值为ASYNC 最小长度：**0** 最大长度：**64**
actions	Array of **ActionInfo** objects	剧本关联流程列表信息 数组长度：**0 - 99**
rule_enable	Boolean	是否启用触发条件过滤器
rules	**RuleInfo** object	剧本触发规格信息
dataclass_id	String	数据类ID 最小长度：**0** 最大长度：**64**
trigger_type	String	剧本触发方式(EVENT--事件触发，TIMER--定时触发) 最小长度：**0** 最大长度：**64**
dataobject_create	Boolean	标识数据对象是否创建时触发剧本
dataobject_update	Boolean	标识数据对象是否更新时触发剧本
dataobject_delete	Boolean	标识数据对象是否删除时触发剧本

参数	参数类型	描述
version_type	Integer	版本类型（0--草稿版本，1--正式版本) 最小值：**0** 最大值：**1**
rule_id	String	过滤规则ID 最小长度：**0** 最大长度：**64**
dataclass_name	String	数据类名称 最小长度：**0** 最大长度：**64**
approve_name	String	审核者 最小长度：**0** 最大长度：**64**

表 4-487 ActionInfo

参数	参数类型	描述
id	String	剧本流程动作ID 最小长度：**32** 最大长度：**64**
name	String	流程动作名称 最小长度：**0** 最大长度：**1024**
description	String	描述 最小长度：**0** 最大长度：**1024**
action_type	String	流程动作类型 最小长度：**0** 最大长度：**64**
action_id	String	流程ID 最小长度：**32** 最大长度：**64**
playbook_id	String	剧本ID 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
playbook_version_id	String	剧本版本ID 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**0** 最大长度：**64**

表 4-488 RuleInfo

参数	参数类型	描述
id	String	规则ID 最小长度：**32** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
rule	String	触发规则 最小长度：**0** 最大长度：**128**

状态码： 400

表 4-489 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-490 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

创建一个剧本版本，剧本版本所属工作空间ID为string，剧本ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，数据类ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，规则为启用。

```
{
  "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"
}
```

响应示例

状态码： 200

请求成功响应信息

```
{
  "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 代码示例

SDK代码示例如下。

Java

创建一个剧本版本，剧本版本所属工作空间ID为string，剧本ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，数据类ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，规则为启用。

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
```

```
        CreatePlaybookVersionRequest request = new CreatePlaybookVersionRequest();
        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

创建一个剧本版本，剧本版本所属工作空间ID为string，剧本ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，数据类ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，规则为启用。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

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

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

    try:
        request = CreatePlaybookVersionRequest()
        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

创建一个剧本版本，剧本版本所属工作空间ID为string，剧本ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，数据类ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，规则为启用。

```
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")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
```

```
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePlaybookVersionRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.6.4 查询剧本版本详情

功能介绍

Show playbook version version

调用方法

请参见**如何调用API**。

URI

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

表 4-491 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
version_id	是	String	剧本版本ID 最小长度：**32** 最大长度：**64**

请求参数

表 4-492 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-493 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-494 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	Error message 最小长度：**1** 最大长度：**32**
data	**PlaybookVersionInfo** object	剧本版本详情信息

表 4-495 PlaybookVersionInfo

参数	参数类型	描述
id	String	剧本版本ID 最小长度：**32** 最大长度：**64**
description	String	描述 最小长度：**0** 最大长度：**1024**
create_time	String	创建时间 最小长度：**0** 最大长度：**64**
update_time	String	更新时间 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
creator_id	String	创建者ID 最小长度：**32** 最大长度：**64**
modifier_id	String	修改者ID 最小长度：**32** 最大长度：**64**
playbook_id	String	剧本ID 最小长度：**32** 最大长度：**64**
version	String	版本号 最小长度：**32** 最大长度：**64**
enabled	Boolean	是否启用。（true--已启用，false-未启用）
status	String	剧本版本状态，编辑中：EDITING 审核中：APPROVING 不通过：UNPASSED 已发布：PUBLISHED 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
action_strategy	String	执行策略. 目前仅支持异步并发执行，对应值为ASYNC 最小长度：**0** 最大长度：**64**
actions	Array of **ActionInfo** objects	剧本关联流程列表信息 数组长度：**0 - 99**
rule_enable	Boolean	是否启用触发条件过滤器
rules	**RuleInfo** object	剧本触发规格信息
dataclass_id	String	数据类ID 最小长度：**0** 最大长度：**64**
trigger_type	String	剧本触发方式(EVENT--事件触发，TIMER--定时触发) 最小长度：**0** 最大长度：**64**
dataobject_create	Boolean	标识数据对象是否创建时触发剧本
dataobject_update	Boolean	标识数据对象是否更新时触发剧本
dataobject_delete	Boolean	标识数据对象是否删除时触发剧本
version_type	Integer	版本类型（0--草稿版本，1--正式版本) 最小值：**0** 最大值：**1**
rule_id	String	过滤规则ID 最小长度：**0** 最大长度：**64**
dataclass_name	String	数据类名称 最小长度：**0** 最大长度：**64**
approve_name	String	审核者 最小长度：**0** 最大长度：**64**

表 4-496 ActionInfo

参数	参数类型	描述
id	String	剧本流程动作ID 最小长度：**32** 最大长度：**64**
name	String	流程动作名称 最小长度：**0** 最大长度：**1024**
description	String	描述 最小长度：**0** 最大长度：**1024**
action_type	String	流程动作类型 最小长度：**0** 最大长度：**64**
action_id	String	流程ID 最小长度：**32** 最大长度：**64**
playbook_id	String	剧本ID 最小长度：**0** 最大长度：**64**
playbook_version_id	String	剧本版本ID 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**0** 最大长度：**64**

表 4-497 RuleInfo

参数	参数类型	描述
id	String	规则ID 最小长度：**32** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**

参数	参数类型	描述
rule	String	触发规则 最小长度：**0** 最大长度：**128**

状态码： 400

表 4-498 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-499 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

请求成功响应信息

```
{
  "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 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
```



```
        ShowPlaybookVersionRequest request = new ShowPlaybookVersionRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ShowPlaybookVersionRequest()
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.6.5 删除剧本版本

功能介绍

删除剧本版本

调用方法

请参见**如何调用API**。

URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}

表 4-500 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
version_id	是	String	剧本版本ID 最小长度：**32** 最大长度：**64**

请求参数

表 4-501 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-502 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-503 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	响应消息 最小长度：**1** 最大长度：**32**

状态码： 400

表 4-504 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-505 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

请求成功响应信息

```
{
  "code" : 0,
  "message" : "Error message"
}
```

SDK 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeletePlaybookVersionRequest request = new DeletePlaybookVersionRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = DeletePlaybookVersionRequest()
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.6.6 更新剧本版本

功能介绍

更新剧本版本

调用方法

请参见**如何调用API**。

URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}

表 4-506 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
version_id	是	String	剧本版本ID 最小长度：**32** 最大长度：**64**

请求参数

表 4-507 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

表 4-508 请求 Body 参数

参数	是否必选	参数类型	描述
description	否	String	描述 最小长度：**0** 最大长度：**1024**
workspace_id	否	String	工作空间ID 最小长度：**0** 最大长度：**2097152**
playbook_id	否	String	剧本ID 最小长度：**32** 最大长度：**64**
dataclass_id	否	String	数据类ID 最小长度：**32** 最大长度：**64**
rule_enable	否	Boolean	是否启用触发条件过滤器
enabled	否	Boolean	是否激活。(false:未激活, true:已激活)

参数	是否必选	参数类型	描述
status	否	String	状态(APPROVING:审核中，EDITING-编辑中，UNPASSED-审核未通过，PUBLISHED-已发布) 最小长度：**0** 最大长度：**64**
rule_id	否	String	规则ID 最小长度：**0** 最大长度：**64**
trigger_type	否	String	触发方式. EVENT--事件触发, TIMER--定时触发 最小长度：**0** 最大长度：**64**
dataobject_create	否	Boolean	数据对象是否创建时触发剧本
dataobject_update	否	Boolean	数据对象是否更新时触发剧本
dataobject_delete	否	Boolean	数据对象是否删除时触发剧本
action_strategy	否	String	执行策略. 目前仅支持异步并发执行，对应值为ASYNC 最小长度：**0** 最大长度：**64**

响应参数

状态码： 200

表 4-509 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-510 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	Error message 最小长度：**1** 最大长度：**32**
data	**PlaybookVersionInfo** object	剧本版本详情信息

表 4-511 PlaybookVersionInfo

参数	参数类型	描述
id	String	剧本版本ID 最小长度：**32** 最大长度：**64**
description	String	描述 最小长度：**0** 最大长度：**1024**
create_time	String	创建时间 最小长度：**0** 最大长度：**64**
update_time	String	更新时间 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
creator_id	String	创建者ID 最小长度：**32** 最大长度：**64**
modifier_id	String	修改者ID 最小长度：**32** 最大长度：**64**

参数	参数类型	描述
playbook_id	String	剧本ID 最小长度：**32** 最大长度：**64**
version	String	版本号 最小长度：**32** 最大长度：**64**
enabled	Boolean	是否启用。（ true--已启用，false-未启用 ）
status	String	剧本版本状态，编辑中：EDITING 审核中：APPROVING 不通过：UNPASSED 已发布：PUBLISHED 最小长度：**0** 最大长度：**64**
action_strategy	String	执行策略. 目前仅支持异步并发执行，对应值为ASYNC 最小长度：**0** 最大长度：**64**
actions	Array of **ActionInfo** objects	剧本关联流程列表信息 数组长度：**0 - 99**
rule_enable	Boolean	是否启用触发条件过滤器
rules	**RuleInfo** object	剧本触发规格信息
dataclass_id	String	数据类ID 最小长度：**0** 最大长度：**64**
trigger_type	String	剧本触发方式(EVENT--事件触发，TIMER--定时触发) 最小长度：**0** 最大长度：**64**
dataobject_create	Boolean	标识数据对象是否创建时触发剧本
dataobject_update	Boolean	标识数据对象是否更新时触发剧本
dataobject_delete	Boolean	标识数据对象是否删除时触发剧本

参数	参数类型	描述
version_type	Integer	版本类型（0--草稿版本，1--正式版本) 最小值：**0** 最大值：**1**
rule_id	String	过滤规则ID 最小长度：**0** 最大长度：**64**
dataclass_name	String	数据类名称 最小长度：**0** 最大长度：**64**
approve_name	String	审核者 最小长度：**0** 最大长度：**64**

表 4-512 ActionInfo

参数	参数类型	描述
id	String	剧本流程动作ID 最小长度：**32** 最大长度：**64**
name	String	流程动作名称 最小长度：**0** 最大长度：**1024**
description	String	描述 最小长度：**0** 最大长度：**1024**
action_type	String	流程动作类型 最小长度：**0** 最大长度：**64**
action_id	String	流程ID 最小长度：**32** 最大长度：**64**
playbook_id	String	剧本ID 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
playbook_version_id	String	剧本版本ID 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**0** 最大长度：**64**

表 4-513 RuleInfo

参数	参数类型	描述
id	String	规则ID 最小长度：**32** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
rule	String	触发规则 最小长度：**0** 最大长度：**128**

状态码： 400

表 4-514 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-515 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

更新一个剧本版本，剧本版本所属工作空间ID为string，剧本ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，数据类ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，剧本状态为已启用。

```
{
  "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"
}
```

响应示例

状态码： 200

请求成功响应信息

```
{
  "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 代码示例

SDK代码示例如下。

Java

更新一个剧本版本，剧本版本所属工作空间ID为string，剧本ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，数据类ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，剧本状态为已启用。

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdatePlaybookVersionRequest request = new UpdatePlaybookVersionRequest();
        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

更新一个剧本版本，剧本版本所属工作空间ID为string，剧本ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，数据类ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，剧本状态为已启用。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = UpdatePlaybookVersionRequest()
        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

更新一个剧本版本，剧本版本所属工作空间ID为string，剧本ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，数据类ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，剧本状态为已启用。

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdatePlaybookVersionRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.7 剧本规则管理

4.7.1 查询剧本规则详情

功能介绍

查询剧本规则详情

调用方法

请参见**如何调用API**。

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/rules/{rule_id}

表 4-516 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
version_id	是	String	version Id value 最小长度：**32** 最大长度：**64**
rule_id	是	String	version Id value 最小长度：**32** 最大长度：**64**

请求参数

表 4-517 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-518 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-519 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	错误信息 最小长度：**1** 最大长度：**32**
data	**RuleInfo** object	剧本触发规格信息

表 4-520 RuleInfo

参数	参数类型	描述
id	String	规则ID 最小长度：**32** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
rule	String	触发规则 最小长度：**0** 最大长度：**128**

状态码： 400

表 4-521 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-522 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

请求成功响应信息

```
{
  "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 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookRuleRequest request = new ShowPlaybookRuleRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ShowPlaybookRuleRequest()
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.7.2 删除剧本规则

功能介绍

删除剧本规则

调用方法

请参见**如何调用API**。

URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/rules/{rule_id}

表 4-523 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
version_id	是	String	剧本版本ID 最小长度：**32** 最大长度：**64**
rule_id	是	String	规则ID 最小长度：**36** 最大长度：**36**

请求参数

表 4-524 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-525 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-526 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	响应消息 最小长度：**1** 最大长度：**32**

状态码： 400

表 4-527 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-528 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

请求成功响应信息

```
{
  "code" : 0,
  "message" : "Error message"
}
```

SDK 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeletePlaybookRuleRequest request = new DeletePlaybookRuleRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = DeletePlaybookRuleRequest()
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
```

```
        Build())

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.7.3 创建剧本规则

功能介绍

创建剧本规则

调用方法

请参见**如何调用API**。

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/rules

表 4-529 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**

参数	是否必选	参数类型	描述
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
version_id	是	String	剧本版本ID 最小长度：**32** 最大长度：**64**

请求参数

表 4-530 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

表 4-531 请求 Body 参数

参数	是否必选	参数类型	描述
rule	是	**ConditionInfo** object	剧本触发规则详情

表 4-532 ConditionInfo

参数	是否必选	参数类型	描述
expression_type	否	String	表达式类型。默认为common,事件触发剧本必填 最小长度：**0** 最大长度：**64**
conditions	否	Array of **ConditionItem** objects	触发条件。事件触发剧本必填 数组长度：**0 - 99**
logics	否	Array of strings	条件逻辑组合。事件触发剧本必填 最小长度：**0** 最大长度：**64** 数组长度：**0 - 99**
cron	否	String	Cron 表达式（定时任务）。定时触发剧本必填 最小长度：**0** 最大长度：**64**
schedule_type	否	String	定时重复类型(second--秒,hour--小时,day--天，week-周)。定时触发剧本必填 最小长度：**0** 最大长度：**64**
start_type	否	String	剧本开始执行类型，IMMEDIATELY--创建完成立即执行, CUSTOM--自定义执行时间。定时触发剧本必填 最小长度：**0** 最大长度：**64**
end_type	否	String	剧本结束执行类型，FOREVER--一直执行, CUSTOM--自定义结束时间。定时触发剧本必填 最小长度：**0** 最大长度：**64**
end_time	否	String	定时结束时间。定时触发剧本必填 最小长度：**0** 最大长度：**64**

参数	是否必选	参数类型	描述
repeat_range	否	String	执行时间段 2021-01-30T23:00:00Z+0800。定时触发剧本必填 最小长度：**0** 最大长度：**64**
only_once	否	Boolean	是否只执行一次。定时触发剧本必填
execution_type	否	String	执行队列类型（PARALLEL-新任务与之前任务并行）。定时触发剧本必填 最小长度：**0** 最大长度：**64**

表 4-533 ConditionItem

参数	是否必选	参数类型	描述
name	否	String	条件名称 最小长度：**0** 最大长度：**64**
detail	否	String	条件详情 最小长度：**0** 最大长度：**1028**
data	否	Array of strings	条件表达式数据 最小长度：**0** 最大长度：**2048** 数组长度：**0 - 99**

响应参数

状态码： 200

表 4-534 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-535 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	错误信息 最小长度：**1** 最大长度：**32**
data	**RuleInfo** object	剧本触发规格信息

表 4-536 RuleInfo

参数	参数类型	描述
id	String	规则ID 最小长度：**32** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
rule	String	触发规则 最小长度：**0** 最大长度：**128**

状态码： 400

表 4-537 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-538 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

创建一条剧本规则，名称为logic1，表达式类型为所有，

