

# Host Security Service

## API Reference

Edição 01  
Data 13-09-2024



**Copyright © Huawei Technologies Co., Ltd. 2024. Todos os direitos reservados.**

Nenhuma parte deste documento pode ser reproduzida ou transmitida em qualquer forma ou por qualquer meio sem consentimento prévio por escrito da Huawei Technologies Co., Ltd.

## **Marcas registadas e permissões**



HUAWEI e outras marcas registadas da Huawei são marcas registadas da Huawei Technologies Co., Ltd.

Todos as outras marcas registadas e os nomes registados mencionados neste documento são propriedade dos seus respectivos detentores.

## **Aviso**

Os produtos, serviços e funcionalidades adquiridos são estipulados pelo contrato feito entre a Huawei e o cliente. Todos ou parte dos produtos, serviços e funcionalidades descritos neste documento pode não estar dentro do âmbito de aquisição ou do âmbito de uso. Salvo especificação em contrário no contrato, todas as declarações, informações e recomendações neste documento são fornecidas "TAL COMO ESTÁ" sem garantias, ou representações de qualquer tipo, seja expressa ou implícita.

As informações contidas neste documento estão sujeitas a alterações sem aviso prévio. Foram feitos todos os esforços na preparação deste documento para assegurar a exatidão do conteúdo, mas todas as declarações, informações e recomendações contidas neste documento não constituem uma garantia de qualquer tipo, expressa ou implícita.

---

# Índice

---

<b>1 Antes de começar.....</b>	<b>1</b>
1.1 Visão geral.....	1
1.2 Chamada de API.....	1
1.3 Pontos de extremidade.....	1
1.4 Limitações e restrições.....	2
1.5 Conceitos básicos.....	2
<b>2 Chamada das APIs.....</b>	<b>4</b>
2.1 Criação de uma solicitação de API.....	4
2.2 Autenticação.....	7
2.3 Resposta.....	8
<b>3 Descrição da API.....</b>	<b>10</b>
3.1 Gerenciamento de ativos.....	10
3.1.1 Coleta de estatísticas de ativos, incluindo contas, portas e processos.....	10
3.1.2 Consulta da lista de contas.....	16
3.1.3 Consulta de estatísticas de portas abertas.....	21
3.1.4 Consulta da lista de processos.....	28
3.1.5 Consulta da lista de softwares.....	33
3.1.6 Consulta de informações sobre itens de inicialização automática.....	39
3.1.7 Consulta da lista de servidores de uma conta.....	44
3.1.8 Consulta da lista de portas abertas de um único servidor.....	52
3.1.9 Consulta da lista de servidores do software.....	58
3.1.10 Consulta da lista de serviços de itens iniciados automaticamente.....	65
3.1.11 Obtenção do histórico de alterações da conta.....	72
3.1.12 Obtenção dos registros históricos de alterações de informações de software.....	80
3.1.13 Obtenção dos registros de alterações históricas de itens iniciados automaticamente.....	87
3.1.14 Impressões digitais de ativos - Processo - Lista de servidores.....	95
3.1.15 Impressões digitais de ativos - Porta - Lista de servidores.....	102
3.1.16 Consulta da lista de middleware.....	109
3.1.17 Consulta da lista de servidores de um middleware específico.....	114
3.2 Prevenção contra ransomware.....	122
3.2.1 Consulta dos servidores protegidos contra ransomware.....	122
3.2.2 Consulta da lista de políticas de proteção contra ransomware.....	132

3.2.3	Modificação das políticas de proteção contra ransomware.....	140
3.2.4	Ativação da prevenção contra ransomware.....	147
3.2.5	Desativação da prevenção contra ransomware.....	162
3.2.6	Consulta da política de backup vinculada ao cofre de proteção do HSS.....	167
3.2.7	Modificação da política de backup vinculada ao cofre.....	175
3.3	Gerenciamento de linha de base.....	185
3.3.1	Consulta da lista de resultados de detecção de senha fraca.....	185
3.3.2	Consulta do relatório de detecção de política de complexidade de senha.....	191
3.3.3	Consulta da lista de resultados da verificação de configuração de segurança do servidor.....	198
3.3.4	Consulta do resultado da verificação de um item de configuração de segurança.....	205
3.3.5	Consulta da lista de verificação de um item de configuração de segurança.....	212
3.3.6	Consulta da lista de servidores afetados de um item de configuração de segurança.....	221
3.3.7	Consulta do relatório de um item de verificação em uma verificação de configuração de segurança.....	227
3.3.8	Ignoração, cancelamento da ignoração, reparação ou verificação dos itens de verificação de configuração com falha.....	234
3.4	Gerenciamento de cotas.....	244
3.4.1	Consulta de informações de cota.....	244
3.4.2	Consulta de detalhes da cota.....	251
3.4.3	Criação de uma cota de pedidos por HSS.....	260
3.4.4	Consulta de informações sobre produtos e ofertas.....	266
3.5	Gerenciamento de containers.....	272
3.5.1	Consulta da lista de nós de container.....	273
3.6	Gerenciamento de eventos.....	281
3.6.1	Consulta da lista de endereços IP bloqueados.....	281
3.6.2	Desbloqueio de um endereço IP bloqueado.....	287
3.6.3	Consulta da lista de arquivos isolados.....	292
3.6.4	Restauração de arquivos isolados.....	308
3.7	Detecção de intrusão.....	313
3.7.1	Manipulação de eventos de alarme.....	313
3.7.2	Consulta da lista de intrusões detectadas.....	332
3.7.3	Consulta da lista branca de alarmes.....	368
3.8	Gerenciamento de servidores.....	377
3.8.1	Consulta de ECSs.....	377
3.8.2	Alteração do status de proteção.....	393
3.8.3	Consulta de grupos de servidores.....	399
3.8.4	Criação de um grupo de servidores.....	404
3.8.5	Edição de um grupo de servidores.....	409
3.8.6	Exclusão de um grupo de servidores.....	415
3.9	Imagem do container.....	419
3.9.1	Consulta da lista de imagens no repositório de imagens do SWR.....	419
3.9.2	Verificação de imagens no repositório de imagens em lotes.....	432
3.9.3	Consulta de informações de vulnerabilidade de imagem.....	442
3.9.4	Informações de CVE correspondentes à vulnerabilidade.....	450

3.9.5 Sincronização da lista de imagens do SWR.....	455
3.9.6 Consulta da lista de resultados de detecção de configuração de segurança de imagem.....	460
3.9.7 Consulta da lista de itens de verificação de um item de configuração de segurança especificado de uma imagem .....	468
3.9.8 Consulta do relatório de verificação de configuração de espelho.....	476
3.10 Gerenciamento de políticas.....	483
3.10.1 Consulta da lista de grupos de políticas.....	483
3.10.2 Aplicação de um grupo de políticas.....	490
3.11 Gerenciamento de vulnerabilidades.....	495
3.11.1 Consulta da lista de vulnerabilidades.....	495
3.11.2 Consulta dos servidores afetados por uma vulnerabilidade.....	506
3.11.3 Alteração do status de uma vulnerabilidade.....	517
3.11.4 Consulta de informações de vulnerabilidade sobre um servidor.....	524
3.11.5 Criação de uma tarefa de verificação de vulnerabilidade.....	536
3.11.6 Consulta de uma política de verificação de vulnerabilidades.....	544
3.11.7 Modificação de uma política de verificação de vulnerabilidades.....	549
3.11.8 Consulta das tarefas de verificação de vulnerabilidades.....	555
3.11.9 Consulta da lista de servidores correspondentes a uma tarefa de verificação de vulnerabilidade.....	562
3.11.10 Consulta de estatísticas de gerenciamento de vulnerabilidades.....	568
3.12 Proteção contra adulteração da Web.....	573
3.12.1 Consulta da lista de proteção.....	573
3.12.2 Ativação ou desativação de WTP.....	581
3.12.3 Ativação ou desativação da WTP dinâmica.....	586
3.12.4 Consulta do status de WTP estática para um servidor.....	591
3.12.5 Consulta do status da WTP dinâmica para um servidor.....	599
3.13 Gerenciamento de tags.....	606
3.13.1 Criação de tags em lotes.....	606
3.13.2 Exclusão de uma tag de recurso.....	611
<b>A Apêndices.....</b>	<b>616</b>
A.1 Código de status.....	616
A.2 Códigos de erro.....	616
<b>B Histórico de alterações.....</b>	<b>617</b>

# 1 Antes de começar

## 1.1 Visão geral

O Host Security Service (HSS) ajuda você a identificar e gerenciar os ativos em seus servidores, eliminar riscos e defender-se contra invasões e adulteração de páginas da Web. Há também funções avançadas de proteção e operações de segurança disponíveis para ajudá-lo a detectar e evitar ameaças facilmente.

Este documento descreve como usar interfaces de programação de aplicações (APIs) para executar operações em HSS.

Se você planeja acessar o HSS por meio de uma API, certifique-se de que está familiarizado com os conceitos do HSS. Para obter detalhes, consulte [Visão geral de serviço](#).

## 1.2 Chamada de API

O HSS oferece suporte a APIs REST (Transferência de Estado Representacional), permitindo que você chame APIs usando HTTPS. Para obter detalhes sobre chamadas de API, consulte [Chamada das APIs](#).

## 1.3 Pontos de extremidade

Um ponto de extremidade é o **endereço de solicitação** para chamar uma API. Os pontos de extremidade variam de acordo com os serviços e as regiões.

A tabela a seguir descreve os pontos de extremidade do HSS. Selecione um desejado com base nos requisitos de serviço.

**Tabela 1-1** Pontos de extremidade do HSS

Nome	Região	Ponto de extremidade	Protocolo
CN-Hong Kong	ap-southeast-1	hss.ap-southeast-1.myhuaweicloud.com	HTTPS

Nome	Região	Ponto de extremidade	Protocolo
AP-Bangkok	ap-southeast-2	hss.ap-southeast-2.myhuaweicloud.com	HTTPS
AP-Singapore	ap-southeast-3	hss.ap-southeast-3.myhuaweicloud.com	HTTPS

## 1.4 Limitações e restrições

Uma API pode ser acessada até 600 vezes/minuto, em que um único usuário ou endereço IP pode acessar uma API até cinco vezes/minuto.

Consulte as descrições de APIs específicas.

## 1.5 Conceitos básicos

- **Conta**

Uma conta é criada após o registro bem-sucedido na plataforma de nuvem. A conta tem permissões de acesso total para todos os seus serviços e recursos em nuvem. Ela pode ser usada para redefinir senhas de usuários e conceder permissões ao usuário. A conta é uma entidade de pagamento e não deve ser usada para realizar o gerenciamento de rotina. Para fins de segurança, crie usuários do IAM e conceda a eles permissões para o gerenciamento de rotina.
- **Usuário**

Um usuário do IAM é criado usando uma conta para usar os serviços em nuvem. Cada usuário do IAM tem suas próprias credenciais de identidade (senha e chaves de acesso). O nome da conta, o nome de usuário e a senha serão necessários para a autenticação da API.
- **Região**

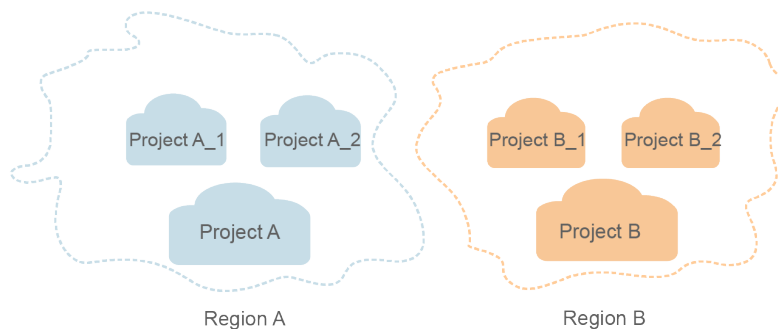
As regiões são divididas com base na localização geográfica e na latência da rede. Os serviços públicos, como Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP) e Image Management Service (IMS), são compartilhados na mesma região. As regiões são classificadas como regiões universais e regiões dedicadas. Uma região universal fornece serviços de nuvem universais para locatários comuns. Uma região dedicada fornece serviços do mesmo tipo apenas ou para locatários específicos.
- **Zona de disponibilidade (AZ)**

Uma AZ compreende um ou vários data centers físicos equipados com instalações independentes de ventilação, incêndio, água e eletricidade. Computação, rede, armazenamento e outros recursos em uma AZ são logicamente divididos em vários clusters. As AZs dentro de uma região são conectadas usando fibras ópticas de alta velocidade para suportar sistemas de alta disponibilidade entre AZs.
- **Projeto**

Um projeto corresponde a uma região. Projetos agrupam e isolam recursos (incluindo recursos de computação, armazenamento e rede) entre regiões físicas. Os usuários

podem receber permissões em um projeto padrão para acessar todos os recursos na região vinculada ao projeto. Para um controle de acesso mais refinado, crie subprojetos em um projeto e compre recursos nos subprojetos. Os usuários podem então receber permissões para acessar apenas recursos específicos nos subprojetos.

**Figura 1-1** Modelo de isolamento do projeto



- Projeto empresarial

Projetos empresariais agrupam e gerenciam recursos entre regiões. Os recursos em projetos empresariais são logicamente isolados uns dos outros. Um projeto empresarial pode conter recursos de várias regiões e os recursos podem ser adicionados ou removidos de projetos empresariais.