```
{
  "rule" : {
    "expression_type" : "common",
    "conditions" : [ {
      "name" : "condition_0",
      "detail" : "123",
      "data" : [ "waf.alarm.level', '>', '3" ]
    } ],
    "logics" : [ "condition_0" ]
  }
}
```

响应示例

状态码： 200

请求成功响应信息

```
{
  "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 代码示例

SDK代码示例如下。

Java

创建一条剧本规则，名称为logic1，表达式类型为所有，

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePlaybookRuleRequest request = new CreatePlaybookRuleRequest();
        CreateRuleInfo body = new CreateRuleInfo();
        List<String> listRuleLogics = new ArrayList<>();
        listRuleLogics.add("condition_0");
        List<String> listConditionsData = new ArrayList<>();
        listConditionsData.add("waf.alarm.level', '>', '3");
        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

创建一条剧本规则，名称为logic1，表达式类型为所有，

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



```
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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = CreatePlaybookRuleRequest()
        listLogicsRule = [
            "condition_0"
        ]
        listDataConditions = [
            "waf.alarm.level", ">", "3"
        ]
        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

创建一条剧本规则，名称为logic1，表达式类型为所有，

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePlaybookRuleRequest{}
    var listLogicsRule = []string{
        "condition_0",
    }
    var listDataConditions = []string{
        "waf.alarm.level', '>', '3",
    }
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.7.4 更新剧本规则

功能介绍

更新剧本规则

调用方法

请参见**如何调用API**。

URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/rules/{rule_id}

表 4-539 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
version_id	是	String	剧本版本ID 最小长度：**32** 最大长度：**64**
rule_id	是	String	剧本规则ID 最小长度：**36** 最大长度：**36**

请求参数

表 4-540 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

表 4-541 请求 Body 参数

参数	是否必选	参数类型	描述
rule	否	**ConditionInfo** object	剧本触发规则详情

表 4-542 ConditionInfo

参数	是否必选	参数类型	描述
expression_type	否	String	表达式类型。默认为common，事件触发剧本必填 最小长度：**0** 最大长度：**64**
conditions	否	Array of **ConditionItem** objects	触发条件。事件触发剧本必填 数组长度：**0 - 99**
logics	否	Array of strings	条件逻辑组合。事件触发剧本必填 最小长度：**0** 最大长度：**64** 数组长度：**0 - 99**

参数	是否必选	参数类型	描述
cron	否	String	Cron 表达式（定时任务）。定时触发剧本必填 最小长度：**0** 最大长度：**64**
schedule_type	否	String	定时重复类型(second--秒, hour--小时,day--天，week-周)。定时触发剧本必填 最小长度：**0** 最大长度：**64**
start_type	否	String	剧本开始执行类型，IMMEDIATELY--创建完成立即执行, CUSTOM--自定义执行时间。定时触发剧本必填 最小长度：**0** 最大长度：**64**
end_type	否	String	剧本结束执行类型，FOREVER--一直执行, CUSTOM--自定义结束时间。定时触发剧本必填 最小长度：**0** 最大长度：**64**
end_time	否	String	定时结束时间。定时触发剧本必填 最小长度：**0** 最大长度：**64**
repeat_range	否	String	执行时间段 2021-01-30T23:00:00Z+0800。定时触发剧本必填 最小长度：**0** 最大长度：**64**
only_once	否	Boolean	是否只执行一次。定时触发剧本必填
execution_type	否	String	执行队列类型（PARALLEL-新任务与之前任务并行）。定时触发剧本必填 最小长度：**0** 最大长度：**64**

表 4-543 ConditionItem

参数	是否必选	参数类型	描述
name	否	String	条件名称 最小长度：**0** 最大长度：**64**
detail	否	String	条件详情 最小长度：**0** 最大长度：**1028**
data	否	Array of strings	条件表达式数据 最小长度：**0** 最大长度：**2048** 数组长度：**0 - 99**

响应参数

状态码： 200

表 4-544 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-545 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	错误信息 最小长度：**1** 最大长度：**32**
data	**RuleInfo** object	剧本触发规格信息

表 4-546 RuleInfo

参数	参数类型	描述
id	String	规则ID 最小长度：**32** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
rule	String	触发规则 最小长度：**0** 最大长度：**128**

状态码： 400

表 4-547 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-548 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

更新一条剧本规则，名称为logic1，表达式类型为所有，

```
{
  "rule" : {
    "expression_type" : "common",
    "conditions" : [ {
      "name" : "condition_0",
      "detail" : "123",
      "data" : [ "waf.alarm.level', '>', '3" ]
    } ],
```

```
    "logics" : "[\"condition_0\"]"
  }
}
```

响应示例

状态码： 200

请求成功响应参数

```
{
  "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 代码示例

SDK代码示例如下。

Java

更新一条剧本规则，名称为logic1，表达式类型为所有，

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdatePlaybookRuleRequest request = new UpdatePlaybookRuleRequest();
        ModifyRuleInfo body = new ModifyRuleInfo();
        List<String> listConditionsData = new ArrayList<>();
        listConditionsData.add('waf.alarm.level', '>', '3');
        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();
        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

更新一条剧本规则，名称为logic1，表达式类型为所有，

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = UpdatePlaybookRuleRequest()
        listDataConditions = [
            "waf.alarm.level", ">", "3"
        ]
        listConditionsRule = [
            ConditionItem(
                name="condition_0",
                detail="123",
                data=listDataConditions
            )
        ]
        rulebody = ConditionInfo(
```

```
        expression_type="common",
        conditions=listConditionsRule,
    )
    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

更新一条剧本规则，名称为logic1，表达式类型为所有，

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdatePlaybookRuleRequest{}
    var listDataConditions = []string{
        "waf.alarm.level", '>', '3",
    }
    nameConditions:= "condition_0"
    detailConditions:= "123"
    var listConditionsRule = []model.ConditionItem{
        {
            Name: &nameConditions,
            Detail: &detailConditions,
            Data: &listDataConditions,
        },
    }
    expressionTypeRule:= "common"
    rulebody := &model.ConditionInfo{
        ExpressionType: &expressionTypeRule,
        Conditions: &listConditionsRule,
    }
    request.Body = &model.ModifyRuleInfo{
        Rule: rulebody,
    }
```

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应参数
400	请求失败响应参数

错误码

请参见**错误码**。

4.8 剧本实例管理

4.8.1 查询剧本实例列表

功能介绍

查询剧本实例列表

调用方法

请参见**如何调用API**。

URI

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

表 4-549 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**

参数	是否必选	参数类型	描述
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**

表 4-550 Query 参数

参数	是否必选	参数类型	描述
status	否	String	剧本实例状态. (RUNNING--运行中、FINISHED--成功、FAILED--失败、RETRYING--重试中、TERMINATING--终止中、TERMINATED--已终止) 最小长度：**0** 最大长度：**64**
name	否	String	实例名称 最小长度：**0** 最大长度：**64**
playbook_name	否	String	剧本名称 最小长度：**0** 最大长度：**64**
dataclass_name	否	String	数据类名称 最小长度：**0** 最大长度：**64**
dataobject_name	否	String	数据对象名称 最小长度：**0** 最大长度：**64**
trigger_type	否	String	触发类型. TIMER--定时触发, EVENT--事件触发 最小长度：**0** 最大长度：**64**
from_date	否	String	查询起始时间 最小长度：**32** 最大长度：**36**
to_date	否	String	查询结束时间 最小长度：**32** 最大长度：**36**

参数	是否必选	参数类型	描述
limit	是	Integer	分页查询参数，用于指定一次查询最多的结果数，从1开始 最小值：**1** 最大值：**999999**
offset	是	Integer	分页查询参数。用于指定查询结果的起始位置，从0开始 最小值：**0** 最大值：**999999**

请求参数

表 4-551 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-552 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-553 响应 Body 参数

参数	参数类型	描述
count	Integer	总数 最小值：**0** 最大值：**99999**
instances	Array of **PlaybookInstanceInfo** objects	剧本实例列表信息 数组长度：**0 - 100**

表 4-554 PlaybookInstanceInfo

参数	参数类型	描述
id	String	剧本实例ID 最小长度：**32** 最大长度：**64**
name	String	剧本实例名称 最小长度：**0** 最大长度：**1024**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
playbook	**PlaybookInfoRef** object	剧本信息
dataclass	**DataclassInfoRef** object	数据类信息
dataobject	**DataobjectInfo** object	数据对象详情
status	String	剧本实例状态. (RUNNING--运行中、FINISHED--成功、FAILED--失败、RETRYING--重试中、TERMINATING--终止中、TERMINATED--已终止) 最小长度：**32** 最大长度：**64**
trigger_type	String	触发类型. TIMER--定时触发, EVENT--事件触发 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
start_time	String	创建时间 最小长度：**0** 最大长度：**64**
end_time	String	更新时间 最小长度：**0** 最大长度：**64**

表 4-555 PlaybookInfoRef

参数	参数类型	描述
id	String	剧本ID 最小长度：**32** 最大长度：**64**
version_id	String	剧本版本ID 最小长度：**32** 最大长度：**64**
name	String	名称 最小长度：**32** 最大长度：**64**
version	String	版本 最小长度：**32** 最大长度：**64**

表 4-556 DataclassInfoRef

参数	参数类型	描述
id	String	数据类ID 最小长度：**32** 最大长度：**64**
name	String	数据类名称 最小长度：**32** 最大长度：**64**

表 4-557 DataobjectInfo

参数	参数类型	描述
id	String	ID值 最小长度：**32** 最大长度：**64**
create_time	String	创建时间 最小长度：**0** 最大长度：**64**
update_time	String	更新时间 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
dataclass_id	String	数据类ID 最小长度：**32** 最大长度：**64**
name	String	名称 最小长度：**0** 最大长度：**1024**
content	String	数据内容 最小长度：**0** 最大长度：**4096**

状态码： 400

表 4-558 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-559 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

请求成功响应信息

```
{
  "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 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybookInstancesRequest request = new ListPlaybookInstancesRequest();
        request.withStatus("<status>");
        request.withName("<name>");
        request.withPlaybookName("<playbook_name>");
        request.withDataclassName("<dataclass_name>");
        request.withDataobjectName("<dataobject_name>");
        request.withTriggerType("<trigger_type>");
        request.withFromDate("<from_date>");
        request.withToDate("<to_date>");
        request.withLimit(<limit>);
        request.withOffset(<offset>);
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListPlaybookInstancesRequest()
        request.status = "<status>"
        request.name = "<name>"
        request.playbook_name = "<playbook_name>"
        request.dataclass_name = "<dataclass_name>"
        request.dataobject_name = "<dataobject_name>"
        request.trigger_type = "<trigger_type>"
        request.from_date = "<from_date>"
        request.to_date = "<to_date>"
        request.limit = <limit>
        request.offset = <offset>
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPlaybookInstancesRequest{}
    statusRequest:= "<status>"
    request.Status = &statusRequest
    nameRequest:= "<name>"
    request.Name = &nameRequest
    playbookNameRequest:= "<playbook_name>"
```

```
    request.PlaybookName = &playbookNameRequest
    dataclassNameRequest:= "<dataclass_name>"
    request.DataclassName = &dataclassNameRequest
    dataobjectNameRequest:= "<dataobject_name>"
    request.DataobjectName = &dataobjectNameRequest
    triggerTypeRequest:= "<trigger_type>"
    request.TriggerType = &triggerTypeRequest
    fromDateRequest:= "<from_date>"
    request.FromDate = &fromDateRequest
    toDateRequest:= "<to_date>"
    request.ToDate = &toDateRequest
    request.Limit = int32(<limit>)
    request.Offset = int32(<offset>)
    response, err := client.ListPlaybookInstances(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.8.2 查询剧本实例详情

功能介绍

Show playbook instance

调用方法

请参见**如何调用API**。

URI

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

表 4-560 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
instance_id	是	String	instance _id 最小长度：**36** 最大长度：**36**

请求参数

表 4-561 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-562 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-563 响应 Body 参数

参数	参数类型	描述
id	String	剧本实例ID 最小长度：**32** 最大长度：**64**
name	String	剧本实例名称 最小长度：**0** 最大长度：**1024**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
playbook	**PlaybookInfoRef** object	剧本信息
dataclass	**DataclassInfoRef** object	数据类信息
dataobject	**DataobjectInfo** object	数据对象详情
status	String	剧本实例状态. (RUNNING--运行中、FINISHED--成功、FAILED--失败、RETRYING--重试中、TERMINATING--终止中、TERMINATED--已终止) 最小长度：**32** 最大长度：**64**
trigger_type	String	触发类型. TIMER--定时触发, EVENT--事件触发 最小长度：**0** 最大长度：**64**
start_time	String	创建时间 最小长度：**0** 最大长度：**64**
end_time	String	更新时间 最小长度：**0** 最大长度：**64**

表 4-564 PlaybookInfoRef

参数	参数类型	描述
id	String	剧本ID 最小长度：**32** 最大长度：**64**
version_id	String	剧本版本ID 最小长度：**32** 最大长度：**64**
name	String	名称 最小长度：**32** 最大长度：**64**
version	String	版本 最小长度：**32** 最大长度：**64**

表 4-565 DataclassInfoRef

参数	参数类型	描述
id	String	数据类ID 最小长度：**32** 最大长度：**64**
name	String	数据类名称 最小长度：**32** 最大长度：**64**

表 4-566 DataobjectInfo

参数	参数类型	描述
id	String	ID值 最小长度：**32** 最大长度：**64**
create_time	String	创建时间 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
update_time	String	更新时间 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
dataclass_id	String	数据类ID 最小长度：**32** 最大长度：**64**
name	String	名称 最小长度：**0** 最大长度：**1024**
content	String	数据内容 最小长度：**0** 最大长度：**4096**

状态码： 400

表 4-567 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-568 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 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 代码示例

SDK代码示例如下。

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");

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

```
        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookInstanceRequest request = new ShowPlaybookInstanceRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ShowPlaybookInstanceRequest()
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	Instance Informations
400	Error response

错误码

请参见**错误码**。

4.8.3 操作剧本实例

功能介绍

操作剧本实例

调用方法

请参见**如何调用API**。

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}/operation

表 4-569 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
instance_id	是	String	剧本实例ID 最小长度：**36** 最大长度：**36**

请求参数

表 4-570 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

表 4-571 请求 Body 参数

参数	是否必选	参数类型	描述
operation	否	String	操作类型。重试： RETRY 终止： TERMINATE 最小长度：**0** 最大长度：**64**

响应参数

状态码： 200

表 4-572 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-573 响应 Body 参数

参数	参数类型	描述
id	String	剧本实例ID 最小长度：**32** 最大长度：**64**
name	String	剧本实例名称 最小长度：**0** 最大长度：**1024**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
playbook	**PlaybookInfoRef** object	剧本信息
dataclass	**DataclassInfoRef** object	数据类信息
dataobject	**DataobjectInfo** object	数据对象详情

参数	参数类型	描述
status	String	剧本实例状态. (RUNNING--运行中、FINISHED--成功、FAILED--失败、RETRYING--重试中、TERMINATING--终止中、TERMINATED--已终止) 最小长度：**32** 最大长度：**64**
trigger_type	String	触发类型. TIMER--定时触发, EVENT--事件触发 最小长度：**0** 最大长度：**64**
start_time	String	创建时间 最小长度：**0** 最大长度：**64**
end_time	String	更新时间 最小长度：**0** 最大长度：**64**

表 4-574 PlaybookInfoRef

参数	参数类型	描述
id	String	剧本ID 最小长度：**32** 最大长度：**64**
version_id	String	剧本版本ID 最小长度：**32** 最大长度：**64**
name	String	名称 最小长度：**32** 最大长度：**64**
version	String	版本 最小长度：**32** 最大长度：**64**

表 4-575 DataclassInfoRef

参数	参数类型	描述
id	String	数据类ID 最小长度：**32** 最大长度：**64**
name	String	数据类名称 最小长度：**32** 最大长度：**64**

表 4-576 DataobjectInfo

参数	参数类型	描述
id	String	ID值 最小长度：**32** 最大长度：**64**
create_time	String	创建时间 最小长度：**0** 最大长度：**64**
update_time	String	更新时间 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**32** 最大长度：**64**
dataclass_id	String	数据类ID 最小长度：**32** 最大长度：**64**
name	String	名称 最小长度：**0** 最大长度：**1024**
content	String	数据内容 最小长度：**0** 最大长度：**4096**

状态码： 400

表 4-577 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-578 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

重试所有操作剧本实例。