Para obter detalhes sobre como obter IDs e recursos de projeto empresarial, consulte [Guia de usuário do Enterprise Management](#).



# 2 Chamada das APIs

---

## 2.1 Criação de uma solicitação de API

Esta seção descreve a estrutura de uma solicitação de API REST e usa a API do IAM para **obtenção de um token de usuário** como exemplo para demonstrar como chamar uma API. O token obtido pode então ser usado para autenticar a chamada das outras API.

### URI de solicitação

Um URI de solicitação está no seguinte formato:

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

Embora um URI de solicitação esteja incluído no cabeçalho da solicitação, a maioria das linguagens de programação ou estruturas exigem que o URI de solicitação seja transmitido separadamente.

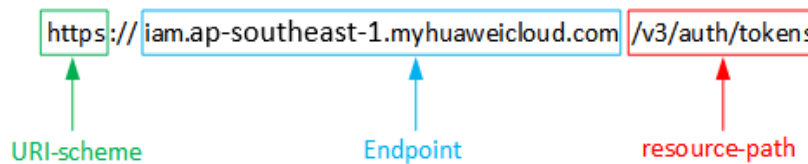
- **URI-scheme:**  
Protocolo usado para transmitir solicitações. Todas as API usam HTTPS.
- **Endpoint:**  
Nome de domínio ou endereço IP do servidor que possui o serviço REST. O endpoint varia entre serviços em diferentes regiões. Ele pode ser obtido em [Regiões e Endpoints](#).  
Por exemplo, o endpoint do IAM na região **CN-Hong Kong** é **iam.ap-southeast-1.myhuaweicloud.com**.
- **resource-path:**  
Caminho de acesso de uma API para executar uma operação especificada. Obtenha o caminho a partir do URI de uma API. Por exemplo, o **resource-path** da API usada para obter um token de usuário é **/v3/auth/tokens**.
- **query-string:**  
Parâmetro de consulta, que é opcional. Verifique se um ponto de interrogação (?) está incluído antes de cada parâmetro de consulta no formato "Nome do parâmetro = valor do parâmetro". Por exemplo, **?limit=10** indica que um máximo de 10 registros de dados serão exibidos.

Por exemplo, para obter um token IAM na região **CN-Hong Kong**, obter o endpoint do IAM (iam.ap-southeast-1.myhuaweicloud.com) para essa região e o **resource-path** (**/v3/auth/**

**tokens**) no URI da API usada para **obter um token de usuário**. Em seguida, construa o URI da seguinte forma:

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

**Figura 2-1** Exemplo de URI



#### 📖 NOTA

Para simplificar a exibição de URI neste documento, cada API é fornecida apenas com um **resource-path** e um método de solicitação. O **URI-scheme** de todas as APIs é **HTTPS**, e os endpoints de todas as APIs na mesma região são idênticos.

## Métodos de solicitação

O protocolo HTTP define os seguintes métodos de solicitação que podem ser usados para enviar uma solicitação ao servidor:

- **GET:** solicita que o servidor retorne os recursos especificados.
- **PUT:** solicita que o servidor atualize os recursos especificados.
- **POST:** solicita que o servidor adicione recursos ou execute operações especiais.
- **DELETE:** solicita que o servidor exclua recursos especificados, por exemplo, um objeto.
- **HEAD:** O mesmo que GET, exceto que o servidor deve retornar apenas o cabeçalho da resposta.
- **PATCH:** solicita ao servidor que atualize o conteúdo parcial de um recurso especificado. Se o recurso não existir, um novo recurso será criado.

Por exemplo, no caso da API usada para **obter um token de usuário**, o método de solicitação é POST. A solicitação é o seguinte:

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

## Cabeçalho da solicitação

Você também pode adicionar campos de cabeçalho adicionais a uma solicitação, como os campos exigidos por um método URI ou HTTP especificado. Por exemplo, para solicitar as informações de autenticação, adicione **Content-type**, que especifica o tipo de corpo da solicitação.

Os campos comuns de cabeçalho de solicitação são os seguintes:

- **Content-Type:** especifica o tipo ou formato do corpo da solicitação. Este campo é obrigatório e seu valor padrão é **aplicação/json**. Outros valores deste campo serão fornecidos para as APIs específicas, se houver.
- **X-Auth-Token:** especifica um token de usuário apenas para autenticação de API baseada em token. O token de usuário é uma resposta à API usada para **obter um token de usuário**. Esta API é a única que não requer autenticação.

 **NOTA**

Além de oferecer suporte à autenticação baseada em token, as API também oferecem suporte à autenticação usando ID da chave de acesso/chave de acesso secreta (AK/SK). Durante a autenticação baseada em AK/SK, um SDK é usado para assinar a solicitação, e os campos de cabeçalho **Authorization** (informações de assinatura) e **X-Sdk-Date** (hora em que a solicitação é enviada) são adicionados automaticamente à solicitação.

Para obter mais informações, consulte [Autenticação baseada em AK/SK](#).

A API usada para [obter um token de usuário](#) não requer autenticação. Portanto, apenas o campo **Content-type** precisa ser adicionado às solicitações para chamar a API. Um exemplo de tais solicitações é o seguinte:

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

## Corpo da solicitação

O corpo de uma solicitação geralmente é enviado em um formato estruturado, conforme especificado no campo de cabeçalho **Content-Type**. O corpo da solicitação transfere o conteúdo, exceto o cabeçalho da solicitação.

O corpo da solicitação varia entre as API. Algumas API não exigem o corpo da solicitação, como as API solicitadas usando os métodos GET e DELETE.

No caso da API usada para [obter um token de usuário](#), os parâmetros da solicitação e a descrição do parâmetro podem ser obtidos da solicitação da API. O seguinte fornece um exemplo de solicitação com um corpo incluído. Defina **username** para o nome de um usuário, **domainname** para o nome da conta que o usuário pertence to, **\*\*\*\*\*** para a senha de login do usuário e **xxxxxxxxxxxxxxxxxxxx** para o nome do projeto. Você pode obter mais informações sobre projetos em [Regiões e Endpoints](#). Verifique o valor da coluna **Region**.

 **NOTA**

O parâmetro **scope** especifica onde um token entra em vigor. Você pode definir **scope** para uma conta ou um projeto em uma conta. No exemplo a seguir, o token tem efeito somente para os recursos em um projeto especificado. Para obter mais informações sobre essa API, consulte [Obtenção de um token de usuário](#).

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

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

```
}  
}
```

Se todos os dados necessários para a solicitação da API estiverem disponíveis, você poderá enviar a solicitação para chamar a API por meio de [curl](#), [Postman](#) ou coding. Na resposta à API usada para obter um token de usuário, **x-subject-token** é o token de usuário desejado. Esse token pode ser usado para autenticar a chamada de outras API.

## 2.2 Autenticação

As solicitações para chamar uma API podem ser autenticadas usando um dos seguintes métodos:

- Autenticação baseada em token: As solicitações são autenticadas usando um token.
- Autenticação baseada em AK/SK: As solicitações são autenticadas criptografando o corpo da solicitação usando um par AK/SK. Este método é recomendado porque fornece uma segurança mais alta do que a autenticação baseada em token.

### Autenticação baseada em token

#### NOTA

O período de validade de um token é de 24 horas. Ao usar um token para autenticação, armazene-o em cache para impedir a chamada freqüente da API do IAM usada para obter um token de usuário.

Um token especifica permissões temporárias em um sistema de computador. Durante a autenticação da API usando um token, o token é adicionado às solicitações para obter permissões para chamar a API.

O token pode ser obtido chamando a API necessária. Para obter mais informações, consulte [Obtenção de um token de usuário](#). Um token no nível do projeto é necessário para chamar essa API, ou seja, **auth.scope** deve ser definido como **project** no corpo da solicitação.

Exemplo:

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

Depois que um token é obtido, o campo de cabeçalho **X-Auth-Token** deve ser adicionado às solicitações para especificar o token ao chamar outras API. Por exemplo, se o token é

**ABCDEFJ..., X-Auth-Token: ABCDEFJ...** pode ser adicionado a uma solicitação da seguinte forma:

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

## Autenticação baseada em AK/SK

### NOTA

A autenticação baseada em AK/SK suporta solicitações de API com um corpo não maior que 12 MB. Para solicitações de API com um corpo maior, a autenticação baseada em token é recomendada.

Na autenticação baseada em AK/SK, AK/SK é usado para assinar solicitações e a assinatura é então adicionada às solicitações de autenticação.

- AK: ID da chave de acesso, que é um identificador exclusivo usado em conjunto com uma chave de acesso secreta para assinar solicitações criptograficamente.
- SK: chave de acesso secreta usada em conjunto com uma AK para assinar solicitações criptograficamente. Ele identifica um remetente da solicitação e impede que a solicitação seja modificada.

Na autenticação baseada em AK/SK, você pode usar um AK/SK para assinar solicitações com base no algoritmo de assinatura ou usar o SDK de assinatura para assinar solicitações. Para obter detalhes sobre como assinar solicitações e usar o SDK de assinatura, consulte [Guia de assinatura da API](#).

---

### AVISO

O SDK de assinatura é usado apenas para solicitações de assinatura e é diferente dos SDK fornecidos pelos serviços.

---

## 2.3 Resposta

### Código de status

Depois de enviar uma solicitação, você receberá uma resposta, incluindo um código de status, cabeçalho de resposta e corpo de resposta.

Um código de status é um grupo de dígitos, variando de 1xx a 5xx. Indica o status de uma solicitação. Para obter mais informações, consulte [Código de status](#).

Por exemplo, se o código de status **201** for retornado para chamar a API usada para [obter um token de usuário](#), a solicitação será bem-sucedida.

### Cabeçalho de resposta

Um cabeçalho de resposta corresponde a um cabeçalho de solicitação, por exemplo, **Content-Type**.

**Figura 2-2** mostra o cabeçalho de resposta para a API de **obtenção de um token de usuário**, no qual **x-subject-token** é o token de usuário desejado. Este token pode ser usado para autenticar a chamada de outras APIs.

**Figura 2-2** Cabeçalho da resposta à solicitação para obter um token de usuário

```

connection → keep-alive

content-type → application/json

date → Tue, 12 Feb 2019 06:52:13 GMT

server → Web Server

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

transfer-encoding → chunked

via → proxy A

x-content-type-options → nosniff

x-download-options → noopen

x-frame-options → SAMEORIGIN

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

x-subject-token
→ MIIVXQVJKoZIhvcNAQcCoIIYJCCEoCAQExDTALBglghkgBZQMEAgEwgharBgkqhkiG9w0BBwGgghacBIIWmHsidG9rZW4iOansiZXhwaXJlc19hdCI6ijwMTktMDItMTNUMC
fj3KIs6YgKnpVNRbW2eZ5eb78SZ0kqJACgkIQ1wi4JlGzrpd18LGXK5tdfdq4lqHCYb8P4NaY0NYejcAgzJVeFYtLWT1GSO0zxKZmlQHqj82HBqHdgIZO9fuEbL5dMhdavj+33wEI
yHRCe9I87o+k9-
j+CMZSEB7bUGd5Uj6eRASXl1jipPEGA270g1FruooL6jqglFkNPQuFSOUB+uSsttVwRtNfsC+qTp22Rkd5MCqFGQ8LcuUjxC3a+9CMBnOintWW7oeRUVhVpXk8pxiX1wTEboX-
RzT6MUbvpvGw-oPNFYxJECKnoH3HRozv0vN--n5d6Nbxg==

x-xss-protection → 1; mode=block;

```

## (Opcional) Corpo de resposta

Um corpo de resposta geralmente é retornado em um formato estruturado, correspondendo ao **Content-Type** no cabeçalho da resposta, e é usado para transferir conteúdo diferente do cabeçalho da resposta.

Veja a seguir parte do corpo da resposta da API para **obter um token de usuário**. Para fins de espaço, apenas parte do conteúdo é exibida aqui.

```

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

```

Se ocorrer um erro durante a chamada da API, o sistema retornará um código de erro e uma mensagem para você. Veja a seguir o formato de um corpo de resposta de erro:

```

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

```

Nas informações anteriores, **error\_code** é um código de erro e **error\_msg** descreve o erro.

# 3 Descrição da API

---

## 3.1 Gerenciamento de ativos

### 3.1.1 Coleta de estatísticas de ativos, incluindo contas, portas e processos

#### Função

Essa API é usada para coletar estatísticas sobre ativos, como contas, portas e processos.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/asset/statistics

**Tabela 3-1** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-2** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>128</b>
host_id	Não	String	ID do host Mínimo: <b>1</b> Máximo: <b>128</b>
category	Não	String	Tipo. O valor padrão é host. As opções são as seguintes: <ul style="list-style-type: none"><li>● host</li><li>● container</li></ul> Mínimo: <b>1</b> Máximo: <b>64</b>

## Parâmetros de solicitação

**Tabela 3-3** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>32</b> Máximo: <b>4096</b>

## Parâmetros de resposta

**Código de status: 200**



**Tabela 3-4** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
account_num	Long	Número de contas de servidor Mínimo: <b>0</b> Máximo: <b>2147483647</b>
port_num	Long	Número de portas abertas Mínimo: <b>0</b> Máximo: <b>2147483647</b>
process_num	Long	Número de processos Mínimo: <b>0</b> Máximo: <b>2147483647</b>
app_num	Long	Pedaços de software Mínimo: <b>0</b> Máximo: <b>2147483647</b>
auto_launch_num	Long	Número de processos de inicialização automática Mínimo: <b>0</b> Máximo: <b>2147483647</b>
web_framework_num	Long	Número de estruturas da Web Mínimo: <b>0</b> Máximo: <b>2147483647</b>
web_site_num	Long	Número de sites Mínimo: <b>0</b> Máximo: <b>2147483647</b>
jar_package_num	Long	Número de pacotes JAR Mínimo: <b>0</b> Máximo: <b>2147483647</b>
kernel_module_num	Long	Número de módulos do kernel Mínimo: <b>0</b> Máximo: <b>2147483647</b>
web_service_num	Long	Número de serviços da Web Mínimo: <b>0</b> Máximo: <b>2147483647</b>
web_app_num	Long	Número de aplicações da Web Mínimo: <b>0</b> Máximo: <b>2147483647</b>

Parâmetro	Tipo	Descrição
database_num	Long	Número de bancos de dados Mínimo: <b>0</b> Máximo: <b>2147483647</b>

## Exemplo de solicitações

Essa API é usada para consultar as informações de impressão digital, contas, portas e processos de um servidor.

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

## Exemplo de respostas

**Código de status: 200**

Informações de estatísticas de ativos

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ShowAssetStatisticSolution {

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

```
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");

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

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

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ShowAssetStatisticRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.host_id = "<host_id>"
        request.category = "<category>"
        response = client.show_asset_statistic(request)
        print(response)
```

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

## Go

```
package main

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

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

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

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

    request := &model.ShowAssetStatisticRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        hostIdRequest:= "<host_id>"
        request.HostId = &hostIdRequest
        categoryRequest:= "<category>"
        request.Category = &categoryRequest
        response, err := client.ShowAssetStatistic(request)
        if err == nil {
            fmt.Printf("%+v\n", response)
        } else {
            fmt.Println(err)
        }
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Informações de estatísticas de ativos

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.1.2 Consulta da lista de contas

#### Função

Essa API é usada para consultar a lista de contas. O número de servidores pode ser consultado com base no parâmetro do nome da conta.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/asset/user/statistics

**Tabela 3-5** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-6** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
user_name	Não	String	Nome da conta. Ele deve estar em conformidade com as regras de nomenclatura de arquivos do Windows. O valor pode conter letras, dígitos, sublinhados (_) e os seguintes caracteres especiais: ! @.-. Pontuações chinesas não são permitidas. Mínimo: <b>1</b> Máximo: <b>128</b>

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>128</b>
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
category	Não	String	Tipo. O valor padrão é host. As opções são as seguintes: <ul style="list-style-type: none"> <li>● host</li> <li>● container</li> </ul> Mínimo: <b>0</b> Máximo: <b>64</b>

## Parâmetros de solicitação

**Tabela 3-7** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>32</b> Máximo: <b>4096</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-8** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total de contas Mínimo: <b>0</b> Máximo: <b>10000</b>
data_list	Array of <a href="#">UserStatisticInfoResponseInfo</a> objects	Lista de estatísticas da conta Comprimento da matriz: <b>0–10000</b>

**Tabela 3-9** UserStatisticInfoResponseInfo

Parâmetro	Tipo	Descrição
user_name	String	Nome da conta. Ele deve estar em conformidade com as regras de nomenclatura de arquivos do Windows. O valor pode conter letras, dígitos, sublinhados (_) e os seguintes caracteres especiais: !@.- Mínimo: <b>1</b> Máximo: <b>128</b>
num	Integer	Número de servidores da conta Mínimo: <b>0</b> Máximo: <b>10000</b>

## Exemplo de solicitações

As primeiras 10 contas são consultadas por padrão.

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

## Exemplo de respostas

**Código de status: 200**

Número de servidores que têm a conta

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListUserStatisticsSolution {

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

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

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListUserStatisticsRequest request = new ListUserStatisticsRequest();
        request.withUserName("<user_name>");
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withLimit("<limit>");
        request.withOffset("<offset>");
        request.withCategory("<category>");
        try {
            ListUserStatisticsResponse response =
client.listUserStatistics(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.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 huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListUserStatisticsRequest()
        request.user_name = "<user_name>"
        request.enterprise_project_id = "<enterprise_project_id>"
        request.limit = <limit>
        request.offset = <offset>
        request.category = "<category>"
        response = client.list_user_statistics(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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

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

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

```
Build()

request := &model.ListUserStatisticsRequest{
  userNameRequest:= "<user_name>"
  request.UserName = &userNameRequest
  enterpriseProjectIdRequest:= "<enterprise_project_id>"
  request.EnterpriseProjectId = &enterpriseProjectIdRequest
  limitRequest:= int32(<limit>)
  request.Limit = &limitRequest
  offsetRequest:= int32(<offset>)
  request.Offset = &offsetRequest
  categoryRequest:= "<category>"
  request.Category = &categoryRequest
  response, err := client.ListUserStatistics(request)
  if err == nil {
    fmt.Printf("%+v\n", response)
  } else {
    fmt.Println(err)
  }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Número de servidores que têm a conta

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.1.3 Consulta de estatísticas de portas abertas

#### Função

Esta API é usada para consultar a lista de portas abertas. O número de servidores pode ser consultado por porta ou tipo de protocolo.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/asset/port/statistics

**Tabela 3-10** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-11** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
port	Não	Integer	Número da porta, que é usado para correspondência exata. Mínimo: <b>1</b> Máximo: <b>65535</b>
port_string	Não	String	Cadeia de portas, que é usada para correspondência difusa. Mínimo: <b>1</b> Máximo: <b>256</b>
type	Não	String	Tipo da porta Mínimo: <b>1</b> Máximo: <b>256</b>
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>128</b>
sort_key	Não	String	Chave de classificação. Atualmente, a classificação por número de porta é suportada. Mínimo: <b>1</b> Máximo: <b>128</b>
sort_dir	Não	String	Se os dados devem ser classificados em ordem crescente ou decrescente. Valor padrão: asc Mínimo: <b>1</b> Máximo: <b>32</b>

Parâmetro	Obrigatório	Tipo	Descrição
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
category	Não	String	Tipo. O valor padrão é host. As opções são as seguintes: <ul style="list-style-type: none"><li>● host</li><li>● container</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>

## Parâmetros de solicitação

Tabela 3-12 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>32</b> Máximo: <b>4096</b>

## Parâmetros de resposta

Código de status: **200**

**Tabela 3-13** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número de portas abertas Mínimo: <b>0</b> Máximo: <b>10000</b>
data_list	Array of <b>PortStatisticResponseInfo</b> objects	Lista de estatísticas de portas abertas Comprimento da matriz: <b>0–10000</b>

**Tabela 3-14** PortStatisticResponseInfo

Parâmetro	Tipo	Descrição
port	Integer	Número da porta Mínimo: <b>0</b> Máximo: <b>65535</b>
type	String	Tipo da porta Mínimo: <b>1</b> Máximo: <b>256</b>
num	Integer	Número de portas Mínimo: <b>0</b> Máximo: <b>10000</b>
status	String	Tipo de risco: danger ou unknown Mínimo: <b>1</b> Máximo: <b>16</b>

## Exemplo de solicitações

As primeiras 10 portas abertas cujo número de porta é 123 e o tipo é host são consultadas por padrão.

```
GET https://{endpoint}/v5/{project_id}/asset/port/statistics?port=123&category=host
```

## Exemplo de respostas

**Código de status: 200**

Retorna as informações da porta, incluindo o número, o tipo, a quantidade e o status de risco da porta.

```
{
  "total_num" : 1,
  "data_list" : [ {
```

```
"num" : 4,  
"port" : 123,  
"type" : "UDP",  
"status" : "danger"  
} ]  
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;  
import com.huaweicloud.sdk.hss.v5.region.HssRegion;  
import com.huaweicloud.sdk.hss.v5.*;  
import com.huaweicloud.sdk.hss.v5.model.*;  
  
public class ListPortStatisticsSolution {  
  
    public static void main(String[] args) {  
        // The AK and SK used for authentication are hard-coded or stored in  
        plaintext, which has great security risks. It is recommended that the AK and SK  
        be stored in ciphertext in configuration files or environment variables and  
        decrypted during use to ensure security.  
        // In this example, AK and SK are stored in environment variables for  
        authentication. Before running this example, set environment variables  
        CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
        String ak = System.getenv("CLOUD_SDK_AK");  
        String sk = System.getenv("CLOUD_SDK_SK");  
  
        ICredential auth = new BasicCredentials()  
            .withAk(ak)  
            .withSk(sk);  
  
        HssClient client = HssClient.newBuilder()  
            .withCredential(auth)  
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))  
            .build();  
        ListPortStatisticsRequest request = new ListPortStatisticsRequest();  
        request.withPort(<port>);  
        request.withPortString("<port_string>");  
        request.withType("<type>");  
        request.withEnterpriseProjectId("<enterprise_project_id>");  
        request.withSortKey("<sort_key>");  
        request.withSortDir("<sort_dir>");  
        request.withLimit(<limit>);  
        request.withOffset(<offset>);  
        request.withCategory("<category>");  
        try {  
            ListPortStatisticsResponse response =  
client.listPortStatistics(request);  
            System.out.println(response.toString());  
        } catch (ConnectionException e) {  
            e.printStackTrace();  
        } catch (RequestTimeoutException e) {  
            e.printStackTrace();  
        } catch (ServiceResponseException e) {  
            e.printStackTrace();  
            System.out.println(e.getHttpStatusCode());  
            System.out.println(e.getRequestId());  
        }  
    }  
}
```

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

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListPortStatisticsRequest()
        request.port = <port>
        request.port_string = "<port_string>"
        request.type = "<type>"
        request.enterprise_project_id = "<enterprise_project_id>"
        request.sort_key = "<sort_key>"
        request.sort_dir = "<sort_dir>"
        request.limit = <limit>
        request.offset = <offset>
        request.category = "<category>"
        response = client.list_port_statistics(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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

```
// In this example, AK and SK are stored in environment variables for
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")

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

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

request := &model.ListPortStatisticsRequest{
    portRequest:= int32(<port>)
    request.Port = &portRequest
    portStringRequest:= "<port_string>"
    request.PortString = &portStringRequest
    typeRequest:= "<type>"
    request.Type = &typeRequest
    enterpriseProjectIdRequest:= "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    sortKeyRequest:= "<sort_key>"
    request.SortKey = &sortKeyRequest
    sortDirRequest:= "<sort_dir>"
    request.SortDir = &sortDirRequest
    limitRequest:= int32(<limit>)
    request.Limit = &limitRequest
    offsetRequest:= int32(<offset>)
    request.Offset = &offsetRequest
    categoryRequest:= "<category>"
    request.Category = &categoryRequest
    response, err := client.ListPortStatistics(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Retorna as informações da porta, incluindo o número, o tipo, a quantidade e o status de risco da porta.

## Códigos de erro

Consulte [Códigos de erro](#).



## 3.1.4 Consulta da lista de processos

### Função

Essa API é usada para consultar a lista de processos e consultar o número de servidores com base no parâmetro de caminho do processo.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/asset/process/statistics

**Tabela 3-15** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-16** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
path	Não	String	Caminho do processo executável Mínimo: <b>1</b> Máximo: <b>256</b>
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>1</b> Máximo: <b>256</b>
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>10</b> Máximo: <b>100</b> Padrão: <b>10</b>

Parâmetro	Obrigatório	Tipo	Descrição
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>10000</b> Padrão: <b>0</b>
category	Não	String	Tipo. O valor padrão é host. As opções são as seguintes: <ul style="list-style-type: none"><li>● host</li><li>● container</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>

## Parâmetros de solicitação

Tabela 3-17 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>32</b> Máximo: <b>4096</b>

## Parâmetros de resposta

Código de status: **200**

Tabela 3-18 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total de estatísticas de processo Mínimo: <b>0</b> Máximo: <b>10000</b>

Parâmetro	Tipo	Descrição
data_list	Array of <b>ProcessStatisticResponseInfo</b> objects	Lista de estatísticas de processo Comprimento da matriz: <b>0–10000</b>

**Tabela 3-19** ProcessStatisticResponseInfo

Parâmetro	Tipo	Descrição
path	String	Caminho do arquivo de execução do processo. Mínimo: <b>1</b> Máximo: <b>256</b>
num	Integer	Número de processos Mínimo: <b>0</b> Máximo: <b>100000</b>

## Exemplo de solicitações

As primeiras 10 contas são consultadas por padrão.

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

## Exemplo de respostas

**Código de status: 200**

Número de servidores que possuem o processo

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

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

public class ListProcessStatisticsSolution {

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

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

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

        ListProcessStatisticsRequest request = new ListProcessStatisticsRequest();
        request.withPath("<path>");
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withLimit(<limit>);
        request.withOffset(<offset>);
        request.withCategory("<category>");
        try {
            ListProcessStatisticsResponse response =
client.listProcessStatistics(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

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

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

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

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

try:
    request = ListProcessStatisticsRequest()
    request.path = "<path>"
    request.enterprise_project_id = "<enterprise_project_id>"
    request.limit = <limit>
    request.offset = <offset>
    request.category = "<category>"
    response = client.list_process_statistics(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ListProcessStatisticsRequest{}
    pathRequest := "<path>"
    request.Path = &pathRequest
    enterpriseProjectIdRequest := "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    limitRequest := int32(<limit>)
    request.Limit = &limitRequest
    offsetRequest := int32(<offset>)
    request.Offset = &offsetRequest
    categoryRequest := "<category>"
    request.Category = &categoryRequest
    response, err := client.ListProcessStatistics(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    }
}
```

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

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Número de servidores que possuem o processo

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.1.5 Consulta da lista de softwares

### Função

Esta API é usada para consultar a lista de softwares. O número de servidores pode ser consultado pelo nome do software.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/asset/app/statistics

Tabela 3-20 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-21** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
app_name	Não	String	Nome do software Mínimo: <b>1</b> Máximo: <b>256</b>
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>1</b> Máximo: <b>256</b>
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>10</b> Máximo: <b>100</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>10000</b> Padrão: <b>0</b>
category	Não	String	Tipo. O valor padrão é host. As opções são as seguintes: <ul style="list-style-type: none"><li>● host</li><li>● container</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>

## Parâmetros de solicitação

**Tabela 3-22** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário.  Mínimo: <b>32</b> Máximo: <b>4096</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-23** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total de estatísticas de processo Mínimo: <b>0</b> Máximo: <b>10000</b>
data_list	Array of <a href="#">AppStatisticResponseInfo</a> objects	Lista de estatísticas de processo Comprimento da matriz: <b>0–10000</b>

**Tabela 3-24** AppStatisticResponseInfo

Parâmetro	Tipo	Descrição
app_name	String	Nome do software Mínimo: <b>1</b> Máximo: <b>128</b>
num	Integer	Número de processos Mínimo: <b>0</b> Máximo: <b>100000</b>

## Exemplo de solicitações

As primeiras 10 listas de software cujo tipo é host são consultadas por padrão.