```
{
  "operation" : "RETRY"
}
```

响应示例

状态码： 200

请求成功响应信息

```
{
  "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 代码示例

SDK代码示例如下。

Java

重试所有操作剧本实例。

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ChangePlaybookInstanceRequest request = new ChangePlaybookInstanceRequest();
        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

重试所有操作剧本实例。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ChangePlaybookInstanceRequest()
        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

重试所有操作剧本实例。

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ChangePlaybookInstanceRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.8.4 查询剧本拓扑关系

功能介绍

查询剧本拓扑关系

调用方法

请参见**如何调用API**。

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}/topology

表 4-579 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**

参数	是否必选	参数类型	描述
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
instance_id	是	String	剧本实例ID 最小长度：**36** 最大长度：**36**

请求参数

表 4-580 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-581 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-582 响应 Body 参数

参数	参数类型	描述
count	Integer	总数 最小值：**0** 最大值：**99999**
action_instances	Array of **ActionInstanceInfo** objects	流程实例列表 数组长度：**0 - 100**

表 4-583 ActionInstanceInfo

参数	参数类型	描述
action	**ActionInfo** object	剧本流程动作信息
instance_log	**AuditLogInfo** object	剧本实例审计日志信息

表 4-584 ActionInfo

参数	参数类型	描述
id	String	剧本流程动作ID 最小长度：**32** 最大长度：**64**
name	String	流程动作名称 最小长度：**0** 最大长度：**1024**
description	String	描述 最小长度：**0** 最大长度：**1024**
action_type	String	流程动作类型 最小长度：**0** 最大长度：**64**
action_id	String	流程ID 最小长度：**32** 最大长度：**64**

参数	参数类型	描述
playbook_id	String	剧本ID 最小长度：**0** 最大长度：**64**
playbook_version_id	String	剧本版本ID 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**0** 最大长度：**64**

表 4-585 AuditLogInfo

参数	参数类型	描述
instance_type	String	实例类型（AOP_WORKFLOW--流程, SCRIPT--脚本, PLAYBOOK--剧本） 最小长度：**0** 最大长度：**64**
action_id	String	流程ID 最小长度：**0** 最大长度：**1028**
action_name	String	流程名称 最小长度：**0** 最大长度：**64**
instance_id	String	实例ID 最小长度：**0** 最大长度：**1028**
parent_instance_id	String	父节点实例ID 最小长度：**0** 最大长度：**64**
log_level	String	日志级别 最小长度：**0** 最大长度：**1028**
input	String	输入 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
output	String	输出 最小长度：**0** 最大长度：**1028**
error_msg	String	错误信息 最小长度：**0** 最大长度：**64**
start_time	String	开始时间 最小长度：**0** 最大长度：**1028**
end_time	String	结束时间 最小长度：**0** 最大长度：**64**
status	String	状态。(RUNNING--运行中、FINISHED--成功、FAILED--失败、RETRYING--重试中、TERMINATING--终止中、TERMINATED--已终止) 最小长度：**0** 最大长度：**1028**
trigger_type	String	触发类型. TIMER--定时触发, EVENT--事件触发 最小长度：**0** 最大长度：**1028**

状态码： 400

表 4-586 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-587 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

请求成功响应信息

```
{
  "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 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPlaybookTopologyRequest request = new ShowPlaybookTopologyRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ShowPlaybookTopologyRequest()
```

```
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.8.5 查询剧本实例审计日志

功能介绍

查询剧本实例审计日志

调用方法

请参见**如何调用API**。

URI

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

表 4-588 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**

表 4-589 Query 参数

参数	是否必选	参数类型	描述
offset	是	Long	offset 最小值：**0** 最大值：**9223372036854775807**
limit	是	Long	limit 最小值：**10** 最大值：**50**
sort_key	否	String	sort_key 最小长度：**1** 最大长度：**256**

参数	是否必选	参数类型	描述
sort_dir	否	String	sort_dir. asc, desc 枚举值： • **asc** • **desc**

请求参数

表 4-590 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

表 4-591 请求 Body 参数

参数	是否必选	参数类型	描述
instance_type	否	String	实例类型（AOP_WORKFLOW--流程, SCRIPT--脚本, PLAYBOOK--剧本） 最小长度：**0** 最大长度：**64**
action_id	否	String	流程ID 最小长度：**0** 最大长度：**1028**
action_name	否	String	流程名称 最小长度：**0** 最大长度：**64**

参数	是否必选	参数类型	描述
instance_id	否	String	实例ID 最小长度：**0** 最大长度：**1028**
parent_instance_id	否	String	父节点实例ID 最小长度：**0** 最大长度：**64**
log_level	否	String	日志级别 最小长度：**0** 最大长度：**1028**
input	否	String	输入 最小长度：**0** 最大长度：**64**
output	否	String	输出 最小长度：**0** 最大长度：**1028**
error_msg	否	String	错误信息 最小长度：**0** 最大长度：**64**
start_time	否	String	开始时间 最小长度：**0** 最大长度：**1028**
end_time	否	String	结束时间 最小长度：**0** 最大长度：**64**
status	否	String	状态。(RUNNING--运行中、FINISHED--成功、FAILED--失败、RETRYING--重试中、TERMINATING--终止中、TERMINATED--已终止) 最小长度：**0** 最大长度：**1028**
trigger_type	否	String	触发类型. TIMER--定时触发, EVENT--事件触发 最小长度：**0** 最大长度：**1028**

响应参数

状态码： 200

表 4-592 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-593 响应 Body 参数

参数	参数类型	描述
count	Integer	总条数 最小值：**0** 最大值：**99999**
audit_logs	Array of **AuditLogInfo** objects	审计日志列表信息 数组长度：**0 - 100**

表 4-594 AuditLogInfo

参数	参数类型	描述
instance_type	String	实例类型（AOP_WORKFLOW--流程, SCRIPT--脚本, PLAYBOOK--剧本） 最小长度：**0** 最大长度：**64**
action_id	String	流程ID 最小长度：**0** 最大长度：**1028**
action_name	String	流程名称 最小长度：**0** 最大长度：**64**
instance_id	String	实例ID 最小长度：**0** 最大长度：**1028**
parent_instance_id	String	父节点实例ID 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
log_level	String	日志级别 最小长度：**0** 最大长度：**1028**
input	String	输入 最小长度：**0** 最大长度：**64**
output	String	输出 最小长度：**0** 最大长度：**1028**
error_msg	String	错误信息 最小长度：**0** 最大长度：**64**
start_time	String	开始时间 最小长度：**0** 最大长度：**1028**
end_time	String	结束时间 最小长度：**0** 最大长度：**64**
status	String	状态。(RUNNING--运行中、FINISHED--成功、FAILED--失败、RETRYING--重试中、TERMINATING--终止中、TERMINATED--已终止) 最小长度：**0** 最大长度：**1028**
trigger_type	String	触发类型. TIMER--定时触发, EVENT--事件触发 最小长度：**0** 最大长度：**1028**

状态码： 400

表 4-595 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-596 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

查询实例类型为APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG，动作id为909494e3-558e-46b6-a9eb-07a8e18ca62f，动作名称为DisabledIp，实例id为909494e3-558e-46b6-a9eb-07a8e18ca62f，父实例id为909494e3-558e-46b6-a9eb-07a8e18ca62f，日志等级为DEBUG INFO WARN，输入为input，输出为output，错误信息为error_msg，开始时间2021-01-30 23：00：00，结束时间2021-01-31 23：00：00，状态为CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED，触发类型为DEBUG, TIMER, EVENT, MANUAL的剧本实例审计日志

```
{
  "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"
}
```

响应示例

状态码： 200

请求成功响应信息

```
{
  "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 代码示例

SDK代码示例如下。

Java

查询实例类型为APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG，动作id为909494e3-558e-46b6-a9eb-07a8e18ca62f，动作名称为DisabledIp，实例id为909494e3-558e-46b6-a9eb-07a8e18ca62f，父实例id为909494e3-558e-46b6-a9eb-07a8e18ca62f，日志等级为DEBUG INFO WARN，输入为input，输出为output，错误信息为error_msg，开始时间2021-01-30 23：00：00，结束时间2021-01-31 23：00：00，状态为CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED，触发类型为DEBUG, TIMER, EVENT, MANUAL的剧本实例审计日志

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybookAuditLogsRequest request = new ListPlaybookAuditLogsRequest();
        request.withOffset(<offset>L);
        request.withLimit(<limit>L);
        request.withSortKey("<sort_key>");
        request.withSortDir(ListPlaybookAuditLogsRequest.SortDirEnum.fromValue("<sort_dir>"));
        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

查询实例类型为APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG，动作id为909494e3-558e-46b6-a9eb-07a8e18ca62f，动作名称为DisabledIp，实例id为909494e3-558e-46b6-a9eb-07a8e18ca62f，父实例id为909494e3-558e-46b6-a9eb-07a8e18ca62f，日志等级为DEBUG INFO WARN，输入为input，输出为output，错误信息为error_msg，开始时间2021-01-30 23：00：00，结束时间2021-01-31 23：00：00，状态为CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED，触发类型为DEBUG, TIMER, EVENT, MANUAL的剧本实例审计日志

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListPlaybookAuditLogsRequest()
        request.offset = <offset>
        request.limit = <limit>
        request.sort_key = "<sort_key>"
        request.sort_dir = "<sort_dir>"
        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

查询实例类型为APP, AOP_WORKFLOW, SCRIPT, PLAYBOOK, TASK, DEBUG，动作id为909494e3-558e-46b6-a9eb-07a8e18ca62f，动作名称为DisabledIp，实例id为909494e3-558e-46b6-a9eb-07a8e18ca62f，父实例id为909494e3-558e-46b6-a9eb-07a8e18ca62f，日志等级为DEBUG INFO WARN，输入为input，输出为output，错误信息为error_msg，开始时间2021-01-30 23：00：00，结束时间2021-01-31 23：00：00，状态为CREATED, RUNNING, FINISHED, RETRYING, TERMINATING, TERMINATED, FAILED，触发类型为DEBUG, TIMER, EVENT, MANUAL的剧本实例审计日志

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPlaybookAuditLogsRequest{}
    request.Offset = int64(<offset>)
    request.Limit = int64(<limit>)
    sortKeyRequest:= "<sort_key>"
    request.SortKey = &sortKeyRequest
    sortDirRequest:= model.GetListPlaybookAuditLogsRequestSortDirEnum().<SORT_DIR>
    request.SortDir = &sortDirRequest
```

```
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.9 剧本审核管理

4.9.1 审核剧本

功能介绍

审核剧本

调用方法

请参见**如何调用API**。

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/approval

表 4-597 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
version_id	是	String	版本ID 最小长度：**32** 最大长度：**64**

请求参数

表 4-598 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**

参数	是否必选	参数类型	描述
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

表 4-599 请求 Body 参数

参数	是否必选	参数类型	描述
result	否	String	审核结果 通过：PASS 不通过：UN_PASS 最小长度：**32** 最大长度：**64**
content	否	String	审核意见 最小长度：**32** 最大长度：**64**

响应参数

状态码： 200

表 4-600 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-601 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	响应消息 最小长度：**1** 最大长度：**32**

参数	参数类型	描述
data	ApproveOpinionDetail object	审核详情信息

表 4-602 ApproveOpinionDetail

参数	参数类型	描述
result	String	审核结果 最小长度：**0** 最大长度：**64**
content	String	审核内容 最小长度：**0** 最大长度：**1028**

状态码： 400

表 4-603 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-604 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

审核一个剧本，审核结果为PASS，审核意见为xxxxx。

```
{
  "result" : "PASS",
```

```
  "content" : "xxxxx"
}
```

响应示例

状态码： 200

请求成功响应信息

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : {
    "result" : "PASS",
    "content" : "need modify"
  }
}
```

SDK 代码示例

SDK代码示例如下。

Java

审核一个剧本，审核结果为PASS，审核意见为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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePlaybookApproveRequest request = new CreatePlaybookApproveRequest();
        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

审核一个剧本，审核结果为PASS，审核意见为xxxxx。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = CreatePlaybookApproveRequest()
        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

审核一个剧本，审核结果为PASS，审核意见为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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePlaybookApproveRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.9.2 查询剧本审核结果

功能介绍

查询剧本审核结果

调用方法

请参见**如何调用API**。

URI

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

表 4-605 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**

表 4-606 Query 参数

参数	是否必选	参数类型	描述
resource_id	否	String	资源ID 最小长度：**0** 最大长度：**64**
approve_type	否	String	审核类型。（PLAYBOOK-剧本, AOP_WORKFLOW--流程) 最小长度：**0** 最大长度：**64**

请求参数

表 4-607 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**

参数	是否必选	参数类型	描述
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-608 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-609 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	响应消息 最小长度：**1** 最大长度：**32**
data	Array of **ApproveOpinionDetail** objects	剧本审核详情 数组长度：**0 - 99**

表 4-610 ApproveOpinionDetail

参数	参数类型	描述
result	String	审核结果 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
content	String	审核内容 最小长度：**0** 最大长度：**1028**

状态码： 400

表 4-611 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-612 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

请求成功响应信息

```
{
  "code" : 0,
  "message" : "Error message",
  "data" : [ {
    "result" : "PASS",
    "content" : "need modify"
  } ]
}
```

SDK 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPlaybookApprovesRequest request = new ListPlaybookApprovesRequest();
        request.withResourceId("<resource_id>");
        request.withApproveType("<approve_type>");
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
```

```
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListPlaybookApprovesRequest()
        request.resource_id = "<resource_id>"
        request.approve_type = "<approve_type>"
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPlaybookApprovesRequest{}
    resourceIdRequest:= "<resource_id>"
    request.ResourceId = &resourceIdRequest
    approveTypeRequest:= "<approve_type>"
    request.ApproveType = &approveTypeRequest
    response, err := client.ListPlaybookApproves(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.10 剧本动作管理

4.10.1 查询剧本动作

功能介绍

查询剧本动作列表

调用方法

请参见**如何调用API**。

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/actions

表 4-613 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**

参数	是否必选	参数类型	描述
version_id	是	String	剧本版本ID 最小长度：**32** 最大长度：**64**

表 4-614 Query 参数

参数	是否必选	参数类型	描述
limit	是	Integer	分页查询参数，用于指定一次查询最多的结果数，从1开始 最小值：**0** 最大值：**999999**
offset	是	Integer	分页查询参数。用于指定查询结果的起始位置，从0开始 最小值：**1** 最大值：**999999**

请求参数

表 4-615 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-616 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-617 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	错误信息 最小长度：**1** 最大长度：**32**
total	Integer	总数 最小值：**0** 最大值：**99999**
size	Integer	分页大小 最小值：**0** 最大值：**9999**
page	Integer	当前页数 最小值：**0** 最大值：**100**
data	Array of **ActionInfo** objects	剧本动作列表信息 数组长度：**0 - 100**

表 4-618 ActionInfo

参数	参数类型	描述
id	String	剧本流程动作ID 最小长度：**32** 最大长度：**64**
name	String	流程动作名称 最小长度：**0** 最大长度：**1024**

参数	参数类型	描述
description	String	描述 最小长度：**0** 最大长度：**1024**
action_type	String	流程动作类型 最小长度：**0** 最大长度：**64**
action_id	String	流程ID 最小长度：**32** 最大长度：**64**
playbook_id	String	剧本ID 最小长度：**0** 最大长度：**64**
playbook_version_id	String	剧本版本ID 最小长度：**0** 最大长度：**64**
project_id	String	项目ID 最小长度：**0** 最大长度：**64**

状态码： 400

表 4-619 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-620 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

请求成功响应参数

```
{
  "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 代码示例

SDK代码示例如下。

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");