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

## Exemplo de respostas

### Código de status: 200

Número de servidores que possuem o software

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListAppStatisticsSolution {

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

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

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

        ListAppStatisticsRequest request = new ListAppStatisticsRequest();
        request.withAppName("<app_name>");
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withLimit("<limit>");
        request.withOffset("<offset>");
        request.withCategory("<category>");
        try {
            ListAppStatisticsResponse response =
                client.listAppStatistics(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        }
    }
}
```

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

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListAppStatisticsRequest()
        request.app_name = "<app_name>"
        request.enterprise_project_id = "<enterprise_project_id>"
        request.limit = <limit>
        request.offset = <offset>
        request.category = "<category>"
        response = client.list_app_statistics(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

func main() {
    // The AK and SK used for authentication are hard-coded or stored in
    // plaintext, which has great security risks. It is recommended that the AK and SK
```

```
be stored in ciphertext in configuration files or environment variables and
decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")

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

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

request := &model.ListAppStatisticsRequest{}
appNameRequest := "<app_name>"
request.AppName = &appNameRequest
enterpriseProjectIdRequest := "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
limitRequest := int32(<limit>)
request.Limit = &limitRequest
offsetRequest := int32(<offset>)
request.Offset = &offsetRequest
categoryRequest := "<category>"
request.Category = &categoryRequest
response, err := client.ListAppStatistics(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Número de servidores que possuem o software

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.1.6 Consulta de informações sobre itens de inicialização automática

### Função

Essa API é usada para consultar as informações de inicialização automática. O tipo de inicialização e o número de servidores podem ser consultados com base no nome de inicialização automática.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/asset/auto-launch/statistics

**Tabela 3-25** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-26** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
name	Não	String	Nome do item iniciado automaticamente Mínimo: <b>1</b> Máximo: <b>256</b>
type	Não	String	Tipo de item iniciado automaticamente <ul style="list-style-type: none"><li>● 0: serviço iniciado automaticamente</li><li>● 1: tarefa agendada</li><li>● 2: pré-carregar biblioteca dinâmica</li><li>● 3: executar chave de registro</li><li>● 4: pasta de inicialização</li></ul> Mínimo: <b>1</b> Máximo: <b>256</b>

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>1</b> Máximo: <b>256</b>
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>10</b> Máximo: <b>100</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>10000</b> Padrão: <b>0</b>

## Parâmetros de solicitação

Tabela 3-27 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>32</b> Máximo: <b>4096</b>

## Parâmetros de resposta

Código de status: **200**

**Tabela 3-28** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total de itens iniciados automaticamente Mínimo: <b>0</b> Máximo: <b>10000</b>
data_list	Array of <b>AutoLaunchStatisticsResponseInfo</b> objects	Lista de estatísticas de itens iniciados automaticamente Comprimento da matriz: <b>0-10000</b>

**Tabela 3-29** AutoLaunchStatisticsResponseInfo

Parâmetro	Tipo	Descrição
name	String	Nome do item iniciado automaticamente Mínimo: <b>1</b> Máximo: <b>256</b>
type	String	Tipo de item iniciado automaticamente <ul style="list-style-type: none"> <li>● 0: serviço iniciado automaticamente</li> <li>● 1: tarefa agendada</li> <li>● 2: pré-carregar biblioteca dinâmica</li> <li>● 3: executar chave de registro</li> <li>● 4: pasta de inicialização</li> </ul> Mínimo: <b>1</b> Máximo: <b>11</b>
num	Integer	Número de servidores que têm os itens de inicialização automática. Mínimo: <b>0</b> Máximo: <b>10000</b>

## Exemplo de solicitações

Os primeiros 10 itens de inicialização automática são consultados por padrão.

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

## Exemplo de respostas

**Código de status: 200**

Número de servidores que possuem o processo

```
{
  "total_num" : 1,
```

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

```
}  
}
```

## Python

```
# coding: utf-8  
  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudsdkhss.v5.region.hss_region import HssRegion  
from huaweicloudsdkcore.exceptions import exceptions  
from huaweicloudsdkhss.v5 import *  
  
if __name__ == "__main__":  
    # The AK and SK used for authentication are hard-coded or stored in  
    plaintext, which has great security risks. It is recommended that the AK and SK  
    be stored in ciphertext in configuration files or environment variables and  
    decrypted during use to ensure security.  
    # In this example, AK and SK are stored in environment variables for  
    authentication. Before running this example, set environment variables  
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak = __import__('os').getenv("CLOUD_SDK_AK")  
    sk = __import__('os').getenv("CLOUD_SDK_SK")  
  
    credentials = BasicCredentials(ak, sk) \  
  
    client = HssClient.new_builder() \  
        .with_credentials(credentials) \  
        .with_region(HssRegion.value_of("<YOUR REGION>")) \  
        .build()  
  
    try:  
        request = ListAutoLaunchStatisticsRequest()  
        request.name = "<name>"  
        request.type = "<type>"  
        request.enterprise_project_id = "<enterprise_project_id>"  
        request.limit = <limit>  
        request.offset = <offset>  
        response = client.list_auto_launch_statistics(request)  
        print(response)  
    except exceptions.ClientRequestException as e:  
        print(e.status_code)  
        print(e.request_id)  
        print(e.error_code)  
        print(e.error_msg)
```

## Go

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in  
    plaintext, which has great security risks. It is recommended that the AK and SK  
    be stored in ciphertext in configuration files or environment variables and  
    decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for  
    authentication. Before running this example, set environment variables  
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
  
    auth := basic.NewCredentialsBuilder().
```



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

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

request := &model.ListAutoLaunchStatisticsRequest{}
nameRequest := "<name>"
request.Name = &nameRequest
typeRequest := "<type>"
request.Type = &typeRequest
enterpriseProjectIdRequest := "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
limitRequest := int32(<limit>)
request.Limit = &limitRequest
offsetRequest := int32(<offset>)
request.Offset = &offsetRequest
response, err := client.ListAutoLaunchStatistics(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Número de servidores que possuem o processo

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.1.7 Consulta da lista de servidores de uma conta

### Função

Essa API é usada para consultar a lista de servidores de uma conta.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

## URI

GET /v5/{project\_id}/asset/users

**Tabela 3-30** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>128</b>

**Tabela 3-31** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
host_id	Não	String	ID do host Mínimo: <b>0</b> Máximo: <b>128</b>
user_name	Não	String	Nome da conta Mínimo: <b>0</b> Máximo: <b>32</b>
host_name	Não	String	Nome do host Mínimo: <b>0</b> Máximo: <b>128</b>
private_ip	Não	String	Endereço IP privado de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
login_permission	Não	Boolean	Se o logon é permitido.
root_permission	Não	Boolean	Se o usuário tem permissões de root
user_group	Não	String	Grupo de usuários do servidor Mínimo: <b>0</b> Máximo: <b>128</b>
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>128</b>

Parâmetro	Obrigatório	Tipo	Descrição
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
category	Não	String	Tipo. O valor padrão é host. As opções são as seguintes: <ul style="list-style-type: none"> <li>● host</li> <li>● container</li> </ul> Mínimo: <b>0</b> Máximo: <b>64</b>
part_match	Não	Boolean	Se a correspondência difusa é usada. O valor padrão é false.

## Parâmetros de solicitação

Tabela 3-32 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>

## Parâmetros de resposta

Código de status: **200**

**Tabela 3-33** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total de contas Mínimo: <b>0</b> Máximo: <b>10000</b>
data_list	Array of <b>UserResponseInfo</b> objects	Lista de informações da conta Comprimento da matriz: <b>0–10000</b>

**Tabela 3-34** UserResponseInfo

Parâmetro	Tipo	Descrição
agent_id	String	ID do agente Mínimo: <b>1</b> Máximo: <b>128</b>
host_id	String	ID do host Mínimo: <b>1</b> Máximo: <b>128</b>
host_name	String	Nome de servidor Mínimo: <b>1</b> Máximo: <b>128</b>
host_ip	String	Endereço IP do servidor Mínimo: <b>1</b> Máximo: <b>128</b>
user_name	String	Nome de usuário Mínimo: <b>1</b> Máximo: <b>128</b>
login_permission	Boolean	Se o usuário tem a permissão de logon
root_permission	Boolean	Se o usuário tem permissões de root
user_group_name	String	Nome do grupo de usuários Mínimo: <b>1</b> Máximo: <b>128</b>
user_home_dir	String	Diretório inicial do usuário Mínimo: <b>1</b> Máximo: <b>256</b>

Parâmetro	Tipo	Descrição
shell	String	Shell de inicialização do usuário Mínimo: <b>1</b> Máximo: <b>128</b>
recent_scan_time	Long	Hora da última verificação Mínimo: <b>0</b> Máximo: <b>4070880000000</b>
container_id	String	ID do container Mínimo: <b>1</b> Máximo: <b>128</b>
container_name	String	Nome do container Mínimo: <b>1</b> Máximo: <b>256</b>

## Exemplo de solicitações

Consultar a lista de servidores cuja conta é daemon por padrão.

```
GET https://{endpoint}/v5/{project_id}/asset/users?user_name=daemon
```

## Exemplo de respostas

**Código de status: 200**

Lista de informações da conta

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "0bf792d910xxxxxxxxxxxx52cb7e63exxx",
    "host_id" : "13xxxxxxxxxece69",
    "host_ip" : "192.168.0.1",
    "host_name" : "test",
    "login_permission" : false,
    "recent_scan_time" : 1667039707730,
    "root_permission" : false,
    "shell" : "/sbin/nologin",
    "user_group_name" : "bin",
    "user_home_dir" : "/bin",
    "user_name" : "bin",
    "container_id" : "ce794b8a6-xxxx-xxxx-xxxx-36bedf2c7a4f6083fb82e5bbc82709b50018",
    "container_name" : "hss_imagescan_W73V1W06"
  } ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

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

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

public class ListUsersSolution {

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

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

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

        ListUsersRequest request = new ListUsersRequest();
        request.withHostId("<host_id>");
        request.withUserName("<user_name>");
        request.withHostName("<host_name>");
        request.withPrivateIp("<private_ip>");
        request.withLoginPermission("<login_permission>");
        request.withRootPermission("<root_permission>");
        request.withUserGroup("<user_group>");
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withLimit("<limit>");
        request.withOffset("<offset>");
        request.withCategory("<category>");
        request.withPartMatch("<part_match>");
        try {
            ListUsersResponse response = client.listUsers(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

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

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListUsersRequest()
        request.host_id = "<host_id>"
        request.user_name = "<user_name>"
        request.host_name = "<host_name>"
        request.private_ip = "<private_ip>"
        request.login_permission = <LoginPermission>
        request.root_permission = <RootPermission>
        request.user_group = "<user_group>"
        request.enterprise_project_id = "<enterprise_project_id>"
        request.limit = <limit>
        request.offset = <offset>
        request.category = "<category>"
        request.part_match = <PartMatch>
        response = client.list_users(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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

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

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

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

request := &model.ListUsersRequest{}
hostIdRequest:= "<host_id>"
request.HostId = &hostIdRequest
userNameRequest:= "<user_name>"
request.UserName = &userNameRequest
hostNameRequest:= "<host_name>"
request.HostName = &hostNameRequest
privateIpRequest:= "<private_ip>"
request.PrivateIp = &privateIpRequest
loginPermissionRequest:= <login_permission>
request.LoginPermission = &loginPermissionRequest
rootPermissionRequest:= <root_permission>
request.RootPermission = &rootPermissionRequest
userGroupRequest:= "<user_group>"
request.UserGroup = &userGroupRequest
enterpriseProjectIdRequest:= "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
limitRequest:= int32(<limit>)
request.Limit = &limitRequest
offsetRequest:= int32(<offset>)
request.Offset = &offsetRequest
categoryRequest:= "<category>"
request.Category = &categoryRequest
partMatchRequest:= <part_match>
request.PartMatch = &partMatchRequest
response, err := client.ListUsers(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia [Código de amostra no API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de informações da conta

## Códigos de erro

Consulte [Códigos de erro](#).