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

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

```
            .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
            .build();
        ListPlaybookActionsRequest request = new ListPlaybookActionsRequest();
        request.withLimit(<limit>);
        request.withOffset(<offset>);
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListPlaybookActionsRequest()
        request.limit = <limit>
        request.offset = <offset>
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPlaybookActionsRequest{}
    request.Limit = int32(<limit>)
    request.Offset = int32(<offset>)
    response, err := client.ListPlaybookActions(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应参数
400	请求失败请求参数

错误码

请参见**错误码**。

4.10.2 创建剧本动作

功能介绍

创建剧本动作

调用方法

请参见**如何调用API**。

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/actions

表 4-621 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
version_id	是	String	剧本版本ID 最小长度：**32** 最大长度：**64**

请求参数

表 4-622 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

表 4-623 请求 Body 参数

参数	是否必选	参数类型	描述
[数组元素]	是	Array of CreateAction objects	创建剧本版本请求

表 4-624 CreateAction

参数	是否必选	参数类型	描述
name	否	String	名称 最小长度：**0** 最大长度：**1024**
description	否	String	描述 最小长度：**0** 最大长度：**1024**
action_type	是	String	类型，默认AOP_WORKFLOW. 最小长度：**0** 最大长度：**64**
action_id	是	String	剧本动作ID 最小长度：**32** 最大长度：**64**
sort_order	否	String	排序方式 最小长度：**0** 最大长度：**64**

响应参数

状态码： 200

表 4-625 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-626 响应 Body 参数

参数	参数类型	描述
code	String	Error code 最小长度：**1** 最大长度：**32**
message	String	Error message 最小长度：**1** 最大长度：**32**
data	Array of **ActionInfo** objects	list of informations of playbook action 数组长度：**0 - 100**

表 4-627 ActionInfo

参数	参数类型	描述
id	String	剧本流程动作ID 最小长度：**32** 最大长度：**64**
name	String	流程动作名称 最小长度：**0** 最大长度：**1024**
description	String	描述 最小长度：**0** 最大长度：**1024**
action_type	String	流程动作类型 最小长度：**0** 最大长度：**64**
action_id	String	流程ID 最小长度：**32** 最大长度：**64**
playbook_id	String	剧本ID 最小长度：**0** 最大长度：**64**
playbook_version_id	String	剧本版本ID 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
project_id	String	项目ID 最小长度：**0** 最大长度：**64**

状态码： 400

表 4-628 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-629 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

创建一个剧本动作，剧本名称为MyXXX，描述为This my XXXX，剧本动作类型为aopworkflow，剧本动作ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，排序顺序为string。

```
[ {
  "name" : "MyXXX",
  "description" : "This my XXXX",
  "action_type" : "aopworkflow",
  "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "sort_order" : "string"
} ]
```

响应示例

状态码： 200

请求成功响应信息

```
{
  "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 代码示例

SDK代码示例如下。

Java

创建一个剧本动作，剧本名称为MyXXX，描述为This my XXXX，剧本动作类型为aopworkflow，剧本动作ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，排序顺序为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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePlaybookActionRequest request = new CreatePlaybookActionRequest();
        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

创建一个剧本动作，剧本名称为MyXXX，描述为This my XXXX，剧本动作类型为aopworkflow，剧本动作ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，排序顺序为string。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = CreatePlaybookActionRequest()
        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

创建一个剧本动作，剧本名称为MyXXX，描述为This my XXXX，剧本动作类型为aopworkflow，剧本动作ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，排序顺序为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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePlaybookActionRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应信息
400	请求失败响应信息

错误码

请参见**错误码**。

4.10.3 删除剧本动作

功能介绍

删除剧本动作

调用方法

请参见**如何调用API**。

URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/actions/{action_id}

表 4-630 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
version_id	是	String	剧本版本ID 最小长度：**32** 最大长度：**64**
action_id	是	String	剧本动作ID 最小长度：**32** 最大长度：**64**

请求参数

表 4-631 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

响应参数

状态码： 200

表 4-632 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-633 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**1** 最大长度：**32**
message	String	响应消息 最小长度：**1** 最大长度：**32**

状态码： 400

表 4-634 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-635 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

无

响应示例

状态码： 200

请求成功响应参数

```
{
  "code" : 0,
  "message" : "Error message"
}
```

SDK 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeletePlaybookActionRequest request = new DeletePlaybookActionRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = DeletePlaybookActionRequest()
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应参数
400	请求失败响应参数

错误码

请参见**错误码**。

4.10.4 更新剧本动作

功能介绍

更新剧本动作

调用方法

请参见**如何调用API**。

URI

PUT /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{version_id}/actions/{action_id}

表 4-636 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间ID 最小长度：**32** 最大长度：**36**
version_id	是	String	剧本版本ID 最小长度：**32** 最大长度：**64**
action_id	是	String	剧本动作ID 最小长度：**32** 最大长度：**64**

请求参数

表 4-637 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**

参数	是否必选	参数类型	描述
content-type	是	String	application/json;charset=UTF-8 缺省值：**application/json;charset=UTF-8** 最小长度：**1** 最大长度：**64**

表 4-638 请求 Body 参数

参数	是否必选	参数类型	描述
name	否	String	名称 最小长度：**0** 最大长度：**1024**
description	否	String	描述 最小长度：**0** 最大长度：**1024**
action_type	否	String	类型，默认AOP_WORKFLOW. 最小长度：**0** 最大长度：**64**
action_id	否	String	剧本动作ID 最小长度：**32** 最大长度：**64**
sort_order	否	String	排序方式 最小长度：**0** 最大长度：**64**

响应参数

状态码： 200

表 4-639 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-640 响应 Body 参数

参数	参数类型	描述
code	String	Error code 最小长度：**1** 最大长度：**32**
message	String	Error message 最小长度：**1** 最大长度：**32**
data	**ActionInfo** object	剧本流程动作信息

表 4-641 ActionInfo

参数	参数类型	描述
id	String	剧本流程动作ID 最小长度：**32** 最大长度：**64**
name	String	流程动作名称 最小长度：**0** 最大长度：**1024**
description	String	描述 最小长度：**0** 最大长度：**1024**
action_type	String	流程动作类型 最小长度：**0** 最大长度：**64**
action_id	String	流程ID 最小长度：**32** 最大长度：**64**
playbook_id	String	剧本ID 最小长度：**0** 最大长度：**64**
playbook_version_id	String	剧本版本ID 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
project_id	String	项目ID 最小长度：**0** 最大长度：**64**

状态码： 400

表 4-642 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-643 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

更新一个剧本动作，剧本名称为MyXXX，描述为This my XXXX，剧本动作类型为aopworkflow，剧本动作ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，排序顺序为string。

```
{
  "name" : "MyXXX",
  "description" : "This my XXXX",
  "action_type" : "aopworkflow",
  "action_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "sort_order" : "string"
}
```

响应示例

状态码： 200

请求成功响应参数

```
{
  "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 代码示例

SDK代码示例如下。

Java

更新一个剧本动作，剧本名称为MyXXX，描述为This my XXXX，剧本动作类型为aopworkflow，剧本动作ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，排序顺序为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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdatePlaybookActionRequest request = new UpdatePlaybookActionRequest();
        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

更新一个剧本动作，剧本名称为MyXXX，描述为This my XXXX，剧本动作类型为aopworkflow，剧本动作ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，排序顺序为string。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = UpdatePlaybookActionRequest()
        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

更新一个剧本动作，剧本名称为MyXXX，描述为This my XXXX，剧本动作类型为aopworkflow，剧本动作ID为909494e3-558e-46b6-a9eb-07a8e18ca62f，排序顺序为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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdatePlaybookActionRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功响应参数
400	请求失败响应参数

错误码

请参见**错误码**。

4.11 事件关系管理

4.11.1 查询关联 Dataobject 列表

功能介绍

查询关联Dataobject列表

调用方法

请参见**如何调用API**。

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}/search

表 4-644 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**
dataclass_type	是	String	关联主体dataobject所属数据类，小写复数，如告警为alerts，事件为incidents 最小长度：**1** 最大长度：**64**
data_object_id	是	String	关联主体dataobject的id 最小长度：**32** 最大长度：**36**
related_dataclass_type	是	String	被关联的dataobject所属数据类，小写复数，如告警为alerts，事件为incidents 最小长度：**1** 最大长度：**64**

请求参数

表 4-645 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

表 4-646 请求 Body 参数

参数	是否必选	参数类型	描述
limit	否	Integer	分页大小 最小值：**0** 最大值：**1000**
offset	否	Integer	偏移量 最小值：**0** 最大值：**1000**
sort_by	否	String	排序字段：create_time | update_time 最小长度：**0** 最大长度：**1000**
order	否	String	排序方式：DESC | ASC 最小长度：**0** 最大长度：**1000** 枚举值： • **DESC** • **ASC**
from_date	否	String	搜索开始时间，例如：2023-02-20T00:00:00.000Z 最小长度：**0** 最大长度：**64**

参数	是否必选	参数类型	描述
to_date	否	String	搜索结束时间，例如：2023-02-27T23:59:59.999Z 最小长度：**0** 最大长度：**64**
condition	否	**condition** object	搜索条件表达式

表 4-647 condition

参数	是否必选	参数类型	描述
conditions	否	Array of **conditions** objects	表达式列表 数组长度：**0 - 999**
logics	否	Array of strings	表达式名称列表 最小长度：**0** 最大长度：**100** 数组长度：**0 - 999**

表 4-648 conditions

参数	是否必选	参数类型	描述
name	否	String	表达式名称 最小长度：**0** 最大长度：**64**
data	否	Array of strings	表达式内容列表 最小长度：**0** 最大长度：**100** 数组长度：**0 - 999**

响应参数

状态码： 200

表 4-649 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-650 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误信息 最小长度：**0** 最大长度：**1024**
total	Integer	告警总数 最小值：**0** 最大值：**10000**
limit	Integer	分页大小 最小值：**0** 最大值：**10000**
offset	Integer	偏移量 最小值：**0** 最大值：**10000**
success	Boolean	是否成功
data	Array of **DataObjectDetail** objects	告警列表 数组长度：**0 - 10000**

表 4-651 DataObjectDetail

参数	参数类型	描述
create_time	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	参数类型	描述
data_object	**DataObject** object	告警实体信息
dataclass_ref	**dataclass_ref** object	数据类对象
format_version	Integer	格式版本 最小值：**0** 最大值：**999**
id	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
project_id	String	当前项目的id 最小长度：**0** 最大长度：**64**
update_time	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
version	Integer	版本 最小值：**0** 最大值：**999**
workspace_id	String	当前的工作空间id 最小长度：**0** 最大长度：**36**

表 4-652 DataObject

参数	参数类型	描述
version	String	告警对象的版本，该字段的值必须为华为云SSA服务确定的官方发布版本之一 最小长度：**0** 最大长度：**64**
id	String	事件唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**

参数	参数类型	描述
domain_id	String	数据投递后，被委托用户的domain_id 最小长度：**0** 最大长度：**36**
region_id	String	数据投递后，被委托用户的region_id 最小长度：**0** 最大长度：**36**
workspace_id	String	当前的工作空间id 最小长度：**0** 最大长度：**36**
environment	**environment** object	告警产生的环境坐标信息
datasource	**datasource** object	首次上报数据源
first_observed_time	String	首次发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
last_observed_time	String	最近发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
create_time	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
arrive_time	String	接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	参数类型	描述
title	String	告警标题 最小长度：**0** 最大长度：**255**
description	String	告警描述信息 最小长度：**0** 最大长度：**1024**
source_url	String	告警URL链接，指向数据源产品中有关当前事件说明的页面 最小长度：**0** 最大长度：**1024**
count	Integer	事件发生次数 最小值：**0** 最大值：**999**
confidence	Integer	事件的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100，0表示置信度为0%，100表示置信度为100% 最小值：**0** 最大值：**100**
severity	String	严重性等级，取值范围：Tips | Low | Medium | High | Fatal 说明： 0: Tips – 未发现任何问题。 1: Low – 无需针对问题执行任何操作。 2: Medium – 问题需要处理，但不紧急。 3: High – 问题必须优先处理。 4: Fatal – 问题必须立即处理，以防止产生进一步的损害 最小长度：**3** 最大长度：**6** 枚举值： • **Tips** • **Low** • **Medium** • **High** • **Fatal**
criticality	Integer	关键性，是指事件涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源 最小值：**0** 最大值：**100**
alert_type	**alert_type** object	告警分类，详细定义参考《 告警类型定义 》

参数	参数类型	描述
network_list	Array of **network_list** objects	网络信息 数组长度：**0 - 999**
resource_list	Array of **resource_list** objects	受影响资源 数组长度：**0 - 999**
remediation	**remediation** object	补救措施
verification_state	String	验证状态，标识事件的准确性。可选类型如下：Unknown – 未知 True_Positive – 确认 False_Positive – 误报 默认填写Unknown 最小长度：**32** 最大长度：**64** 枚举值： • **Unknown** • **True_Positive** • **False_Positive**
handle_status	String	事件处理状态，可选类型如下： Open – 打开，默认 Block – 阻塞 Closed – 关闭 默认填写Open 最小长度：**4** 最大长度：**5** 枚举值： • **Open** • **Block** • **Closed**
sla	Integer	约束闭环时间：设置风险接受持续时间。单位：小时 最小值：**0** 最大值：**999**
update_time	String	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

参数	参数类型	描述
close_time	String	关闭时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
ipdrr_phase	String	周期/处置阶段编号 Prepartion|Detection and Analysis|Containm，Eradication& Recovery|Post-Incident-Activity 最小长度：**0** 最大长度：**64** 枚举值： • **Prepartion** • **Detection and Analysis** • **Containm，Eradication& Recovery** • **Post-Incident-Activity**
simulation	String	调试字段 最小长度：**0** 最大长度：**64**
actor	String	告警调查员 最小长度：**0** 最大长度：**64**
owner	String	责任人、服务责任人 最小长度：**0** 最大长度：**64**
creator	String	创建人 最小长度：**0** 最大长度：**64**
close_reason	String	关闭原因: 误检 - False detection 已解决 - Resolved 重复 - Repeated 其他 - Other 最小长度：**0** 最大长度：**64** 枚举值： • **False detection** • **Resolved** • **Repeated** • **Other**

参数	参数类型	描述
close_comment	String	关闭评论 最小长度：**0** 最大长度：**1024**
malware	**malware** object	恶意软件
system_info	Object	系统信息
process	Array of **process** objects	进程信息 数组长度：**0 - 999**
user_info	Array of **user_info** objects	用户信息 数组长度：**0 - 999**
file_info	Array of **file_info** objects	文件信息 数组长度：**0 - 999**

表 4-653 environment

参数	参数类型	描述
vendor_type	String	环境供应商：HWCP/HWC/AWS/Azure/GCP 最小长度：**0** 最大长度：**64**
domain_id	String	租户id 最小长度：**0** 最大长度：**64**
region_id	String	区域od，全局服务global 最小长度：**0** 最大长度：**64**
cross_workspace_id	String	数据投递前的源工作空间id，在源空间下值为null，投递后为被委托用户的id 最小长度：**0** 最大长度：**64**
project_id	String	项目id， 全局服务默认null 最小长度：**0** 最大长度：**64**

表 4-654 datasource

参数	参数类型	描述
source_type	Integer	数据源类型，取值范围如下： 1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**1** 最大值：**3** 枚举值： • **1** • **2** • **3**
domain_id	String	数据源产品所属账号的id 最小长度：**0** 最大长度：**36**
project_id	String	数据源产品所属项目的id 最小长度：**0** 最大长度：**64**
region_id	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义，例如cn-north-1 最小长度：**0** 最大长度：**64**
company_name	String	数据源产品所属公司的名称 最小长度：**0** 最大长度：**16**
product_name	String	数据源产品的名称 最小长度：**0** 最大长度：**24**
product_feature	String	产品功能特性名称，用来指明检测到当前事件的产品的功能特性 最小长度：**0** 最大长度：**24**
product_module	String	检测模块列表 最小长度：**0** 最大长度：**1024**

表 4-655 alert_type

参数	参数类型	描述
category	String	类别 最小长度：**0** 最大长度：**1024**
alert_type	String	告警类型 最小长度：**0** 最大长度：**1024**

表 4-656 network_list

参数	参数类型	描述
direction	String	方向，取值范围：IN | OUT 最小长度：**0** 最大长度：**3** 枚举值： • **IN** • **OUT**
protocol	String	协议，包含7层和4层的协议 参考：IANA registered name https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml 最小长度：**0** 最大长度：**64**
src_ip	String	源IP地址 最小长度：**0** 最大长度：**64**
src_port	Integer	源端口，0–65535 最小值：**0** 最大值：**65535**
src_domain	String	源域名 最小长度：**0** 最大长度：**128**
src_geo	**src_geo** object	源IP的地理位置信息

参数	参数类型	描述
dest_ip	String	目的IP地址 最小长度：**32** 最大长度：**64**
dest_port	String	目的端口，0–65535 最小长度：**0** 最大长度：**65535**
dest_domain	String	目的域名 最小长度：**0** 最大长度：**128**
dest_geo	**dest_geo** object	目标IP的地理位置信息

表 4-657 src_geo

参数	参数类型	描述
latitude	Number	纬度 最小值：**0** 最大值：**90**
longitude	Number	经度 最小值：**0** 最大值：**180**
city_code	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-658 dest_geo

参数	参数类型	描述
latitude	Number	纬度 最小值：**0** 最大值：**90**

参数	参数类型	描述
longitude	Number	经度 最小值：**0** 最大值：**180**
city_code	String	城市编码，Beijing | Shanghai 最小长度：**0** 最大长度：**64**
country_code	String	国家简码，参考ISO 3166-1 alpha-2，例如：CN | US | DE | IT | SG 最小长度：**0** 最大长度：**64**

表 4-659 resource_list

参数	参数类型	描述
id	String	云服务资源id 最小长度：**0** 最大长度：**36**
name	String	资源名称 最小长度：**0** 最大长度：**255**
type	String	资源类型；引用华为云RMS type字段 最小长度：**0** 最大长度：**64**
provider	String	云服务名称；引用华为云RMS provider字段 最小长度：**0** 最大长度：**64**
region_id	String	区域；按照华为云regionId填写，如cn-north-1等 最小长度：**0** 最大长度：**36**
domain_id	String	资源所属账号ID，UUID格式 最小长度：**0** 最大长度：**36**
project_id	String	资源所属项目ID，UUID格式 最小长度：**0** 最大长度：**36**

参数	参数类型	描述
ep_id	String	企业项目id 最小长度：**0** 最大长度：**128**
ep_name	String	企业项目名称 最小长度：**0** 最大长度：**128**
tags	String	资源标签 1、最多50个key/values对 2、values：最大255字符，取值范围：字母数字,空格,+, -, =, ., _, :, /,@ 最小长度：**0** 最大长度：**2048**

表 4-660 remediation

参数	参数类型	描述
recommendation	String	推荐处理方法 最小长度：**0** 最大长度：**128**
url	String	链接，指向该事件的一般修复信息。该URL必须可以从公网访问，不需要提供凭证 最小长度：**0** 最大长度：**2048**

表 4-661 malware

参数	参数类型	描述
malware_family	String	恶意家族 最小长度：**0** 最大长度：**64**
malware_class	String	恶意软件分类 最小长度：**0** 最大长度：**64**

表 4-662 process

参数	参数类型	描述
process_name	String	进程名 最小长度：**0** 最大长度：**64**
process_path	String	进程执行文件路径 最小长度：**0** 最大长度：**512**
process_pid	Integer	进程id 最小值：**0** 最大值：**65535**
process_uid	Integer	进程用户id 最小值：**0** 最大值：**655350**
process_cmdline	String	进程命令行 最小长度：**0** 最大长度：**128**
process_parent_name	String	父进程名称 最小长度：**0** 最大长度：**64**
process_parent_path	String	父进程执行文件路径 最小长度：**0** 最大长度：**512**
process_parent_pid	Integer	父进程id 最小值：**0** 最大值：**65535**
process_parent_uid	Integer	父进程用户id 最小值：**0** 最大值：**655350**
process_parent_cmdline	String	父进程命令行 最小长度：**0** 最大长度：**128**
process_child_name	String	子进程名称 最小长度：**0** 最大长度：**64**

参数	参数类型	描述
process_child_path	String	子进程执行文件路径 最小长度：**0** 最大长度：**512**
process_child_pid	Integer	子进程id 最小值：**0** 最大值：**65535**
process_child_uid	Integer	子进程用户id 最小值：**0** 最大值：**655350**
process_child_cmdline	String	子进程命令行 最小长度：**0** 最大长度：**128**
process_launche_time	String	进程启动时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**
process_terminate_time	String	进程结束时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区 最小长度：**0** 最大长度：**30**

表 4-663 user_info

参数	参数类型	描述
user_id	String	用户uid 最小长度：**0** 最大长度：**36**
user_name	String	用户名称 最小长度：**32** 最大长度：**64**

表 4-664 file_info

参数	参数类型	描述
file_path	String	文件路径/名称 最小长度：**0** 最大长度：**128**
file_content	String	文件内容 最小长度：**0** 最大长度：**1024**
file_new_path	String	文件新路径/名称 最小长度：**32** 最大长度：**64**
file_hash	String	文件hash 最小长度：**0** 最大长度：**128**
file_md5	String	文件md5 最小长度：**0** 最大长度：**128**
file_sha256	String	文件sha256 最小长度：**0** 最大长度：**128**
file_attr	String	文件属性 最小长度：**0** 最大长度：**1024**

表 4-665 dataclass_ref

参数	参数类型	描述
id	String	数据类唯一标识，UUID格式，最大36个字符 最小长度：**0** 最大长度：**36**
name	String	数据类名称 最小长度：**0** 最大长度：**36**

状态码： 400

表 4-666 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-667 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

查询数据对象的关系列表，偏移量为10，查询3条