## 3.1.8 Consulta da lista de portas abertas de um único servidor

### Função

Essa API é usada para consultar a lista de portas abertas de um único servidor.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/asset/ports

**Tabela 3-35** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-36** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
host_id	Sim	String	ID de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
host_name	Não	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
host_ip	Não	String	Endereço IP do servidor Mínimo: <b>0</b> Máximo: <b>128</b>
port	Não	Integer	Número da porta Mínimo: <b>1</b> Máximo: <b>65535</b>
type	Não	String	Tipo da porta: TCP ou UDP. Mínimo: <b>0</b> Máximo: <b>128</b>

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>256</b>
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>10</b> Máximo: <b>100</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>10000</b> Padrão: <b>0</b>
category	Não	String	Tipo. O valor padrão é host. As opções são as seguintes: <ul style="list-style-type: none"> <li>● host</li> <li>● container</li> </ul> Mínimo: <b>0</b> Máximo: <b>64</b>

## Parâmetros de solicitação

**Tabela 3-37** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>32</b> Máximo: <b>4096</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-38** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número de portas abertas Mínimo: <b>0</b> Máximo: <b>10000</b>
data_list	Array of <b>PortResponseInfo</b> objects	Lista de informações da porta Comprimento da matriz: <b>0–10000</b>

**Tabela 3-39** PortResponseInfo

Parâmetro	Tipo	Descrição
host_id	String	ID de servidor Mínimo: <b>1</b> Máximo: <b>128</b>
laddr	String	Endereço IP de escuta Mínimo: <b>1</b> Máximo: <b>128</b>
status	String	Status da porta. <ul style="list-style-type: none"><li>● normal</li><li>● danger</li><li>● unknown</li></ul> Mínimo: <b>1</b> Máximo: <b>10</b>
port	Integer	Número da porta Mínimo: <b>0</b> Máximo: <b>65535</b>
type	String	Tipo da porta: TCP ou UDP. Mínimo: <b>1</b> Máximo: <b>64</b>
pid	Integer	ID do processo Mínimo: <b>1</b> Máximo: <b>65535</b>

Parâmetro	Tipo	Descrição
path	String	Caminho do arquivo de execução do processo. Mínimo: <b>1</b> Máximo: <b>256</b>
agent_id	String	ID do agente Mínimo: <b>1</b> Máximo: <b>64</b>
container_id	String	ID do container Mínimo: <b>0</b> Máximo: <b>128</b>

## Exemplo de solicitações

As primeiras 10 portas abertas cujo host\_id é dd91cd32-a238-4c0e-bc01-3b11653714ac são consultadas por padrão.

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

## Exemplo de respostas

**Código de status: 200**

Lista de informações da porta

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

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

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

public class ListPortsSolution {

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

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

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

        ListPortsRequest request = new ListPortsRequest();
        request.withHostId("<host_id>");
        request.withHostName("<host_name>");
        request.withHostIp("<host_ip>");
        request.withPort("<port>");
        request.withType("<type>");
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withLimit("<limit>");
        request.withOffset("<offset>");
        request.withCategory("<category>");
        try {
            ListPortsResponse response = client.listPorts(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

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

```
from huaweicloudsdkhss.v5 import *

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListPortsRequest()
        request.host_id = "<host_id>"
        request.host_name = "<host_name>"
        request.host_ip = "<host_ip>"
        request.port = <port>
        request.type = "<type>"
        request.enterprise_project_id = "<enterprise_project_id>"
        request.limit = <limit>
        request.offset = <offset>
        request.category = "<category>"
        response = client.list_ports(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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

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

    client := hss.NewHssClient(
        hss.HssClientBuilder().
```

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

request := &model.ListPortsRequest{}
request.HostId = "<host_id>"
hostNameRequest:= "<host_name>"
request.HostName = &hostNameRequest
hostIpRequest:= "<host_ip>"
request.HostIp = &hostIpRequest
portRequest:= int32(<port>)
request.Port = &portRequest
typeRequest:= "<type>"
request.Type = &typeRequest
enterpriseProjectIdRequest:= "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
limitRequest:= int32(<limit>)
request.Limit = &limitRequest
offsetRequest:= int32(<offset>)
request.Offset = &offsetRequest
categoryRequest:= "<category>"
request.Category = &categoryRequest
response, err := client.ListPorts(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia [Código de amostra no API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de informações da porta

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.1.9 Consulta da lista de servidores do software

### Função

Esta API é usada para consultar a lista de servidores do software.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

## URI

GET /v5/{project\_id}/asset/apps

**Tabela 3-40** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-41** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
host_id	Sim	String	ID de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
host_name	Não	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
app_name	Não	String	Nome do software Mínimo: <b>0</b> Máximo: <b>128</b>
host_ip	Não	String	Endereço IP do servidor Mínimo: <b>0</b> Máximo: <b>128</b>
version	Não	String	Versão do software Mínimo: <b>0</b> Máximo: <b>128</b>
install_dir	Não	String	Diretório de instalação Mínimo: <b>0</b> Máximo: <b>512</b>
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>1</b> Máximo: <b>256</b>



Parâmetro	Obrigatório	Tipo	Descrição
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>10</b> Máximo: <b>100</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>10000</b> Padrão: <b>0</b>
category	Não	String	Tipo. O valor padrão é host. As opções são as seguintes: <ul style="list-style-type: none"><li>● host</li><li>● container</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>
part_match	Não	Boolean	Se a correspondência difusa é usada. O valor padrão é false.

## Parâmetros de solicitação

Tabela 3-42 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>32</b> Máximo: <b>4096</b>

## Parâmetros de resposta

Código de status: **200**

**Tabela 3-43** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Total de softwares Mínimo: <b>0</b> Máximo: <b>10000</b>
data_list	Array of <b>ApiResponseInfo</b> objects	Lista de softwares Comprimento da matriz: <b>0-10000</b>

**Tabela 3-44** ApiResponseInfo

Parâmetro	Tipo	Descrição
agent_id	String	ID do agente do HSS Mínimo: <b>0</b> Máximo: <b>128</b>
host_id	String	ID de servidor Mínimo: <b>1</b> Máximo: <b>128</b>
host_name	String	Nome de servidor Mínimo: <b>1</b> Máximo: <b>256</b>
host_ip	String	Endereço IP do servidor Mínimo: <b>1</b> Máximo: <b>256</b>
app_name	String	Nome do software Mínimo: <b>1</b> Máximo: <b>128</b>
version	String	Número da versão Mínimo: <b>1</b> Máximo: <b>128</b>
update_time	Long	Hora da última atualização, em milissegundos. Mínimo: <b>0</b> Máximo: <b>2147483647</b>
recent_scan_time	Long	Hora da última verificação, em milissegundos. Mínimo: <b>0</b> Máximo: <b>2147483647</b>

Parâmetro	Tipo	Descrição
container_id	String	ID do container Mínimo: 1 Máximo: 128
container_name	String	Nome do container Mínimo: 1 Máximo: 256

## Exemplo de solicitações

Os primeiros 10 servidores cujo nome de software é ACL são consultados por padrão.

```
GET https://{endpoint}/v5/{project_id}/asset/apps?app_name=acl
```

## Exemplo de respostas

**Código de status: 200**

Aplicações instaladas em um host

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" :
    "c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8",
    "host_id" : "55dac7fe-d81b-43bc-a4a7-4710fe673972",
    "host_name" : "xxxx",
    "host_ip" : "192.168.0.126",
    "app_name" : "acl",
    "version" : "2.2.51-14.eulerosv2r7",
    "update_time" : 1668150671981,
    "recent_scan_time" : 1668506044147,
    "container_id" :
    "ce794b8a6071f5fd7e4d142dab7b36bedf2c7a4f6083fb82e5bbc82709b50018",
    "container_name" : "hss_imagescan_W73V1W06"
  } ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListAppsSolution {
```

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

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

    HssClient client = HssClient.newBuilder()
        .withCredential(auth)
        .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
        .build();
    ListAppsRequest request = new ListAppsRequest();
    request.withHostId("<host_id>");
    request.withHostName("<host_name>");
    request.withAppName("<app_name>");
    request.withHostIp("<host_ip>");
    request.withVersion("<version>");
    request.withInstallDir("<install_dir>");
    request.withEnterpriseProjectId("<enterprise_project_id>");
    request.withLimit(<limit>);
    request.withOffset(<offset>);
    request.withCategory("<category>");
    request.withPartMatch(<part_match>);
    try {
        ListAppsResponse response = client.listApps(request);
        System.out.println(response.toString());
    } catch (ConnectionException e) {
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
```

## Python

```
# coding: utf-8

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

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

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

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

try:
    request = ListAppsRequest()
    request.host_id = "<host_id>"
    request.host_name = "<host_name>"
    request.app_name = "<app_name>"
    request.host_ip = "<host_ip>"
    request.version = "<version>"
    request.install_dir = "<install_dir>"
    request.enterprise_project_id = "<enterprise_project_id>"
    request.limit = <limit>
    request.offset = <offset>
    request.category = "<category>"
    request.part_match = <PartMatch>
    response = client.list_apps(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ListAppsRequest{}
    request.HostId = "<host_id>"
    hostNameRequest := "<host_name>"
    request.HostName = &hostNameRequest
    appNameRequest := "<app_name>"
    request.AppName = &appNameRequest
    hostIpRequest := "<host_ip>"
```

```
request.HostIp = &hostIpRequest
versionRequest:= "<version>"
request.Version = &versionRequest
installDirRequest:= "<install_dir>"
request.InstallDir = &installDirRequest
enterpriseProjectIdRequest:= "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
limitRequest:= int32(<limit>)
request.Limit = &limitRequest
offsetRequest:= int32(<offset>)
request.Offset = &offsetRequest
categoryRequest:= "<category>"
request.Category = &categoryRequest
partMatchRequest:= <part_match>
request.PartMatch = &partMatchRequest
response, err := client.ListApps(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Aplicações instaladas em um host

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.1.10 Consulta da lista de serviços de itens iniciados automaticamente

### Função

Esta API é usada para consultar a lista de serviços de itens iniciados automaticamente.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/asset/auto-launchs

**Tabela 3-45** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-46** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
host_id	Não	String	ID de servidor Mínimo: <b>1</b> Máximo: <b>128</b>
host_name	Não	String	Nome de servidor Mínimo: <b>1</b> Máximo: <b>128</b>
name	Não	String	Nome do item iniciado automaticamente Mínimo: <b>1</b> Máximo: <b>256</b>
host_ip	Não	String	Endereço IP do servidor Mínimo: <b>1</b> Máximo: <b>128</b>
type	Não	String	Tipo de item iniciado automaticamente <ul style="list-style-type: none"><li>● 0: serviço iniciado automaticamente</li><li>● 1: tarefa agendada</li><li>● 2: pré-carregar biblioteca dinâmica</li><li>● 3: executar chave de registro</li><li>● 4: pasta de inicialização</li></ul> Mínimo: <b>1</b> Máximo: <b>128</b>
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>1</b> Máximo: <b>256</b>

Parâmetro	Obrigatório	Tipo	Descrição
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>10</b> Máximo: <b>100</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>10000</b> Padrão: <b>0</b>
part_match	Não	Boolean	Se a correspondência difusa é usada. O valor padrão é false.

## Parâmetros de solicitação

Tabela 3-47 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>32</b> Máximo: <b>4096</b>

## Parâmetros de resposta

Código de status: **200**

Tabela 3-48 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total de itens de inicialização automática Mínimo: <b>0</b> Máximo: <b>10000</b>



Parâmetro	Tipo	Descrição
data_list	Array of <b>AutoLauchResponseInfo</b> objects	Lista de itens iniciados automaticamente Comprimento da matriz: <b>0–10000</b>

**Tabela 3-49** AutoLauchResponseInfo

Parâmetro	Tipo	Descrição
agent_id	String	ID do agente Mínimo: <b>0</b> Máximo: <b>128</b>
host_id	String	ID de servidor Mínimo: <b>1</b> Máximo: <b>128</b>
host_name	String	Nome de servidor Mínimo: <b>1</b> Máximo: <b>256</b>
host_ip	String	Endereço IP do servidor Mínimo: <b>1</b> Máximo: <b>256</b>
name	String	Nome do item iniciado automaticamente Mínimo: <b>1</b> Máximo: <b>256</b>
type	Integer	Tipo de item iniciado automaticamente <ul style="list-style-type: none"> <li>● 0: serviço iniciado automaticamente</li> <li>● 1: tarefa agendada</li> <li>● 2: pré-carregar biblioteca dinâmica</li> <li>● 3: executar chave de registro</li> <li>● 4: pasta de inicialização</li> </ul> Mínimo: <b>0</b> Máximo: <b>11</b>
path	String	Caminho do item de inicialização automática Mínimo: <b>1</b> Máximo: <b>256</b>

Parâmetro	Tipo	Descrição
hash	String	Valor de hash do arquivo gerado usando o algoritmo SHA256 Mínimo: <b>1</b> Máximo: <b>128</b>
run_user	String	Usuário que inicia a execução Mínimo: <b>1</b> Máximo: <b>128</b>
recent_scan_time	Long	Hora da última verificação Mínimo: <b>0</b> Máximo: <b>4824430336000</b>

## Exemplo de solicitações

Os primeiros 10 serviços cujo nome de item de inicialização automática é S50multi-queue são consultados por padrão.

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

## Exemplo de respostas

**Código de status: 200**

Lista de inicialização automática

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" :
"9e742932bff2894e3d0869d03989b05cefb27a6cbc201d98c4465296xxxxxxxx",
    "host_id" : "3d0581a5-03b9-4311-9149-c026b0726a7e",
    "host_name" : "name",
    "host_ip" : "3d0581a5-03b9-4311-9149-c026b0726a7e",
    "name" : "S12hostguard",
    "type" : 0,
    "path" : "/etc/hostguard",
    "hash" : "xxxxxxxx227bffa0c04425ba6c8e0024046caa38dfbca6281b40109xxxxxxxx",
    "run_user" : "user",
    "recent_scan_time" : 1668240858425
  } ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

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

public class ListAutoLaunchsSolution {

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

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

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ListAutoLaunchsRequest request = new ListAutoLaunchsRequest();
        request.withHostId("<host_id>");
        request.withHostName("<host_name>");
        request.withName("<name>");
        request.withHostIp("<host_ip>");
        request.withType("<type>");
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withLimit(<limit>);
        request.withOffset(<offset>);
        request.withPartMatch(<part_match>);
        try {
            ListAutoLaunchsResponse response = client.listAutoLaunchs(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.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 huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

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