```
{
  "limit" : 3,
  "offset" : 10
}
```

响应示例

状态码： 200

查询关联Dataobject列表返回body体

```
{
  "code" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "message" : "Error message",
  "total" : 41,
  "limit" : 3,
  "offset" : 10,
  "data" : null
}
```

SDK 代码示例

SDK代码示例如下。

Java

查询数据对象的关系列表，偏移量为10，查询3条

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListDataobjectRelationsRequest request = new ListDataobjectRelationsRequest();
        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

查询数据对象的关系列表，偏移量为10，查询3条

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")
```

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

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

    try:
        request = ListDataobjectRelationsRequest()
        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

查询数据对象的关系列表，偏移量为10，查询3条

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListDataobjectRelationsRequest{}
    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)
```

```
  }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	查询关联Dataobject列表返回body体
400	查询关联Dataobject列表错误返回body体

错误码

请参见**错误码**。

4.11.2 关联 Dataobject

功能介绍

关联Dataobject

调用方法

请参见**如何调用API**。

URI

POST /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}

表 4-668 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**

参数	是否必选	参数类型	描述
dataclass_type	是	String	关联主体dataobject所属数据类，小写复数，如告警为alerts，事件为incidents 最小长度：**1** 最大长度：**64**
data_object_id	是	String	关联主体dataobject的id 最小长度：**32** 最大长度：**36**
related_dataclass_type	是	String	被关联的dataobject所属数据类，小写复数，如告警为alerts，事件为incidents 最小长度：**1** 最大长度：**64**

请求参数

表 4-669 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

表 4-670 请求 Body 参数

参数	是否必选	参数类型	描述
ids	否	Array of strings	关联dataobject的ID列表 最小长度：**32** 最大长度：**64** 数组长度：**0 - 100**

响应参数

状态码： 200

表 4-671 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-672 响应 Body 参数

参数	参数类型	描述
code	String	Id value 最小长度：**0** 最大长度：**64**
message	String	Error message 最小长度：**0** 最大长度：**32**
request_id	String	Error message 最小长度：**0** 最大长度：**32**
success	Boolean	Error message 最小长度：**1** 最大长度：**32**
total	Integer	tatal count 最小值：**0** 最大值：**99999**
limit	Integer	current page count 最小值：**0** 最大值：**9999**
offset	Integer	current page size 最小值：**0** 最大值：**100**
data	**DataResponse** object	indicator batch operation response

表 4-673 DataResponse

参数	参数类型	描述
success_ids	Array of strings	id list 最小长度：**32** 最大长度：**64** 数组长度：**0 - 999**
error_ids	Array of strings	id list 最小长度：**32** 最大长度：**64** 数组长度：**0 - 999**

状态码： 400

表 4-674 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-675 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

创建一条ID为f60bf0e7-73b8-4832-8fc4-8c2a12830552的事件关系。

```
{
  "ids" : [ "f60bf0e7-73b8-4832-8fc4-8c2a12830552" ]
}
```

响应示例

状态码： 200

关联Dataobject返回body体

```
{
  "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 代码示例

SDK代码示例如下。

Java

创建一条ID为f60bf0e7-73b8-4832-8fc4-8c2a12830552的事件关系。

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateDataobjectRelationsRequest request = new CreateDataobjectRelationsRequest();
        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

创建一条ID为f60bf0e7-73b8-4832-8fc4-8c2a12830552的事件关系。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = CreateDataobjectRelationsRequest()
        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

创建一条ID为f60bf0e7-73b8-4832-8fc4-8c2a12830552的事件关系。

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateDataobjectRelationsRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	关联Dataobject返回body体
400	关联Dataobject错误返回body体

错误码

请参见**错误码**。

4.11.3 取消关联 Dataobject

功能介绍

取消关联Dataobject

调用方法

请参见**如何调用API**。

URI

DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}

表 4-676 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**
dataclass_type	是	String	关联主体dataobject所属数据类，小写复数，如告警为alerts，事件为incidents 最小长度：**1** 最大长度：**64**
data_object_id	是	String	关联主体dataobject的id 最小长度：**32** 最大长度：**36**
related_dataclass_type	是	String	被关联的dataobject所属数据类，小写复数，如告警为alerts，事件为incidents 最小长度：**1** 最大长度：**64**

请求参数

表 4-677 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

表 4-678 请求 Body 参数

参数	是否必选	参数类型	描述
ids	否	Array of strings	关联dataobject的ID列表 最小长度：**32** 最大长度：**64** 数组长度：**0 - 100**

响应参数

状态码： 200

表 4-679 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-680 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误信息 最小长度：**0** 最大长度：**1024**
data	**BatchOperateDataobjectResult** object	批量操作告警返回对象

表 4-681 BatchOperateDataobjectResult

参数	参数类型	描述
error_ids	Array of strings	失败id 最小长度：**0** 最大长度：**100** 数组长度：**0 - 100**
success_ids	Array of strings	成功id 最小长度：**0** 最大长度：**100** 数组长度：**0 - 100**

状态码： 400

表 4-682 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-683 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

删除一条ID为f60bf0e7-73b8-4832-8fc4-8c2a12830552的事件关系。

```
{
  "ids" : [ "f60bf0e7-73b8-4832-8fc4-8c2a12830552" ]
}
```

响应示例

状态码： 200

取消关联Dataobject返回body体

```
{
  "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 代码示例

SDK代码示例如下。

Java

删除一条ID为f60bf0e7-73b8-4832-8fc4-8c2a12830552的事件关系。

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteDataobjectRelationsRequest request = new DeleteDataobjectRelationsRequest();
        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

删除一条ID为f60bf0e7-73b8-4832-8fc4-8c2a12830552的事件关系。

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = SecMasterClient.new_builder() \
        .with_credentials(credentials) \
```

```
        .with_region(SecMasterRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteDataobjectRelationsRequest()
        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

删除一条ID为f60bf0e7-73b8-4832-8fc4-8c2a12830552的事件关系。

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteDataobjectRelationsRequest{}
    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)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	取消关联Dataobject返回body体
400	取消关联Dataobject错误返回body体

错误码

请参见**错误码**。

4.12 数据类管理

4.12.1 查询数据类列表

功能介绍

查询数据类列表

调用方法

请参见**如何调用API**。

URI

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

表 4-684 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**

表 4-685 Query 参数

参数	是否必选	参数类型	描述
offset	否	Number	偏移量 最小值：**0** 最大值：**999999999** 缺省值：**0**
limit	否	Number	数据量 最小值：**1** 最大值：**100** 缺省值：**10**
name	否	String	名称查询 最小长度：**0** 最大长度：**64**
business_code	否	String	业务编码 最小长度：**0** 最大长度：**64**
description	否	String	描述 最小长度：**0** 最大长度：**1024**
is_built_in	否	Boolean	是否内置

请求参数

表 4-686 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

响应参数

状态码： 200

表 4-687 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-688 响应 Body 参数

参数	参数类型	描述
dataclass_details	Array of **DataClassResponseBody** objects	数据类详情 数组长度：**0 - 100**
total	Number	数据总量 最小值：**2** 最大值：**999999999**

表 4-689 DataClassResponseBody

参数	参数类型	描述
id	String	数据类ID 最小长度：**32** 最大长度：**64**
create_time	String	创建时间 最小长度：**0** 最大长度：**64**
update_time	String	更新时间 最小长度：**0** 最大长度：**64**
creator_id	String	创建者ID 最小长度：**32** 最大长度：**64**
creator_name	String	创建者名称 最小长度：**32** 最大长度：**64**

参数	参数类型	描述
modifier_id	String	修改者ID 最小长度：**32** 最大长度：**64**
modifier_name	String	修改这名称 最小长度：**32** 最大长度：**64**
cloud_pack_version	String	订阅包版本 最小长度：**2** 最大长度：**64**
region_id	String	区域ID 最小长度：**0** 最大长度：**64**
project_id	String	租户ID 最小长度：**0** 最大长度：**64**
workspace_id	String	工作空间ID 最小长度：**0** 最大长度：**64**
domain_id	String	domain id 最小长度：**0** 最大长度：**64**
name	String	数据类名称 最小长度：**2** 最大长度：**64**
business_code	String	数据类业务编码 最小长度：**2** 最大长度：**64**
description	String	数据类描述 最小长度：**2** 最大长度：**1024**
is_built_in	Boolean	是否内置，true内置，false非内置
parent_id	String	父级id 最小长度：**32** 最大长度：**64**

参数	参数类型	描述
type_num	Number	子类型数量 最小值：**0** 最大值：**99999**

状态码： 400

表 4-690 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-691 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

查询数据类列表，偏移量为10，查询3条

```
{
  "limit" : 3,
  "offset" : 10
}
```

响应示例

状态码： 200

请求成功

```
{
  "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" : "张三",
```

```
  "modifier_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "modifier_name" : "李四",
  "cloud_pack_version" : "订阅包版本",
  "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" : "证据",
  "business_code" : "Evidence",
  "description" : "我的数据类描述",
  "is_built_in" : false,
  "parent_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
  "type_num" : 9
 } ]
}
```

SDK 代码示例

SDK代码示例如下。

Java

查询数据类列表，偏移量为10，查询3条

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListDataclassRequest request = new ListDataclassRequest();
        request.withOffset(<offset>);
        request.withLimit(<limit>);
        request.withName("<name>");
        request.withBusinessCode("<business_code>");
        request.withDescription("<description>");
        request.withIsBuiltIn(<is_built_in>);
        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

查询数据类列表，偏移量为10，查询3条

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListDataclassRequest()
        request.offset = <offset>
        request.limit = <limit>
        request.name = "<name>"
        request.business_code = "<business_code>"
        request.description = "<description>"
        request.is_built_in = <IsBuiltIn>
        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