```
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak = __import__('os').getenv("CLOUD_SDK_AK")
sk = __import__('os').getenv("CLOUD_SDK_SK")

credentials = BasicCredentials(ak, sk) \

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

try:
    request = ListAutoLaunchsRequest()
    request.host_id = "<host_id>"
    request.host_name = "<host_name>"
    request.name = "<name>"
    request.host_ip = "<host_ip>"
    request.type = "<type>"
    request.enterprise_project_id = "<enterprise_project_id>"
    request.limit = <limit>
    request.offset = <offset>
    request.part_match = <PartMatch>
    response = client.list_auto_launchs(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ListAutoLaunchsRequest{}
    requestIdRequest := "<host_id>"
    request.HostId = &hostIdRequest
    request.HostNameRequest := "<host_name>"
```

```
request.HostName = &hostNameRequest
nameRequest:= "<name>"
request.Name = &nameRequest
hostIpRequest:= "<host_ip>"
request.HostIp = &hostIpRequest
typeRequest:= "<type>"
request.Type = &typeRequest
enterpriseProjectIdRequest:= "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
limitRequest:= int32(<limit>)
request.Limit = &limitRequest
offsetRequest:= int32(<offset>)
request.Offset = &offsetRequest
partMatchRequest:= <part_match>
request.PartMatch = &partMatchRequest
response, err := client.ListAutoLaunchs(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de inicialização automática

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.1.11 Obtenção do histórico de alterações da conta

#### Função

Essa API é usada para obter o histórico de alterações da conta.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/asset/user/change-history

**Tabela 3-50** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-51** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
user_name	Não	String	Nome de usuário Mínimo: <b>1</b> Máximo: <b>128</b>
host_id	Não	String	ID de servidor Mínimo: <b>1</b> Máximo: <b>128</b>
root_permission	Não	Boolean	Se o usuário tem permissões de root
host_name	Não	String	Nome de servidor Mínimo: <b>1</b> Máximo: <b>128</b>
private_ip	Não	String	Endereço IP privado de servidor Mínimo: <b>1</b> Máximo: <b>128</b>
change_type	Não	String	Tipo de alteração de conta. As opções são as seguintes: <ul style="list-style-type: none"><li>● ADD</li><li>● DELETE</li><li>● MODIFY</li></ul> Mínimo: <b>1</b> Máximo: <b>128</b>
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>10</b> Máximo: <b>100</b> Padrão: <b>10</b>

Parâmetro	Obrigatório	Tipo	Descrição
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>10000</b> Padrão: <b>0</b>
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>1</b> Máximo: <b>256</b>
start_time	Não	Long	Hora de início de uma mudança. Seu valor é um carimbo de data/hora de 13 dígitos. Mínimo: <b>0</b> Máximo: <b>4070880000000</b>
end_time	Não	Long	Hora de término de uma alteração. Seu valor é um carimbo de data/hora de 13 dígitos. Mínimo: <b>0</b> Máximo: <b>4070880000000</b>

## Parâmetros de solicitação

Tabela 3-52 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>32</b> Máximo: <b>4096</b>

## Parâmetros de resposta

Código de status: **200**

**Tabela 3-53** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total de contas alteradas Mínimo: <b>0</b> Máximo: <b>10000000</b>
data_list	Array of <b>UserChangeHistoryResponseInfo</b> objects	Histórico de alterações de conta Comprimento da matriz: <b>0–200</b>

**Tabela 3-54** UserChangeHistoryResponseInfo

Parâmetro	Tipo	Descrição
agent_id	String	ID do agente Mínimo: <b>1</b> Máximo: <b>128</b>
change_type	String	Tipo de alteração. Seu valor pode ser: <ul style="list-style-type: none"><li>● ADD</li><li>● DELETE</li><li>● MODIFY</li></ul> Mínimo: <b>1</b> Máximo: <b>128</b>
host_id	String	ID do host Mínimo: <b>1</b> Máximo: <b>128</b>
host_name	String	Nome de servidor Mínimo: <b>1</b> Máximo: <b>128</b>
private_ip	String	Endereço IP privado de servidor Mínimo: <b>1</b> Máximo: <b>128</b>
login_permission	Boolean	Se o usuário tem a permissão de logon
root_permission	Boolean	Se o usuário tem permissões de root
user_group_name	String	Nome do grupo de usuários Mínimo: <b>1</b> Máximo: <b>128</b>



Parâmetro	Tipo	Descrição
user_home_dir	String	Diretório inicial do usuário Mínimo: <b>1</b> Máximo: <b>128</b>
shell	String	Shell de inicialização do usuário Mínimo: <b>1</b> Máximo: <b>128</b>
user_name	String	Nome da conta Mínimo: <b>1</b> Máximo: <b>128</b>
expire_time	Long	Tempo de expiração, que é um carimbo de data/hora. A unidade padrão é milissegundo. Mínimo: <b>0</b> Máximo: <b>4070880000000</b>
recent_scan_time	Long	Hora em que uma conta é adicionada, modificada ou excluída. Mínimo: <b>0</b> Máximo: <b>4070880000000</b>

## Exemplo de solicitações

Os primeiros 10 registros de alteração de conta cuja hora de início é 1700446129130 e a hora de término é 1701050929130 são consultados por padrão.

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

## Exemplo de respostas

**Código de status: 200**

Histórico de alterações da conta

```
{  
  "total_num" : 1,  
  "data_list" : [ {  
    "agent_id" : "0bf792d910xxxxxxxxxxxx52cb7e63exxx",  
    "host_id" : "13xxxxxxxxxece69",  
    "private_ip" : "192.168.0.1",  
    "host_name" : "test",  
    "user_home_dir" : "/test",  
    "login_permission" : false,  
    "recent_scan_time" : 1667039707730,  
    "expire_time" : 1667039707730,  
    "root_permission" : false,  
    "shell" : "/sbin/nologin",  
    "user_group_name" : "bin",  
    "user_name" : "bin",  
    "change_type" : "ADD"  }  
]
```

```
} ]  
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;  
import com.huaweicloud.sdk.hss.v5.region.HssRegion;  
import com.huaweicloud.sdk.hss.v5.*;  
import com.huaweicloud.sdk.hss.v5.model.*;  
  
public class ListUserChangeHistoriesSolution {  
  
    public static void main(String[] args) {  
        // The AK and SK used for authentication are hard-coded or stored in  
        plaintext, which has great security risks. It is recommended that the AK and SK  
        be stored in ciphertext in configuration files or environment variables and  
        decrypted during use to ensure security.  
        // In this example, AK and SK are stored in environment variables for  
        authentication. Before running this example, set environment variables  
        CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
        String ak = System.getenv("CLOUD_SDK_AK");  
        String sk = System.getenv("CLOUD_SDK_SK");  
  
        ICredential auth = new BasicCredentials()  
            .withAk(ak)  
            .withSk(sk);  
  
        HssClient client = HssClient.newBuilder()  
            .withCredential(auth)  
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))  
            .build();  
  
        ListUserChangeHistoriesRequest request = new  
ListUserChangeHistoriesRequest();  
        request.withUserName("<user_name>");  
        request.withHostId("<host_id>");  
        request.withRootPermission("<root_permission>");  
        request.withHostName("<host_name>");  
        request.withPrivateIp("<private_ip>");  
        request.withChangeType("<change_type>");  
        request.withLimit("<limit>");  
        request.withOffset("<offset>");  
        request.withEnterpriseProjectId("<enterprise_project_id>");  
        request.withStartTime("<start_time>L");  
        request.withEndTime("<end_time>L");  
        try {  
            ListUserChangeHistoriesResponse response =  
client.listUserChangeHistories(request);  
            System.out.println(response.toString());  
        } catch (ConnectionException e) {  
            e.printStackTrace();  
        } catch (RequestTimeoutException e) {  
            e.printStackTrace();  
        } catch (ServiceResponseException e) {  
            e.printStackTrace();  
            System.out.println(e.getHttpStatusCode());  
            System.out.println(e.getRequestId());  
            System.out.println(e.getErrorCode());  
        }  
    }  
}
```

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

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListUserChangeHistoriesRequest()
        request.user_name = "<user_name>"
        request.host_id = "<host_id>"
        request.root_permission = <RootPermission>
        request.host_name = "<host_name>"
        request.private_ip = "<private_ip>"
        request.change_type = "<change_type>"
        request.limit = <limit>
        request.offset = <offset>
        request.enterprise_project_id = "<enterprise_project_id>"
        request.start_time = <start_time>
        request.end_time = <end_time>
        response = client.list_user_change_histories(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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

```

decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")

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

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

request := &model.ListUserChangeHistoriesRequest{
    userNameRequest:= "<user_name>"
    request.UserName = &userNameRequest
    hostIdRequest:= "<host_id>"
    request.HostId = &hostIdRequest
    rootPermissionRequest:= <root_permission>
    request.RootPermission = &rootPermissionRequest
    hostNameRequest:= "<host_name>"
    request.HostName = &hostNameRequest
    privateIpRequest:= "<private_ip>"
    request.PrivateIp = &privateIpRequest
    changeTypeRequest:= "<change_type>"
    request.ChangeType = &changeTypeRequest
    limitRequest:= int32(<limit>)
    request.Limit = &limitRequest
    offsetRequest:= int32(<offset>)
    request.Offset = &offsetRequest
    enterpriseProjectIdRequest:= "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    startTimeRequest:= int64(<start_time>)
    request.StartTime = &startTimeRequest
    endTimeRequest:= int64(<end_time>)
    request.EndTime = &endTimeRequest
    response, err := client.ListUserChangeHistories(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}

```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Histórico de alterações da conta

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.1.12 Obtenção dos registros históricos de alterações de informações de software

#### Função

Esta API é usada para obter os registros históricos de alterações de informações de software.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/asset/app/change-history

**Tabela 3-55** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-56** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
host_id	Não	String	ID de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
host_ip	Não	String	Endereço IP do servidor Mínimo: <b>0</b> Máximo: <b>128</b>
host_name	Não	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
app_name	Não	String	Nome do software Mínimo: <b>0</b> Máximo: <b>128</b>

Parâmetro	Obrigatório	Tipo	Descrição
variation_type	Não	String	Tipo de alteração. Seu valor pode ser: <ul style="list-style-type: none"> <li>● add</li> <li>● delete</li> <li>● modify</li> </ul> Mínimo: <b>0</b> Máximo: <b>10</b>
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>256</b>
sort_key	Não	String	Chave de classificação. Atualmente, a classificação por recent_scan_time é suportada. Mínimo: <b>1</b> Máximo: <b>128</b>
sort_dir	Não	String	Modo de classificação. O valor padrão é decrescente. <ul style="list-style-type: none"> <li>● <b>asc</b>: ordem crescente</li> <li>● <b>desc</b>: ordem decrescente</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>10</b> Máximo: <b>100</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>10000</b> Padrão: <b>0</b>

Parâmetro	Obrigatório	Tipo	Descrição
start_time	Não	Long	Hora de início de uma mudança. Seu valor é um carimbo de data/hora de 13 dígitos. Mínimo: <b>0</b> Máximo: <b>9007199254740992</b>
end_time	Não	Long	Hora de término de uma alteração. Seu valor é um carimbo de data/hora de 13 dígitos. Mínimo: <b>0</b> Máximo: <b>9007199254740992</b>

## Parâmetros de solicitação

Tabela 3-57 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>32</b> Máximo: <b>4096</b>

## Parâmetros de resposta

Código de status: **200**

Tabela 3-58 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número de alterações de software Mínimo: <b>0</b> Máximo: <b>10000</b>
data_list	Array of <a href="#">AppChangeResponseInfo</a> objects	Histórico de alterações da conta Comprimento da matriz: <b>0–10000</b>

**Tabela 3-59** AppChangeResponseInfo

Parâmetro	Tipo	Descrição
agent_id	String	ID do agente Mínimo: <b>0</b> Máximo: <b>128</b>
variation_type	String	Tipo de alteração. ● add ● delete ● modify Mínimo: <b>0</b> Máximo: <b>10</b>
host_id	String	host_id Mínimo: <b>1</b> Máximo: <b>128</b>
app_name	String	Nome do software Mínimo: <b>1</b> Máximo: <b>128</b>
host_name	String	Nome do host Mínimo: <b>1</b> Máximo: <b>128</b>
host_ip	String	Endereço IP do servidor Mínimo: <b>1</b> Máximo: <b>256</b>
version	String	Número da versão Mínimo: <b>1</b> Máximo: <b>128</b>
update_time	Long	Tempo de atualização do software Mínimo: <b>0</b> Máximo: <b>4824430336000</b>
recent_scan_time	Long	Última verificação, em ms. Mínimo: <b>0</b> Máximo: <b>4824430336000</b>

## Exemplo de solicitações

Os primeiros 10 registros de alteração de software cuja hora de início é 1700446175490 e a hora de término é 1701050975490 são consultados por padrão.



```
GET https://{endpoint}/v5/{project_id}/asset/app/change-history?  
start_time=1700446175490&end_time=1701050975490
```

## Exemplo de respostas

### Código de status: 200

Lista de informações do histórico de alterações do aplicativo

```
{  
  "total_num" : 1,  
  "data_list" : [ {  
    "agent_id" :  
"d83c7be8a106485a558f97446617443b87604c8116e3cf0453c2a44exxxxxxxx",  
    "variation_type" : "abnormal_behavior",  
    "host_id" : "f4aaca51-xxxx-xxxx-xxxx-891c9e84d885",  
    "app_name" : "hostguard",  
    "host_name" : "host_name",  
    "host_ip" : "host_ip",  
    "version" : "3.2.3",  
    "update_time" : 1668246126302,  
    "recent_scan_time" : 1668246126302  
  } ]  
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

```
request.withHostIp("<host_ip>");
request.withHostName("<host_name>");
request.withAppName("<app_name>");
request.withVariationType("<variation_type>");
request.withEnterpriseProjectId("<enterprise_project_id>");
request.withSortKey("<sort_key>");
request.withSortDir("<sort_dir>");
request.withLimit(<limit>);
request.withOffset(<offset>);
request.withStartTime(<start_time>L);
request.withEndTime(<end_time>L);
try {
    ListAppChangeHistoriesResponse response =
client.listAppChangeHistories(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.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 huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListAppChangeHistoriesRequest()
        request.host_id = "<host_id>"
        request.host_ip = "<host_ip>"
        request.host_name = "<host_name>"
        request.app_name = "<app_name>"
        request.variation_type = "<variation_type>"
        request.enterprise_project_id = "<enterprise_project_id>"
        request.sort_key = "<sort_key>"
        request.sort_dir = "<sort_dir>"
        request.limit = <limit>
        request.offset = <offset>
        request.start_time = <start_time>
```

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

## Go

```
package main

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

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

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

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

    request := &model.ListAppChangeHistoriesRequest{}
    hostIdRequest := "<host_id>"
    request.HostId = &hostIdRequest
    hostIpRequest := "<host_ip>"
    request.HostIp = &hostIpRequest
    hostNameRequest := "<host_name>"
    request.HostName = &hostNameRequest
    appNameRequest := "<app_name>"
    request.AppName = &appNameRequest
    variationTypeRequest := "<variation_type>"
    request.VariationType = &variationTypeRequest
    enterpriseProjectIdRequest := "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    sortKeyRequest := "<sort_key>"
    request.SortKey = &sortKeyRequest
    sortDirRequest := "<sort_dir>"
    request.SortDir = &sortDirRequest
    limitRequest := int32(<limit>)
    request.Limit = &limitRequest
    offsetRequest := int32(<offset>)
    request.Offset = &offsetRequest
    startTimeRequest := int64(<start_time>)
    request.StartTime = &startTimeRequest
    endTimeRequest := int64(<end_time>)
    request.EndTime = &endTimeRequest
    response, err := client.ListAppChangeHistories(request)
```

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

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de informações do histórico de alterações do aplicativo

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.1.13 Obtenção dos registros de alterações históricas de itens iniciados automaticamente

#### Função

Essa API é usada para obter os registros de alterações históricas dos itens de inicialização automática.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/asset/auto-launch/change-history

**Tabela 3-60** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-61** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
host_id	Não	String	ID de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
host_ip	Não	String	Endereço IP do servidor Mínimo: <b>0</b> Máximo: <b>128</b>
host_name	Não	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
auto_launch_name	Não	String	Nome do item iniciado automaticamente Mínimo: <b>0</b> Máximo: <b>128</b>
type	Não	Integer	Tipo de item iniciado automaticamente. <ul style="list-style-type: none"><li>● 0: serviço iniciado automaticamente</li><li>● 1: tarefa agendada</li><li>● 2: pré-carregar a biblioteca dinâmica.</li><li>● 3: executar chave de registro</li><li>● 4: pasta de inicialização</li></ul> Mínimo: <b>0</b> Máximo: <b>100</b>
variation_type	Não	String	Tipo de alteração. Seu valor pode ser: <ul style="list-style-type: none"><li>● add</li><li>● delete</li><li>● modify</li></ul> Mínimo: <b>0</b> Máximo: <b>10</b>
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>256</b>

Parâmetro	Obrigatório	Tipo	Descrição
sort_key	Não	String	Chave de classificação. Atualmente, a classificação por recent_scan_time é suportada. Mínimo: <b>0</b> Máximo: <b>128</b>
sort_dir	Não	String	Modo de classificação. O valor padrão é decrescente. <ul style="list-style-type: none"> <li>● <b>asc</b>: ordem crescente</li> <li>● <b>desc</b>: ordem decrescente</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
start_time	Não	Long	Hora de início de uma mudança. Seu valor é um carimbo de data/hora de 13 dígitos. Mínimo: <b>0</b> Máximo: <b>9007199254740992</b>
end_time	Não	Long	Hora de término de uma alteração. Seu valor é um carimbo de data/hora de 13 dígitos. Mínimo: <b>0</b> Máximo: <b>9007199254740992</b>

## Parâmetros de solicitação

**Tabela 3-62** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>32</b> Máximo: <b>4096</b>

## Parâmetros de resposta

**Código de status: 200****Tabela 3-63** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número de alterações de itens iniciados automaticamente Mínimo: <b>0</b> Máximo: <b>10000</b>
data_list	Array of <b>AutoLaunchChangeResponseInfo</b> objects	Histórico de alterações da conta Comprimento da matriz: <b>0–10000</b>

**Tabela 3-64** AutoLaunchChangeResponseInfo

Parâmetro	Tipo	Descrição
agent_id	String	ID do agente Mínimo: <b>0</b> Máximo: <b>128</b>

Parâmetro	Tipo	Descrição
variation_type	String	Tipo de alteração. <ul style="list-style-type: none"><li>● add</li><li>● delete</li><li>● modify</li></ul> Mínimo: <b>0</b> Máximo: <b>10</b>
type	Integer	Tipo de item iniciado automaticamente <ul style="list-style-type: none"><li>● 0: serviço iniciado automaticamente</li><li>● 1: tarefa agendada</li><li>● 2: pré-carregar biblioteca dinâmica</li><li>● 3: executar chave de registro</li><li>● 4: pasta de inicialização</li></ul> Mínimo: <b>0</b> Máximo: <b>11</b>
host_id	String	host_id Mínimo: <b>1</b> Máximo: <b>128</b>
host_name	String	Nome do ECS Mínimo: <b>1</b> Máximo: <b>256</b>
host_ip	String	Endereço IP do servidor Mínimo: <b>1</b> Máximo: <b>256</b>
path	String	Caminho do item de inicialização automática Mínimo: <b>1</b> Máximo: <b>256</b>
hash	String	Valor de hash do arquivo gerado usando o algoritmo SHA256 Mínimo: <b>1</b> Máximo: <b>128</b>
run_user	String	Usuário que inicia a execução Mínimo: <b>1</b> Máximo: <b>64</b>
name	String	Nome do item iniciado automaticamente Mínimo: <b>1</b> Máximo: <b>256</b>



Parâmetro	Tipo	Descrição
recent_scan_time	Long	Hora da última atualização. O valor é um carimbo de data/hora de 13 bits. Mínimo: <b>0</b> Máximo: <b>4824430336000</b>

## Exemplo de solicitações

Os primeiros 10 registros de alteração de item de inicialização automática cuja hora de início é 1693101881568 e hora de término é 1701050681569 são consultados por padrão.

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

## Exemplo de respostas

**Código de status: 200**

Lista de informações do histórico de alterações do aplicativo

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" :
"d83c7be8a106485a558f97446617443b87604c8116e3cf0453c2a44exxxxxxxx",
    "variation_type" : "add",
    "type" : 0,
    "host_id" : "host_id",
    "host_name" : "host_name",
    "host_ip" : "host_ip",
    "path" : "/path",
    "hash" : "xxxxxxxx227bffa0c04425ba6c8e0024046caa38dfbca6281b40109xxxxxxxx",
    "run_user" : "SYSTEM",
    "name" : "S12hostguard",
    "recent_scan_time" : 1668246126302
  } ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListAutoLaunchChangeHistoriesSolution {

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

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

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

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

ListAutoLaunchChangeHistoriesRequest request = new
ListAutoLaunchChangeHistoriesRequest();
request.withHostId("<host_id>");
request.withHostIp("<host_ip>");
request.withHostName("<host_name>");
request.withAutoLaunchName("<auto_launch_name>");
request.withType(<type>);
request.withVariationType("<variation_type>");
request.withEnterpriseProjectId("<enterprise_project_id>");
request.withSortKey("<sort_key>");
request.withSortDir("<sort_dir>");
request.withLimit(<limit>);
request.withOffset(<offset>);
request.withStartTime(<start_time>L);
request.withEndTime(<end_time>L);
try {
    ListAutoLaunchChangeHistoriesResponse response =
client.listAutoLaunchChangeHistories(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

```
# coding: utf-8

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

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

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

credentials = BasicCredentials(ak, sk) \

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

try:
    request = ListAutoLaunchChangeHistoriesRequest()
    request.host_id = "<host_id>"
    request.host_ip = "<host_ip>"
    request.host_name = "<host_name>"
    request.auto_launch_name = "<auto_launch_name>"
    request.type = <type>
    request.variation_type = "<variation_type>"
    request.enterprise_project_id = "<enterprise_project_id>"
    request.sort_key = "<sort_key>"
    request.sort_dir = "<sort_dir>"
    request.limit = <limit>
    request.offset = <offset>
    request.start_time = <start_time>
    request.end_time = <end_time>
    response = client.list_auto_launch_change_histories(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ListAutoLaunchChangeHistoriesRequest{}
    hostIdRequest := "<host_id>"
    request.HostId = &hostIdRequest
```

```
hostIpRequest:= "<host_ip>"
request.HostIp = &hostIpRequest
hostNameRequest:= "<host_name>"
request.HostName = &hostNameRequest
autoLaunchNameRequest:= "<auto_launch_name>"
request.AutoLaunchName = &autoLaunchNameRequest
typeRequest:= int32(<type>)
request.Type = &typeRequest
variationTypeRequest:= "<variation_type>"
request.VariationType = &variationTypeRequest
enterpriseProjectIdRequest:= "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
sortKeyRequest:= "<sort_key>"
request.SortKey = &sortKeyRequest
sortDirRequest:= "<sort_dir>"
request.SortDir = &sortDirRequest
limitRequest:= int32(<limit>)
request.Limit = &limitRequest
offsetRequest:= int32(<offset>)
request.Offset = &offsetRequest
startTimeRequest:= int64(<start_time>)
request.StartTime = &startTimeRequest
endTimeRequest:= int64(<end_time>)
request.EndTime = &endTimeRequest
response, err := client.ListAutoLaunchChangeHistories(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de informações do histórico de alterações do aplicativo

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.1.14 Impressões digitais de ativos - Processo - Lista de servidores

### Função

Servidores ou containers com o processo

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

## URI

GET /v5/{project\_id}/asset/processes/detail

**Tabela 3-65** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-66** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>1</b> Máximo: <b>256</b>
host_name	Não	String	Nome de servidor Mínimo: <b>1</b> Máximo: <b>256</b>
host_ip	Não	String	Endereço IP do servidor Mínimo: <b>1</b> Máximo: <b>256</b>
path	Não	String	Caminho do arquivo de execução do processo. Mínimo: <b>1</b> Máximo: <b>256</b>
category	Não	String	Tipo. O valor padrão é host. As opções são as seguintes: <ul style="list-style-type: none"><li>● host</li><li>● container</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>

Parâmetro	Obrigatório	Tipo	Descrição
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>10</b> Máximo: <b>100</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>

## Parâmetros de solicitação

**Tabela 3-67** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>32</b> Máximo: <b>4096</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-68** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total de estatísticas do servidor Mínimo: <b>0</b> Máximo: <b>10000</b>

Parâmetro	Tipo	Descrição
data_list	Array of <a href="#">ProcessesHostResponseInfo</a> objects	Lista de estatísticas do servidor Comprimento da matriz: <b>0–10000</b>

**Tabela 3-69** ProcessesHostResponseInfo

Parâmetro	Tipo	Descrição
hash	String	O valor de SHA256 do caminho. Mínimo: <b>1</b> Máximo: <b>256</b>
host_ip	String	Endereço IP do servidor Mínimo: <b>1</b> Máximo: <b>256</b>
host_name	String	Nome de servidor Mínimo: <b>1</b> Máximo: <b>256</b>
launch_params	String	Parâmetro de inicialização Mínimo: <b>1</b> Máximo: <b>256</b>
launch_time	Long	Hora de início Mínimo: <b>0</b> Máximo: <b>4070880000000</b>
process_path	String	Caminho do arquivo executável do processo Mínimo: <b>1</b> Máximo: <b>256</b>
process_pid	Integer	PID do processo Mínimo: <b>0</b> Máximo: <b>65535</b>
run_permission	String	Permissão de arquivo Mínimo: <b>1</b> Máximo: <b>256</b>
container_id	String	ID do container Mínimo: <b>1</b> Máximo: <b>128</b>

Parâmetro	Tipo	Descrição
container_name	String	Nome do container Mínimo: 1 Máximo: 256

## Exemplo de solicitações

Os primeiros 10 servidores cujo caminho do processo é /usr/bin/bash são consultados por padrão.