查询数据类列表，偏移量为10，查询3条

```
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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListDataclassRequest{}
    offsetRequest:= float32(<offset>)
    request.Offset = &offsetRequest
    limitRequest:= float32(<limit>)
    request.Limit = &limitRequest
    nameRequest:= "<name>"
    request.Name = &nameRequest
    businessCodeRequest:= "<business_code>"
    request.BusinessCode = &businessCodeRequest
    descriptionRequest:= "<description>"
    request.Description = &descriptionRequest
    isBuiltInRequest:= <is_built_in>
    request.IsBuiltIn = &isBuiltInRequest
    response, err := client.ListDataclass(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功
400	查询数据类列表错误返回body体

错误码

请参见**错误码**。

4.12.2 查询字段列表

功能介绍

查询字段列表

调用方法

请参见**如何调用API**。

URI

GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields

表 4-692 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**
dataclass_id	是	String	数据类id 最小长度：**32** 最大长度：**36**

表 4-693 Query 参数

参数	是否必选	参数类型	描述
offset	否	Number	偏移量 最小值：**0** 最大值：**999999999** 缺省值：**0**
limit	否	Number	数据量 最小值：**1** 最大值：**100** 缺省值：**10**

参数	是否必选	参数类型	描述
name	否	String	名称查询 最小长度：**0** 最大长度：**64**
is_built_in	否	Boolean	是否内置
field_category	否	String	字段分类 最小长度：**0** 最大长度：**1024**
mapping	否	Boolean	是否展示在分类映射外的其他地方

请求参数

表 4-694 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

响应参数

状态码： 200

表 4-695 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-696 响应 Body 参数

参数	参数类型	描述
field_details	Array of **FieldResponseBody** objects	list of informations of field 数组长度：**0 - 100**
total	Number	数据总量 最小值：**2** 最大值：**999999999**

表 4-697 FieldResponseBody

参数	参数类型	描述
id	String	Id value 最小长度：**32** 最大长度：**64**
cloud_pack_version	String	订阅包版本 最小长度：**2** 最大长度：**64**
business_id	String	关联业务id 最小长度：**32** 最大长度：**64**
business_type	String	关联业务 最小长度：**2** 最大长度：**64**
dataclass_name	String	数据类名称 最小长度：**2** 最大长度：**64**
business_code	String	字段业务编码 最小长度：**2** 最大长度：**64**
field_key	String	字段key 最小长度：**2** 最大长度：**64**
name	String	字段名称 最小长度：**2** 最大长度：**64**

参数	参数类型	描述
description	String	字段描述 最小长度：**2** 最大长度：**1024**
default_value	String	默认值 最小长度：**2** 最大长度：**1024**
display_type	String	显示类型 最小长度：**2** 最大长度：**64**
field_type	String	字段类型，如shorttext,radio,grid等 最小长度：**2** 最大长度：**64**
extra_json	String	附加json 最小长度：**2** 最大长度：**64**
field_tooltip	String	工具提示 最小长度：**2** 最大长度：**64**
iu_type	String	输入输出类型 最小长度：**2** 最大长度：**64**
used_by	String	使用业务 最小长度：**2** 最大长度：**64**
json_schema	String	json模式 最小长度：**2** 最大长度：**64**
is_built_in	Boolean	是否内置，true内置，false非内置
case_sensitive	Boolean	大小写敏感，true敏感，false不敏感
read_only	Boolean	只读模式，true只读，false非只读
required	Boolean	是否必填，true必填，false非必填
searchable	Boolean	可搜索，true可搜索，false非可搜索
visible	Boolean	可见，true可见，false非可见
maintainable	Boolean	可维护，true可维护，false非可维护

参数	参数类型	描述
editable	Boolean	可编辑，true可编辑，false非可编辑
creatable	Boolean	可创建，true可创建，false非可创建
mapping	Boolean	是否展示在分类映射外的其他地方
target_api	String	目标api 最小长度：**0** 最大长度：**1024**
creator_id	String	Creator id value 最小长度：**32** 最大长度：**64**
creator_name	String	Creator name value 最小长度：**32** 最大长度：**64**
modifier_id	String	Modifier id value 最小长度：**32** 最大长度：**64**
modifier_name	String	Modifier name value 最小长度：**32** 最大长度：**64**
create_time	String	Create time 最小长度：**0** 最大长度：**64**
update_time	String	Update time 最小长度：**0** 最大长度：**64**

状态码： 400

表 4-698 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-699 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

查询字段列表，偏移量为10，查询3条

```
{
  "limit" : 3,
  "offset" : 10
}
```

响应示例

状态码： 200

请求成功

```
{
  "total" : 41,
  "field_details" : [ {
    "id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "cloud_pack_version" : "订阅包版本",
    "business_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "business_type" : "业务类型",
    "dataclass_name" : "业务id",
    "business_code" : "My Field",
    "field_key" : "字段key",
    "name" : "字段名称",
    "description" : "字段描述",
    "default_value" : "默认值",
    "display_type" : "显示类型",
    "field_type" : "shorttext",
    "extra_json" : "{}",
    "field_tooltip" : "工具提示",
    "iu_type" : "输入输出类型",
    "used_by" : "使用业务",
    "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" : "目标api",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_name" : "张三",
    "modifier_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
```

```
    "modifier_name" : "李四",
    "create_time" : "2021-01-30T23:00:00Z+0800",
    "update_time" : "2021-01-30T23:00:00Z+0800"
  } ]
}
```

SDK 代码示例

SDK代码示例如下。

Java

查询字段列表，偏移量为10，查询3条

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListDataclassFieldsRequest request = new ListDataclassFieldsRequest();
        request.withOffset(<offset>);
        request.withLimit(<limit>);
        request.withName("<name>");
        request.withIsBuiltIn(<is_built_in>);
        request.withFieldCategory("<field_category>");
        request.withMapping(<mapping>);
        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

查询字段列表，偏移量为10，查询3条

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListDataclassFieldsRequest()
        request.offset = <offset>
        request.limit = <limit>
        request.name = "<name>"
        request.is_built_in = <IsBuiltIn>
        request.field_category = "<field_category>"
        request.mapping = <Mapping>
        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

查询字段列表，偏移量为10，查询3条

```
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")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
```

```
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListDataclassFieldsRequest{}
    offsetRequest:= float32(<offset>)
    request.Offset = &offsetRequest
    limitRequest:= float32(<limit>)
    request.Limit = &limitRequest
    nameRequest:= "<name>"
    request.Name = &nameRequest
    isBuiltInRequest:= <is_built_in>
    request.IsBuiltIn = &isBuiltInRequest
    fieldCategoryRequest:= "<field_category>"
    request.FieldCategory = &fieldCategoryRequest
    mappingRequest:= <mapping>
    request.Mapping = &mappingRequest
    response, err := client.ListDataclassFields(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功
400	查询数据类列表错误返回body体

错误码

请参见**错误码**。

4.13 流程管理

4.13.1 查询流程列表

功能介绍

查询流程列表

调用方法

请参见**如何调用API**。

URI

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

表 4-700 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**

表 4-701 Query 参数

参数	是否必选	参数类型	描述
offset	否	Number	偏移量 最小值：**0** 最大值：**999999999** 缺省值：**0**
limit	否	Number	数据量 最小值：**1** 最大值：**100** 缺省值：**10**
order	否	String	排序顺序，asc：升序，desc：降序 最小长度：**0** 最大长度：**4** 枚举值： • **asc** • **desc**

参数	是否必选	参数类型	描述
sortby	否	String	排序字段，create_time：创建时间，category：类型分类名称 最小长度：**2** 最大长度：**32** 枚举值： • **category** • **create_time**
enabled	否	Boolean	是否启用
last_version	否	Boolean	最新版本号
name	否	String	流程名称 最小长度：**1** 最大长度：**64**
description	否	String	流程描述 最小长度：**1** 最大长度：**512**
dataclass_id	否	String	数据类ID 最小长度：**1** 最大长度：**64**
dataclass_name	否	String	数据类名称 最小长度：**1** 最大长度：**64**
aop_type	否	String	流程类型 最小长度：**1** 最大长度：**64**

请求参数

表 4-702 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**

参数	是否必选	参数类型	描述
content-type	是	String	内容类型 缺省值：**application/json;charset=UTF-8** 最小长度：**0** 最大长度：**64**

响应参数

状态码： 200

表 4-703 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-704 响应 Body 参数

参数	参数类型	描述
code	String	返回码 最小长度：**0** 最大长度：**1000**
total	Integer	数据总条数 最小值：**0** 最大值：**1000**
offset	Integer	当前页大小 最小值：**0** 最大值：**1000**
limit	Integer	当前页码 最小值：**0** 最大值：**1000**
message	String	请求ID 最小长度：**32** 最大长度：**36**
success	Boolean	是否成功

参数	参数类型	描述
data	Array of **AopWorkflowInfo** objects	流程信息列表 数组长度：**0 - 100**

表 4-705 AopWorkflowInfo

参数	参数类型	描述
id	String	流程ID 最小长度：**32** 最大长度：**64**
name	String	流程名称 最小长度：**0** 最大长度：**1024**
description	String	描述 最小长度：**0** 最大长度：**1024**
project_id	String	租户ID 最小长度：**32** 最大长度：**64**
owner_id	String	所有者ID 最小长度：**32** 最大长度：**64**
creator_id	String	创建者ID 最小长度：**32** 最大长度：**64**
edit_role	String	编辑角色 最小长度：**32** 最大长度：**64**
use_role	String	是用角色 最小长度：**32** 最大长度：**64**
approve_role	String	审核人 最小长度：**32** 最大长度：**64**
enabled	Boolean	是否已启用

参数	参数类型	描述
workspace_id	String	工作空间ID 最小长度：**32** 最大长度：**64**
version_id	String	流程版本ID 最小长度：**32** 最大长度：**64**
current_approval_version_id	String	当前待审核版本号 最小长度：**1** 最大长度：**64**
current_rejected_versoin_id	String	当前拒绝的版本号 最小长度：**1** 最大长度：**64**
aop_type	String	aop的类型有以下的值 NORMAL, 通用 SURVEY, 调查 HEMOSTASIS,止血 EASE;缓解 最小长度：**1** 最大长度：**64**
engine_type	String	引擎的类型分为共享版和专项版 最小长度：**1** 最大长度：**64**
dataclass_id	String	数据类的ID 最小长度：**1** 最大长度：**64**

状态码： 400

表 4-706 响应 Header 参数

参数	参数类型	描述
X-request-id	String	请求ID,格式为：request_uuid-timestamp-hostname

表 4-707 响应 Body 参数

参数	参数类型	描述
code	String	错误码 最小长度：**0** 最大长度：**64**
message	String	错误描述 最小长度：**0** 最大长度：**1024**

请求示例

查询流程列表，偏移量为10，查询3条

```
{
  "limit" : 3,
  "offset" : 10
}
```

响应示例

状态码： 200

请求成功

```
{
  "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" : "流程名称",
    "description" : "描述",
    "project_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "owner_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "creator_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f",
    "edit_role" : "编辑者",
    "use_role" : "使用者",
    "approve_role" : "审批者",
    "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;缓解",
    "engine_type" : "public_engine",
    "dataclass_id" : "909494e3-558e-46b6-a9eb-07a8e18ca62f"
  } ]
}
```

SDK 代码示例

SDK代码示例如下。

Java

查询流程列表，偏移量为10，查询3条

```
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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        ListWorkflowsRequest request = new ListWorkflowsRequest();
        request.withEnabled(<enabled>);
        request.withLastVersion(<last_version>);
        request.withName("<name>");
        request.withDescription("<description>");
        request.withDataclassId("<dataclass_id>");
        request.withDataclassName("<dataclass_name>");
        request.withAopType("<aop_type>");
        request.withOffset(<offset>);
        request.withLimit(<limit>);
        request.withOrder(ListWorkflowsRequest.OrderEnum.fromValue("<order>"));
        request.withSortby(ListWorkflowsRequest.SortbyEnum.fromValue("<sortby>"));
        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

查询流程列表，偏移量为10，查询3条

```
# coding: utf-8

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListWorkflowsRequest()
        request.enabled = <Enabled>
        request.last_version = <LastVersion>
        request.name = "<name>"
        request.description = "<description>"
        request.dataclass_id = "<dataclass_id>"
        request.dataclass_name = "<dataclass_name>"
        request.aop_type = "<aop_type>"
        request.offset = <offset>
        request.limit = <limit>
        request.order = "<order>"
        request.sortby = "<sortby>"
        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

查询流程列表，偏移量为10，查询3条

```
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")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
```



```
        WithSk(sk).
        Build()

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListWorkflowsRequest{}
    enabledRequest:= <enabled>
    request.Enabled = &enabledRequest
    lastVersionRequest:= <last_version>
    request.LastVersion = &lastVersionRequest
    nameRequest:= "<name>"
    request.Name = &nameRequest
    descriptionRequest:= "<description>"
    request.Description = &descriptionRequest
    dataclassIdRequest:= "<dataclass_id>"
    request.DataclassId = &dataclassIdRequest
    dataclassNameRequest:= "<dataclass_name>"
    request.DataclassName = &dataclassNameRequest
    aopTypeRequest:= "<aop_type>"
    request.AopType = &aopTypeRequest
    offsetRequest:= float32(<offset>)
    request.Offset = &offsetRequest
    limitRequest:= float32(<limit>)
    request.Limit = &limitRequest
    orderRequest:= model.GetListWorkflowsRequestOrderEnum().<ORDER>
    request.Order = &orderRequest
    sortbyRequest:= model.GetListWorkflowsRequestSortbyEnum().<SORTBY>
    request.Sortby = &sortbyRequest
    response, err := client.ListWorkflows(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	请求成功
400	查询数据类列表错误返回body体

错误码

请参见**错误码**。

4.14 数据空间管理

4.14.1 创建数据空间

功能介绍

创建数据空间

调用方法

请参见**如何调用API**。

URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces

表 4-708 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**

请求参数

表 4-709 请求 Body 参数

参数	是否必选	参数类型	描述
dataspace_name	是	String	数据空间名称 最小长度：**5** 最大长度：**63**
description	是	String	描述 最小长度：**1** 最大长度：**255**

响应参数

无

请求示例

```
{
  "dataspace_name" : "dataspace-01",
```

```
  "description" : "test dataspace"
}
```

响应示例

状态码： 200

```
{
  "domain_id" : "0531ed520xxxxxxebedb6e57xxxxxxxx",
  "region_id" : "cn-north-1",
  "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 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateDataspaceRequest request = new CreateDataspaceRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = CreateDataspaceRequest()
        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")
```

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
200	

错误码

请参见**错误码**。

4.15 管道管理

4.15.1 创建数据管道

功能介绍

创建数据管道

调用方法

请参见**如何调用API**。

URI

POST /v1/{project_id}/workspaces/{workspace_id}/siem/pipes

表 4-710 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目id 最小长度：**32** 最大长度：**36**
workspace_id	是	String	工作空间id 最小长度：**32** 最大长度：**36**

请求参数

表 4-711 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值） 最小长度：**0** 最大长度：**2097152**

表 4-712 请求 Body 参数

参数	是否必选	参数类型	描述
dataspace_id	是	String	工作空间ID 最小长度：**36** 最大长度：**36**
pipe_name	是	String	数据管道名称 最小长度：**5** 最大长度：**63**
description	否	String	描述 最小长度：**1** 最大长度：**255**
storage_period	是	Integer	数据的保存时间，单位为天；默认30天，取值范围为1~3600 最小值：**1** 最大值：**3600**

参数	是否必选	参数类型	描述
shards	是	Integer	数据管道分区个数；默认创建1个，最大支持创建64个分区 最小值：**1** 最大值：**64**
timestamp_field	否	String	时间戳字段 缺省值：**__time** 最小长度：**1** 最大长度：**256**
mapping	否	Map<String,KeyIndex>	索引字段映射；每个key对象承载一个字段的信息；存在多个key对象，key可变，表示字段名称；可嵌套

表 4-713 KeyIndex

参数	是否必选	参数类型	描述
type	否	String	字段类型；text 全文索引字段、keyword 结构化字段、long Long、integer Integer、double Double、float Float、date 时间字段 枚举值： • **text** • **keyword** • **long** • **integer** • **double** • **float** • **date**
is_chinese_exist	否	Boolean	是否包含中文
properties	否	Map<String,KeyIndex>	嵌套结构

响应参数

状态码： 201

表 4-714 响应 Body 参数

参数	参数类型	描述
domain_id	String	用户domainId 最小长度：**32** 最大长度：**36**
project_id	String	项目id 最小长度：**32** 最大长度：**36**
dataspace_id	String	数据空间id 最小长度：**32** 最大长度：**36**
dataspace_name	String	数据空间名称 最小长度：**32** 最大长度：**36**
pipe_id	String	管道id 最小长度：**32** 最大长度：**36**
pipe_name	String	管道名称 最小长度：**32** 最大长度：**36**
pipe_type	String	管道类型（system-defined，系统预定义)、1（user-defined，用户自定义) 最小长度：**5** 最大长度：**128**
description	String	描述信息 最小长度：**5** 最大长度：**128**
storage_period	Integer	索引存储天数 最小值：**1** 最大值：**100000**
shards	Integer	索引分片数量 最小值：**1** 最大值：**128**
create_by	String	创建者 最小长度：**5** 最大长度：**128**

参数	参数类型	描述
create_time	Integer	创建时间 最小值：**0** 最大值：**1010000000**
update_by	String	更新者 最小长度：**5** 最大长度：**128**
update_time	Integer	更新时间 最小值：**0** 最大值：**10000000000**

状态码： 400

表 4-715 响应 Body 参数

参数	参数类型	描述
error_msg	String	无效请求提示信息 最小长度：**1** 最大长度：**128**
error_code	String	错误码 最小长度：**1** 最大长度：**128**

状态码： 401

表 4-716 响应 Body 参数

参数	参数类型	描述
error_msg	String	权限错误 最小长度：**1** 最大长度：**128**
error_code	String	错误码 最小长度：**1** 最大长度：**128**

状态码： 500

表 4-717 响应 Body 参数

参数	参数类型	描述
error_msg	String	系统内部错误 最小长度：**1** 最大长度：**128**
error_code	String	错误码 最小长度：**1** 最大长度：**128**

请求示例

```
{
  "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",
      "format" : "yyyy-MM-dd HH:mm:ss"
    }
  }
}
```

响应示例

状态码： 201

创建成功返回值

```
{
  "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 代码示例

SDK代码示例如下。

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");

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

        SecMasterClient client = SecMasterClient.newBuilder()
                .withCredential(auth)
                .withRegion(SecMasterRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePipeRequest request = new CreatePipeRequest();
        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

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 = __import__('os').getenv("CLOUD_SDK_AK")
```

```
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = CreatePipeRequest()
        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")

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

    client := secmaster.NewSecMasterClient(
        secmaster.SecMasterClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

更多

更多编程语言的SDK代码示例，请参见**API Explorer**的代码示例页签，可生成自动对应的SDK代码示例。

状态码

状态码	描述
201	创建成功返回值
400	错误请求
401	认证失败
403	禁止访问
500	系统内部错误

错误码

请参见**错误码**。

4.16 V1

4.16.1 事件管理

4.16.1.1 上报安全产品数据

功能介绍

批量数据上报，每批次最多不超过50条。

此接口为继承态势感知 SA的接口。

调试

您可以在**API Explorer**中调试该接口，支持自动认证鉴权。API Explorer可以自动生成SDK代码示例，并提供SDK代码示例调试功能。

URI

POST /v2/{project_id}/events/import

表 4-718 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户项目ID。 最小长度：**32** 最大长度：**36**

请求参数

表 4-719 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
X-Language	否	String	语言。 最小长度：**2** 最大长度：**6**

表 4-720 请求 Body 参数

参数	是否必选	参数类型	描述
events	是	Array of **Event** objects	event 批量导入

表 4-721 Event

参数	是否必选	参数类型	描述
version	是	String	SA数据对象版本号，数据接入时需携带版本号。版本号由SA服务团队负责更新，数据源只可填写SA给定的版本号。目前版本为1.0.0。 最小长度：**5** 最大长度：**5**
environment	是	**Environment** object	环境坐标，DRP。
data_source	是	**DataSource** object	提供数据来源相关信息，必选对象。
first_observed_time	是	String	首次发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。

参数	是否必选	参数类型	描述
last_observed_time	否	String	最新发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。
create_time	是	String	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。
arrive_time	否	String	数据接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。 是指事件数据被SA侧接收的时间，由SA接收时填写，产品上报数据时不用填写。
event_id	是	String	事件唯一标识，UUID格式。 最小长度：**32** 最大长度：**36**
title	是	String	事件标题，最大255字符。 最小长度：**1** 最大长度：**255**
description	是	String	事件描述信息，最大1024个字符 最小长度：**1** 最大长度：**1024**
source_url	否	String	事件URL链接，指向数据源产品中有关当前事件说明的页面。 最小长度：**1** 最大长度：**4096**
count	是	Integer	事件发生次数，默认为1，必填。 最小值：**1** 最大值：**9223372036854775807**

参数	是否必选	参数类型	描述
confidence	否	Integer	事件的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100，0表示置信度为0%，100表示置信度为100%。 最小值：**0** 最大值：**100**
severity	是	**Severity** object	严重性对象。
criticality	否	Integer	关键性，是指事件涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源。 最小值：**0** 最大值：**100**
type	是	**Type** object	事件分类。
compliance	否	**Compliance** object	扩展信息，用来提供合规检查信息。合规检查相关的数据上报时，必须填充此对象。
network	否	**Network** object	扩展信息，用来提供网络信息。
vulnerability_patch	否	**Vulnerability Patch** object	扩展信息，用来提供漏洞信息。
malware	否	**Malware** object	恶意软件。
threat_intel	否	**ThreatIntel** object	威胁情报。
resource	是	**Resource** object	受影响资源。
remediation	否	**Remediation** object	补救措施。
data_source_fields	否	Object	数据源自定义信息，最多支持50个key/value对，约束条件：1、该对象不能包含冗余数据，并且不能与已定义的SSA事件格式字段冲突。 2、字段名称可以包含字母数字字符、空格和以下符号：_ . / = + \ - @。 示例："data_source_fields": { "key1": "value1", "key2", "value2", }

参数	是否必选	参数类型	描述
verification_state	否	String	事件验证状态，标识事件的准确性。 Unknown – 未知，默认 True_positive – 确认 False_positive – 误报。 最小长度：**1** 最大长度：**512**
handle_status	是	String	事件处理状态，New/Ignored/Resolved；默认New。 最小长度：**1** 最大长度：**512**
phase	否	String	阶段：Prepartion|Detection and Analysis|Containm，Eradication& Recovery| Post-Incident-Activity。 最小长度：**1** 最大长度：**32**
sla	否	Integer	约束闭环时间：单位：天。 最小值：**1** 最大值：**90**

表 4-722 Environment

参数	是否必选	参数类型	描述
type	是	String	环境供应商，HWCP/HWC/AWS/Azure/GCP等。 最小长度：**1** 最大长度：**36**
domain_id	是	String	租户账号ID，用来标识事件所属租户。 最小长度：**32** 最大长度：**36**
project_id	否	String	租户项目ID，用来标识事件所属项目区域。 最小长度：**32** 最大长度：**36**

参数	是否必选	参数类型	描述
region_id	否	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义。 最小长度：**1** 最大长度：**512**

表 4-723 DataSource

参数	是否必选	参数类型	描述
type	否	Integer	数据源类型，取值范围如下： 1 - 华为产品 2 - 第三方产品 3 - 租户私有产品 最小值：**1** 最大值：**3**
domain_id	否	String	数据源产品所属管理账号的ID，最大36个字符。 最小长度：**32** 最大长度：**36**
project_id	否	String	数据源产品所属项目的ID，最大36个字符。 最小长度：**32** 最大长度：**36**
region_id	否	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义。 最小长度：**1** 最大长度：**512**
company_name	是	String	数据源产品所属公司的名称。 最小长度：**1** 最大长度：**512**
product_name	是	String	数据源产品的名称。 最小长度：**1** 最大长度：**512**
product_feature	否	String	产品功能特性名称，用来指明检测到当前事件的产品的功能特性。 最小长度：**1** 最大长度：**512**

表 4-724 Severity

参数	是否必选	参数类型	描述
label	是	String	严重性等级取值范围：TIPS、LOW、MEDIUM、HIGH、FATAL。 TIPS：未发现任何问题。 LOW：无需针对问题执行任何操作。 MEDIUM：问题需要处理，但不紧急。 HIGH：问题必须优先处理。 FATAL：问题必须立即处理，以防止产生进一步的损害。 最小长度：**1** 最大长度：**512**
normalize_score	否	Integer	严重性评分取值范围：0-100；与严重性等级的对应关系：TIPS 0； LOW 1-39； MEDIUM 40-69； HIGH 70-89； FATAL 90-100。 最小值：**0** 最大值：**100**
original_score	否	Integer	严重性原始评分，指在数据源产品中的评分。 最小值：**0** 最大值：**9223372036854775807**

表 4-725 Type

参数	是否必选	参数类型	描述
business	是	String	事件所属业务领域标签，可选类别如下： attack – 攻击 vulnerability – 漏洞 compliance check – 合规检查 risk - 风险 public opinion - 舆情 illegal&violation - 违法违规 security bulletin - 公告 最小长度：**1** 最大长度：**512**
category	否	String	类别，推荐使用预定义的类型分类。 最小长度：**1** 最大长度：**512**

参数	是否必选	参数类型	描述
classifier	否	String	分类器，推荐使用预定义的分类器。 如果指定了分类器，则必须指定类别。 最小长度：**1** 最大长度：**512**
tech_domain	否	String	技术领域标签： OS：主机 APP：应用 NET：网络 OPS：运维 CS：云服务 CSP：平台云服务 最小长度：**1** 最大长度：**512**
properties	否	**TypeProperties** object	属性信息。

表 4-726 TypeProperties

参数	是否必选	参数类型	描述
killchain	否	String	Kill chain事件分类，仅当business为attack有效 最小长度：**1** 最大长度：**512**
ttps	否	String	Mitre Array 事件分类，仅当business为attack有效 最小长度：**1** 最大长度：**512**
effects	否	String	影响，适用全部类型 最小长度：**1** 最大长度：**512**

表 4-727 Compliance

参数	是否必选	参数类型	描述
checkitem_id	是	String	检查项（检查规则）编号 最小长度：**1** 最大长度：**512**

参数	是否必选	参数类型	描述
checkpoint_id	是	String	检查点（检查结果）编号，检查项对同一个资源的检查结果 最小长度：**1** 最大长度：**512**
spec_id	是	String	检查规范编号，默认选第一个 最小长度：**1** 最大长度：**512**
status	是	String	合规检查结果，取值定义：PASSED、WARNING、FAILED、NOT_AVAILABLE。 说明： PASSED - 接受评估的所有资源都已通过安全检查。 WARNING - 某些信息缺失或配置不支持此检查。 FAILED - 至少有一个接受评估的资源未能通过安全检查。 NOT_AVAILABLE - 由于服务中断或 API 错误，无法执行检查。 最小长度：**1** 最大长度：**512**
properties	否	String	属性信息 最小长度：**1** 最大长度：**512**

表 4-728 Network

参数	是否必选	参数类型	描述
direction	否	String	方向，取值范围：IN、OUT。 最小长度：**2** 最大长度：**3**
protocol	否	String	协议。 最小长度：**0** 最大长度：**512**
src_ip	否	String	源IP地址。 最小长度：**7** 最大长度：**15**
src_port	否	Integer	源端口，0–65535。 最小值：**0** 最大值：**65535**

参数	是否必选	参数类型	描述
src_domain	否	String	源域名，最大128个字符。 最小长度：**1** 最大长度：**128**
src_geo	否	**Geo** object	源IP的地理位置信息。
dest_ip	否	String	目标IP地址。 最小长度：**7** 最大长度：**15**
dest_port	否	Integer	目标端口，0–65535。 最小值：**0** 最大值：**65535**
dest_domain	否	String	目标域名，最大128个字符。 最小长度：**1** 最大长度：**128**
dest_geo	否	**Geo** object	目标IP的地理位置信息。

表 4-729 Geo

参数	是否必选	参数类型	描述
latitude	否	Number	纬度。 最小值：**-90.0** 最大值：**90.0**
longitude	否	Number	经度。 最小值：**-180.0** 最大值：**180.0**
city_code	否	String	城市编码。 最小长度：**1** 最大长度：**128**
country_code	否	String	国家简码ISO 3166-1 alpha-2，例如：CN、US、DE、IT、SG。 最小长度：**1** 最大长度：**128**

表 4-730 VulnerabilityPatch

参数	是否必选	参数类型	描述
patch_id	是	String	补丁编号。 最小长度：**1** 最大长度：**256**
patch_name	否	String	补丁名称。 最小长度：**1** 最大长度：**256**
type	否	String	补丁类型（0：linux，1：windows，2：web-cms）。 最小长度：**1** 最大长度：**32**
major_level	否	String	重要等级。 最小长度：**1** 最大长度：**32**
status	否	String	补丁状态。 最小长度：**1** 最大长度：**32**
repair_cmd	否	String	修复命令。 最小长度：**0** 最大长度：**512**
repair_necessity	否	String	修复必要程度（1：需立刻修复，2：可延后修复，3：暂可以不修复）。 最小长度：**0** 最大长度：**512**
release_time	否	String	发布时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息 为事件发生时区，无法解析时区的时间，默认时区填东八区。
reference_url	否	String	参考链接。 最小长度：**0** 最大长度：**512**
vendor_name	否	String	漏洞报告提供者信息。 最小长度：**1** 最大长度：**32**

参数	是否必选	参数类型	描述
vulnerable_package	否	String	受影响软件版本。 最小长度：**1** 最大长度：**32**
cve_ids	否	String	CVE编号列表。 最小长度：**1** 最大长度：**256**

表 4-731 Malware

参数	是否必选	参数类型	描述
name	是	String	恶意软件名称，最大64个字符。 最小长度：**1** 最大长度：**64**
sha256	否	String	恶意软件sha256 最小长度：**1** 最大长度：**1024**
type	是	String	恶意软件类型，遵循STIX规范：adware、backdoor、bot、bootkit、ddos、downloader、dropper、exploit-kit、keylogger、ransomware、remote-access-trojan、resource-exploitation、rogue-security-software、rootkit、screen-capture、spyware、trojan、unknown、virus、webshell、wiper、worm 最小长度：**1** 最大长度：**512**
path	否	String	恶意软件在系统中的路径，最大512个字符。 最小长度：**0** 最大长度：**512**
state	否	String	恶意软件状态，取值范围：OBSERVED、REMOVAL_FAILED、REMOVED。 最小长度：**0** 最大长度：**512**

参数	是否必选	参数类型	描述
properties	否	MalwareProperties object	属性信息。

表 4-732 MalwareProperties

参数	是否必选	参数类型	描述
pid	否	String	进程ID。 最小长度：**1** 最大长度：**64**
user	否	String	系统角色（例如:root，service）。 最小长度：**1** 最大长度：**64**
mod	否	String	系统权限（例如：777，755）。 最小长度：**1** 最大长度：**64**
start_time	否	String	进程启动时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。

表 4-733 ThreatIntel

参数	是否必选	参数类型	描述
id	是	String	情报Id。 最小长度：**0** 最大长度：**32**
indicator_type	否	String	威胁情报类型，Domain、Email_Address、Hash_MD5、Hash_SHA1、Hash_SHA256、Hash_SHA512、IPv4_Address、IPv6_Address、URL。 最小长度：**0** 最大长度：**64**

参数	是否必选	参数类型	描述
labels	否	String	标签，如'矿池','外联'等，"Directory Scan|Directory Traversal"。 最小长度：**0** 最大长度：**512**
confidence	否	Integer	置信度，不同来源目前置信度分值定义不一样（分数）。 最小值：**0** 最大值：**9223372036854775807**
information_source	是	String	威胁情报源，最大64个字符。 最小长度：**0** 最大长度：**64**
severity	否	Integer	严重程度，不同渠道定义值不一样（分数）。 最小值：**0** 最大值：**9223372036854775807**
description	是	String	威胁情报描述。 最小长度：**0** 最大长度：**4096**
modified	否	String	威胁情报的更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。
valid_from	否	String	有效期开始（可读字符串）。 最小长度：**0** 最大长度：**32**
valid_until	否	String	有效期结束（可读字符串）。 最小长度：**0** 最大长度：**32**
properties	否	**ThreatIntelProperties** object	威胁情报属性信息。

表 4-734 ThreatIntelProperties

参数	是否必选	参数类型	描述
file_md5	否	String	恶意软件Md5。 最小长度：**1** 最大长度：**64**
file_sha1	否	String	恶意软件Sha1。 最小长度：**1** 最大长度：**255**
file_sha256	否	String	恶意软件Sha256值。 最小长度：**1** 最大长度：**255**
file_name	否	String	文件名称。 最小长度：**1** 最大长度：**255**
create_time	否	String	编译时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。
file_class	否	String	文件类别，TEXT|XCODE。 最小长度：**1** 最大长度：**255**
file_family	否	String	家族，例如：wannacry（勒索软件）。 最小长度：**1** 最大长度：**255**
file_maltype	否	String	类别，例如：trojan（特洛伊）。 最小长度：**1** 最大长度：**255**
ip_resolves_to_refs	否	String	mac地址。 最小长度：**1** 最大长度：**255**
belongs_to_refs	否	String	IP AS 自治系统。 最小长度：**1** 最大长度：**255**

参数	是否必选	参数类型	描述
ip_location	否	String	地区 格式：country/provice/city/lngwgs/latwgs。 最小长度：**1** 最大长度：**255**
domain_family	否	String	例如：banjori|iodine。 最小长度：**1** 最大长度：**255**
domain_resolves_to_refs	否	String	解析的IP地址。 最小长度：**1** 最大长度：**255**
domain_dns_type	否	String	DNS类别。A|NS|CNAME|TXT。 最小长度：**1** 最大长度：**255**
url_host	否	String	例：3ms.huawei.com。 最小长度：**1** 最大长度：**255**
url_resolves_to_refs	否	String	IP地址。 最小长度：**1** 最大长度：**255**
display_name	否	String	显示名称。 最小长度：**1** 最大长度：**128**
url_belongs_to_ref	否	String	邮箱账户，@之前部分。 最小长度：**1** 最大长度：**128**

表 4-735 Resource

参数	是否必选	参数类型	描述
id	是	String	资源ID。 最小长度：**32** 最大长度：**36**
name	是	String	资源名称；最大长度255个字符。 最小长度：**1** 最大长度：**255**

参数	是否必选	参数类型	描述
type	是	String	资源类型。 最小长度：**1** 最大长度：**128**
provider	是	String	云服务名称。 最小长度：**1** 最大长度：**128**
region_id	否	String	区域。 最小长度：**1** 最大长度：**128**
domain_id	是	String	资源所属租户账号ID。 最小长度：**32** 最大长度：**36**
project_id	否	String	资源所属项目ID。 最小长度：**32** 最大长度：**36**
ep_id	否	String	企业项目ID。 最小长度：**32** 最大长度：**36**
ep_name	否	String	企业项目名称。 最小长度：**32** 最大长度：**36**
tags	否	Object	资源标签 1、最多50个key/values对。 2、values：最大255字符。 3、取值范围：字母数字、空格、“+”、“-”、“=”、“.”、“_”、“:”、“/”、“@”。

表 4-736 Remediation

参数	是否必选	参数类型	描述
recommendation	是	String	处理建议，最长512个字符。 最小长度：**1** 最大长度：**512**

参数	是否必选	参数类型	描述
url	否	String	链接，指向该事件的一般修复信息。该URL必须可以从公网访问，不需要提供凭证。 最小长度：**1** 最大长度：**128**

响应参数

状态码： 400

表 4-737 响应 Body 参数

参数	参数类型	描述
error_msg	String	无效请求提示信息 最小长度：**1** 最大长度：**128**
error_code	String	错误码 最小长度：**1** 最大长度：**128**

状态码： 401

表 4-738 响应 Body 参数

参数	参数类型	描述
error_msg	String	权限错误 最小长度：**1** 最大长度：**128**
error_code	String	错误码 最小长度：**1** 最大长度：**128**

状态码： 500

表 4-739 响应 Body 参数

参数	参数类型	描述
error_msg	String	系统内部错误 最小长度：**1** 最大长度：**128**
error_code	String	错误码 最小长度：**1** 最大长度：**128**

请求示例

```
POST https://{endpoint}/v2/{project_id}/events/import

{
  "events" : [ {
    "version" : "1.1.0",
    "environment" : {
      "type" : "xxx",
      "domain_id" : "dfaf9864b95c448797b5dc0f0xxxxxxx",
      "project_id" : "2b31ed520xxxxxxebedb6e57xxxxxxxx",
      "region_id" : "xx-xx-1"
    },
    "data_source" : {
      "type" : 1,
      "domain_id" : "dfaf9864b95c448797b5dc0f0xxxxxxx",
      "project_id" : "2b31ed520xxxxxxebedb6e57xxxxxxxx",
      "region_id" : "xx-xx-1",
      "company_name" : "xxx",
      "product_name" : "xxx",
      "product_feature" : "xxx"
    },
    "first_observed_time" : "2020-10-10T13:10:40.436+0800",
    "last_observed_time" : "2020-10-10T13:10:40.436+0800",
    "create_time" : "2020-10-10T13:10:40.436+0800",
    "arrive_time" : "2020-10-21T01:20:31.343+0800",
    "event_id" : "1683fbf6-01fd-49f4-8222-0fe33d3f2d2e",
    "title" : "TCP Malformed",
    "description" : "TCP Malformed",
    "count" : 1,
    "severity" : {
      "original_score" : 1,
      "label" : "TIPS"
    },
    "type" : [ {
      "business" : "attack",
      "category" : "Brute Force",
      "classifier" : "ssh"
    } ],
    "network" : {
      "direction" : "IN",
      "dest_ip" : "xxx.xxx.xxx.xxx",
      "dest_port" : 80,
      "dest_geo" : {
        "latitude" : 1.352083,
        "longitude" : 103.81984
      }
    },
    "resource" : [ {
      "id" : "f1f4076a-9d12-497f-aac4-a9dcb5462fcc",
      "name" : "ecs-s3_large_2_win-20200828214727",
```

```
    "type" : "cloudservers",
    "provider" : "ecs",
    "region_id" : "xx-xx-1",
    "domain_id" : "dfaf9864b95c448797b5dc0f00709a55",
    "project_id" : "2b31ed520xxxxxxebedb6e57xxxxxxxx",
    "ep_id" : "7e998f85-xxxx-xxxx-xxxx-xxxxxxxx",
    "ep_name" : "test001"
   } ],
   "verification_state" : "Unknown",
   "handle_status" : "New"
 } ]
}
```

响应示例

无

状态码

状态码	描述
201	Succeeded
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

错误码

请参见**错误码**。

4.16.2 产品管理

4.16.2.1 检查心跳健康

功能介绍

SA提供心跳接口，集成产品定时（每五分钟）发送心跳报文到态势感知，用来确认集成产品与态势感知之间的通路是否健康。

此接口为继承态势感知 SA的接口。

调试

您可以在**API Explorer**中调试该接口，支持自动认证鉴权。API Explorer可以自动生成SDK代码示例，并提供SDK代码示例调试功能。

URI

POST /v1/{project_id}/products/health-check

表 4-740 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户项目ID。 最小长度：**32** 最大长度：**36**

请求参数

表 4-741 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token。 通过调用IAM服务获取用户Token接口获取（响应消息头中X-Subject-Token的值）。 最小长度：**1** 最大长度：**2097152**
X-Language	否	String	语言 最小长度：**2** 最大长度：**6**

表 4-742 请求 Body 参数

参数	是否必选	参数类型	描述
domain_id	是	String	数据源产品所属账号的ID。 最小长度：**32** 最大长度：**36**
project_id	是	String	数据源产品所属项目的ID。 最小长度：**32** 最大长度：**36**
region	是	String	数据源产品所在区域。 最小长度：**1** 最大长度：**512**
company_name	是	String	数据源产品所属公司的名称。 最小长度：**1** 最大长度：**512**

参数	是否必选	参数类型	描述
product_name	是	String	数据源产品的名称。 最小长度：**1** 最大长度：**512**

响应参数

状态码： 400

表 4-743 响应 Body 参数

参数	参数类型	描述
error_msg	String	无效数据的描述信息。 最小长度：**1** 最大长度：**128**
error_code	String	错误码。 最小长度：**1** 最大长度：**128**

状态码： 401

表 4-744 响应 Body 参数

参数	参数类型	描述
error_msg	String	token认证错误。 最小长度：**1** 最大长度：**128**
error_code	String	错误码。 最小长度：**1** 最大长度：**128**

状态码： 403

表 4-745 响应 Body 参数

参数	参数类型	描述
error_msg	String	权限错误。 最小长度：**1** 最大长度：**128**
error_code	String	错误码。 最小长度：**1** 最大长度：**128**

状态码： 500

表 4-746 响应 Body 参数

参数	参数类型	描述
error_msg	String	系统内部错误。 最小长度：**1** 最大长度：**128**
error_code	String	错误码。 最小长度：**1** 最大长度：**128**

请求示例

```
POST https://{endpoint}/v1/{project_id}/products/health-check

{
  domain_id: "dfaf9864b95c448797b5dc0f0xxxxxxx",
  project_id: "2b31ed520xxxxxxebedb6e57xxxxxxxx",
  region: "xx-xx-1",
  company_name: "xxx",
  product_name: "xxx"
}
```

响应示例

无

状态码

状态码	描述
201	Succeeded
400	Bad Request

状态码	描述
401	Unauthorized
403	Forbidden
500	Internal Server Error

错误码

请参见**错误码**。

A 附录

A.1 状态码

- 正常

返回值	说明
201	成功。

- 异常

状态码	编码	说明
400	Bad Request	参数错误。
401	Unauthorized	认证失败。
403	Forbidden	拒绝访问。
500	Internal Server Error	系统内部错误。

A.2 错误码

当您调用API时，如果遇到“APIGW”开头的错误码，请参见**API网关错误码**进行处理。

状态码	错误码	错误信息	描述	处理措施
400	sa.00000001	Bad Request	参数错误	请检查请求参数
400	sa.00100004	Forbidden	不存在产品信息	检查产品信息
400	SecMaster.11061001	进程状态有误	--	--

状态码	错误码	错误信息	描述	处理措施
400	SecMaster.11061002	模型数量超出范围限制	--	--
400	SecMaster.11061003	schedule参数超出范围	--	--
400	SecMaster.11061004	告警名称已存在	--	--
400	SecMaster.20010001	无效的工作空间ID	--	--
400	SecMaster.20030001	无效的参数	--	--
400	SecMaster.20030002	无效的项目ID	--	--
400	SecMaster.20030003	无效的名称	--	--
400	SecMaster.20030004	创建数据对象失败	--	--
400	SecMaster.20030005	获取数据对象失败	--	--
400	SecMaster.20030009	无效的排序字段	--	--
400	SecMaster.20030010	无效的排序	--	--
400	SecMaster.20030011	更新数据对象错误	--	--
400	SecMaster.20030012	删除数据对象错误	--	--
400	SecMaster.20030013	搜索数据对象错误	--	--
400	SecMaster.20030022	查询特定数据类失败	--	--
400	SecMaster.20030025	验证数据对象失败	--	--
400	SecMaster.20039999	未知错误	--	--
400	SecMaster.20040000	未知错误	--	--
400	SecMaster.20040402	查询数据类失败	--	--

状态码	错误码	错误信息	描述	处理措施
400	SecMaster.20040516	字段超过最大限制	--	--
400	SecMaster.20041001	无效的工作空间ID	--	--
400	SecMaster.20041002	无效的参数	--	--
400	SecMaster.20041003	无效的项目ID	--	--
400	SecMaster.20041031	获取数据对象失败	--	--
400	SecMaster.20041033	未选择关联数据对象	--	--
400	SecMaster.20041504	创建事件失败	--	--
400	SecMaster.20041507	更新事件失败	--	--
400	SecMaster.20041508	删除事件失败	--	--
400	SecMaster.20041509	单日事件创建个数超过最大限制	--	--
400	SecMaster.20041804	告警转事件请求内容错误	--	--
400	SecMaster.20041805	创建告警失败	--	--
400	SecMaster.20041808	更新告警失败	--	--
400	SecMaster.20041809	删除告警失败	--	--
400	SecMaster.20041810	单日告警创建个数超过最大限制	--	--
400	SecMaster.20041811	单日告警转事件个数超过最大限制	--	--
400	SecMaster.20041903	获取数据类失败	--	--
400	SecMaster.20041904	威胁情报数据不存在	--	--

状态码	错误码	错误信息	描述	处理措施
400	SecMaster.20041905	创建威胁情报失败	--	--
400	SecMaster.20041906	更新威胁情报失败	--	--
400	SecMaster.20041907	删除威胁情报失败	--	--
400	SecMaster.20042501	单日指标创建个数超过最大限制	--	--
400	SecMaster.20048001	剧本存在正在运行的实例或存在激活版本不能删除	--	--
400	SecMaster.20048002	剧本不存在激活版本，不能启用	--	--
400	SecMaster.20048003	剧本状态错误，不能审核	--	--
400	SecMaster.20048004	资源不存在	--	--
400	SecMaster.20048005	剧本审核不通过，不能激活	--	--
400	SecMaster.20048006	剧本ID错误	--	--
400	SecMaster.20048007	剧本版本ID错误	--	--
400	SecMaster.20048008	剧本动作ID错误	--	--
400	SecMaster.20048009	剧本规则ID错误	--	--
400	SecMaster.20048013	剧本启用中，不能失活版本	--	--
400	SecMaster.20048014	剧本已经发布，不能编辑	--	--
400	SecMaster.20048015	剧本名称重复	--	--
400	SecMaster.20048016	剧本定时任务时间范围错误	--	--

状态码	错误码	错误信息	描述	处理措施
400	SecMaster.20048017	剧本定时任务Corn表达式错误	--	--
400	SecMaster.20048018	版本数量已达到上线	--	--
400	SecMaster.20048019	剧本存在审核中版本，不能新建版本	--	--
400	SecMaster.20048020	数据对象ID错误	--	--
400	SecMaster.20048021	搜索内容无效	--	--
400	SecMaster.20048022	查询结束时间必需大于查询起始时间	--	--
400	SecMaster.20048023	注册剧本定时任务失败	--	--
400	SecMaster.20048024	禁用剧本定时任务失败	--	--
400	SecMaster.20048025	结束时间必须大于开始时间	--	--
400	SecMaster.20048026	无效的剧本结束时间	--	--
400	SecMaster.20048027	数据类ID不能为空	--	--
400	SecMaster.20048028	存在未启用的匹配流程，不能提交版本	--	--
400	SecMaster.20048029	剧本数据转换错误	--	--
400	SecMaster.20048030	剧本个数超过最大限制	--	--
400	SecMaster.20048031	剧本关联匹配流程个数超过限制	--	--
400	SecMaster.20048032	无效的剧本调度时间间隔	--	--

状态码	错误码	错误信息	描述	处理措施
400	SecMaster.20048033	剧本关联的匹配流程不能为空	--	--
400	SecMaster.20048034	匹配流程与剧本数据类不一致	--	--
400	SecMaster.20048035	系统内置剧本不允许修改	--	--
400	SecMaster.20048036	系统内置剧本不允许删除	--	--
403	sa.00000010	Forbidden	拒绝访问	开通SA权限
403	sa.00000012	Unauthorized	无效的用户TOKEN	重新申请Token
403	sa.00100001	Forbidden	接收权限不存在	检查导入权限
500	sa.00000008	Internal Server Error	系统内部错误	联系管理员

A.3 获取项目 ID

调用 API 获取项目 ID

项目ID可以通过调用**查询指定条件下的项目信息**API获取。

获取项目ID的接口为“GET https://{Endpoint}/v3/projects”，其中{Endpoint}为IAM的终端节点，可以从**地区和终端节点**获取。接口的认证鉴权请参见**认证鉴权**。

响应示例如下，其中projects下的“id”即为项目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"
    }
}
```

从控制台获取项目 ID

在调用接口的时候，部分URL中需要填入项目编号，所以需要获取到项目编号。项目编号获取步骤如下：

1. 登录管理控制台。
2. 单击用户名，在下拉列表中单击“我的凭证”。
3. 在“API凭证”页面的项目列表中查看项目ID。

图 A-1 查看项目 ID

B 修订记录

发布日期	修改说明
2024-03-20	第六次正式发布。 ● 更新部分API的接口参数描述和示例。
2024-01-31	第五次正式发布。 ● 更新部分API的接口参数描述和示例。
2023-12-11	第四次正式发布。 ● 新增API的在线调试、CLI示例、SDK代码示例等优化内容。 ● 新增数据空间、管道管理相关API说明。
2023-11-03	第三次正式发布。 ● 更新API参数信息说明。 ● 更新错误码信息。
2023-08-10	第二次正式发布。 ● 更新API参数信息说明。 ● 更新错误码信息。
2022-12-20	第一次正式发布。