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

## Exemplo de respostas

**Código de status: 200**

Servidores com o processo

```
{
  "total_num" : 1,
  "data_list" : [ {
    "hash" : "xxxxxx96a7ceb67731c0158xxxxxxff8456914d8275d221671d1190e888xxxxx",
    "host_ip" : "192.168.0.1",
    "host_name" : "ecs-euler-z00800211",
    "launch_params" : "",
    "launch_time" : 1673504622000,
    "process_path" : "/CloudResetPwdUpdateAgent/bin/wrapper",
    "process_pid" : 888,
    "run_permission" : "rwx-----",
    "container_id" :
"ce794b8a6071f5fd7e4d142dab7b36bedf2c7a4f6083fb82e5bbc82709b50018",
    "container_name" : "hss_imagescan_W73V1W06"
  } ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListProcessesHostSolution {

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



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

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

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

ListProcessesHostRequest request = new ListProcessesHostRequest();
request.withEnterpriseProjectId("<enterprise_project_id>");
request.withHostName("<host_name>");
request.withHostIp("<host_ip>");
request.withPath("<path>");
request.withCategory("<category>");
request.withLimit(<limit>);
request.withOffset(<offset>);
try {
    ListProcessesHostResponse response =
client.listProcessesHost(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
```

```
request = ListProcessesHostRequest()
request.enterprise_project_id = "<enterprise_project_id>"
request.host_name = "<host_name>"
request.host_ip = "<host_ip>"
request.path = "<path>"
request.category = "<category>"
request.limit = <limit>
request.offset = <offset>
response = client.list_processes_host(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ListProcessesHostRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        hostNameRequest:= "<host_name>"
        request.HostName = &hostNameRequest
        hostIpRequest:= "<host_ip>"
        request.HostIp = &hostIpRequest
        pathRequest:= "<path>"
        request.Path = &pathRequest
        categoryRequest:= "<category>"
        request.Category = &categoryRequest
        limitRequest:= int32(<limit>)
        request.Limit = &limitRequest
        offsetRequest:= int32(<offset>)
        request.Offset = &offsetRequest
        response, err := client.ListProcessesHost(request)
        if err == nil {
            fmt.Printf("%+v\n", response)
        } else {
```

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

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Servidores com o processo

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.1.15 Impressões digitais de ativos - Porta - Lista de servidores

#### Função

Servidores ou containers com a porta

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/asset/ports/detail

**Tabela 3-70** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-71** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>1</b> Máximo: <b>256</b>
host_name	Não	String	Nome de servidor Mínimo: <b>1</b> Máximo: <b>256</b>
host_ip	Não	String	Endereço IP do servidor Mínimo: <b>1</b> Máximo: <b>256</b>
port	Sim	Integer	Número da porta Mínimo: <b>1</b> Máximo: <b>65535</b>
type	Não	String	Tipo da porta: TCP ou UDP. Mínimo: <b>1</b> Máximo: <b>256</b>
category	Não	String	Tipo. O valor padrão é host. As opções são as seguintes: <ul style="list-style-type: none"><li>● host</li><li>● container</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>10</b> Máximo: <b>100</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>10000</b> Padrão: <b>0</b>

## Parâmetros de solicitação

**Tabela 3-72** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>32</b> Máximo: <b>4096</b>

## Parâmetros de resposta

**Código de status: 200****Tabela 3-73** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Total de servidores Mínimo: <b>0</b> Máximo: <b>10000</b>
data_list	Array of <b>PortHostResponseInfo</b> objects	Lista de informações do servidor Comprimento da matriz: <b>0-10000</b>

**Tabela 3-74** PortHostResponseInfo

Parâmetro	Tipo	Descrição
container_id	String	ID da imagem Mínimo: <b>1</b> Máximo: <b>256</b>
host_id	String	ID de servidor Mínimo: <b>1</b> Máximo: <b>256</b>
host_ip	String	Endereço IP do servidor Mínimo: <b>1</b> Máximo: <b>256</b>

Parâmetro	Tipo	Descrição
host_name	String	Nome de servidor Mínimo: <b>1</b> Máximo: <b>256</b>
laddr	String	Endereço IP de escuta Mínimo: <b>1</b> Máximo: <b>256</b>
path	String	Caminho do arquivo de execução do processo. Mínimo: <b>1</b> Máximo: <b>256</b>
pid	Integer	pid Mínimo: <b>0</b> Máximo: <b>100000</b>
port	Integer	Porta Mínimo: <b>0</b> Máximo: <b>65535</b>
status	String	Status Mínimo: <b>1</b> Máximo: <b>256</b>
type	String	Tipo da porta: TCP ou UDP. Mínimo: <b>1</b> Máximo: <b>256</b>
container_name	String	Nome do container Mínimo: <b>1</b> Máximo: <b>256</b>
agent_id	String	ID do agente Mínimo: <b>1</b> Máximo: <b>128</b>

## Exemplo de solicitações

Os primeiros 10 servidores cujo número de porta é 22 são consultados por padrão.

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

## Exemplo de respostas

**Código de status: 200**

Servidores com a porta

```
{
  "total_num" : 1,
  "data_list" : [ {
    "host_id" : "03117200-xxxx-xxxx-xxxx-a89a10e66dbe",
    "host_ip" : "192.168.0.1",
    "host_name" : "ecs-eule",
    "laddr" : "0.0.0.0",
    "path" : "C:\\Windows\\system32\\svchost.exe",
    "port" : 888,
    "status" : "unknow",
    "type" : "UDP",
    "container_id" : "ce794b8a6-xxxx-xxxx-xxxx-36bedf2c7a4f6083fb82e5bbc82709b50018",
    "container_name" : "hss_imagescan_W73V1W06",
    "agent_id" : "03jjj-xxxx-xxxx-wwwsedf"
  } ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListPortHostSolution {

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

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

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

        ListPortHostRequest request = new ListPortHostRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withHostName("<host_name>");
        request.withHostIp("<host_ip>");
        request.withPort("<port>");
        request.withType("<type>");
        request.withCategory("<category>");
        request.withLimit("<limit>");
        request.withOffset("<offset>");
        try {
            ListPortHostResponse response = client.listPortHost(request);
        }
    }
}
```

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

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListPortHostRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.host_name = "<host_name>"
        request.host_ip = "<host_ip>"
        request.port = <port>
        request.type = "<type>"
        request.category = "<category>"
        request.limit = <limit>
        request.offset = <offset>
        response = client.list_port_host(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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



```
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

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

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

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

    request := &model.ListPortHostRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        hostNameRequest:= "<host_name>"
        request.HostName = &hostNameRequest
        hostIpRequest:= "<host_ip>"
        request.HostIp = &hostIpRequest
        request.Port = int32(<port>)
        typeRequest:= "<type>"
        request.Type = &typeRequest
        categoryRequest:= "<category>"
        request.Category = &categoryRequest
        limitRequest:= int32(<limit>)
        request.Limit = &limitRequest
        offsetRequest:= int32(<offset>)
        request.Offset = &offsetRequest
        response, err := client.ListPortHost(request)
        if err == nil {
            fmt.Printf("%+v\n", response)
        } else {
            fmt.Println(err)
        }
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Servidores com a porta

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.1.16 Consulta da lista de middleware

#### Função

Essa API é usada para consultar a lista de middleware. A lista de servidores pode ser consultada pelo nome do middleware.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/asset/midwares

Tabela 3-75 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>20</b> Máximo: <b>64</b>

Tabela 3-76 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>64</b>
file_name	Não	String	Nome do arquivo JAR Mínimo: <b>0</b> Máximo: <b>256</b>
category	Não	String	Tipo. Seu valor pode ser: ● host ● container Mínimo: <b>0</b> Máximo: <b>64</b>

Parâmetro	Obrigatório	Tipo	Descrição
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>

## Parâmetros de solicitação

**Tabela 3-77** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token de usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>32</b> Máximo: <b>2097152</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-78** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total de pacotes JAR Mínimo: <b>0</b> Máximo: <b>10000</b>

Parâmetro	Tipo	Descrição
data_list	Array of <a href="#">JarPackageStatisticsResponseInfo</a> objects	Lista de estatísticas de pacote JAR Comprimento da matriz: <b>0–300000</b>

**Tabela 3-79** JarPackageStatisticsResponseInfo

Parâmetro	Tipo	Descrição
file_name	String	Nome do arquivo JAR Mínimo: <b>0</b> Máximo: <b>256</b>
num	Integer	Número total de pacotes JAR Mínimo: <b>0</b> Máximo: <b>300000</b>

## Exemplo de solicitações

Os primeiros 10 registros de middleware cujo nome é rt.jar e o tipo é host são consultados por padrão.

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

## Exemplo de respostas

**Código de status: 200**

Estatísticas de JarPackage

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
```

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

public class ListJarPackageStatisticsSolution {

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

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

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

        ListJarPackageStatisticsRequest request = new
ListJarPackageStatisticsRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withFileName("<file_name>");
        request.withCategory("<category>");
        request.withLimit(<limit>);
        request.withOffset(<offset>);
        try {
            ListJarPackageStatisticsResponse response =
client.listJarPackageStatistics(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

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

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

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

credentials = BasicCredentials(ak, sk) \

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

try:
    request = ListJarPackageStatisticsRequest()
    request.enterprise_project_id = "<enterprise_project_id>"
    request.file_name = "<file_name>"
    request.category = "<category>"
    request.limit = <limit>
    request.offset = <offset>
    response = client.list_jar_package_statistics(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ListJarPackageStatisticsRequest{}
    enterpriseProjectIdRequest := "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    fileNameRequest := "<file_name>"
    request.FileName = &fileNameRequest
    categoryRequest := "<category>"
    request.Category = &categoryRequest
    limitRequest := int32(<limit>)
    request.Limit = &limitRequest
    offsetRequest := int32(<offset>)
    request.Offset = &offsetRequest
```

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

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Estatísticas de JarPackage

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.1.17 Consulta da lista de servidores de um middleware específico

### Função

Essa API é usada para consultar a lista de servidores de um middleware especificado. Você pode consultar a lista de servidores de middleware pelo seu nome de middleware.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/asset/midwares/detail

Tabela 3-80 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>20</b> Máximo: <b>64</b>

**Tabela 3-81** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>64</b>
file_name	Sim	String	Nome do arquivo Mínimo: <b>1</b> Máximo: <b>256</b>
category	Não	String	Tipo. Seu valor pode ser: <ul style="list-style-type: none"><li>● host</li><li>● container</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>
host_name	Não	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>64</b>
host_ip	Não	String	Endereço IP do servidor Mínimo: <b>0</b> Máximo: <b>64</b>
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>10</b> Máximo: <b>100</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>300000</b> Padrão: <b>0</b>
part_match	Não	Boolean	Se a correspondência difusa é usada. O valor padrão é false.



## Parâmetros de solicitação

**Tabela 3-82** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token de usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token.  Mínimo: <b>32</b> Máximo: <b>2097152</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-83** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Total Mínimo: <b>0</b> Máximo: <b>10000</b>
data_list	Array of <b>JarPackageHostInfo</b> objects	Lista de servidores Comprimento da matriz: <b>0-10000</b>

**Tabela 3-84** JarPackageHostInfo

Parâmetro	Tipo	Descrição
agent_id	String	agent_id Mínimo: <b>1</b> Máximo: <b>64</b>
host_id	String	ID de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
host_name	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>256</b>

Parâmetro	Tipo	Descrição
host_ip	String	Endereço IP do servidor Mínimo: <b>0</b> Máximo: <b>128</b>
file_name	String	Nome do pacote JAR Mínimo: <b>0</b> Máximo: <b>256</b>
name	String	Nome do pacote JAR (sem sufixo) Mínimo: <b>0</b> Máximo: <b>256</b>
catalogue	String	Tipo de pacote JAR Mínimo: <b>0</b> Máximo: <b>32</b>
file_type	String	Sufixo do pacote JAR Mínimo: <b>0</b> Máximo: <b>32</b>
version	String	Versão do pacote JAR Mínimo: <b>0</b> Máximo: <b>64</b>
path	String	Caminho do pacote JAR Mínimo: <b>0</b> Máximo: <b>512</b>
hash	String	Hash do pacote JAR Mínimo: <b>0</b> Máximo: <b>512</b>
size	Integer	Tamanho do pacote JAR Mínimo: <b>0</b> Máximo: <b>2147483647</b>
uid	Integer	UID Mínimo: <b>0</b> Máximo: <b>2147483647</b>
gid	Integer	gid Mínimo: <b>0</b> Máximo: <b>2147483647</b>

Parâmetro	Tipo	Descrição
mode	String	Permissões de arquivo Mínimo: <b>0</b> Máximo: <b>32</b>
pid	Integer	ID do processo Mínimo: <b>0</b> Máximo: <b>2147483647</b>
proc_path	String	Caminho do arquivo executável do processo Mínimo: <b>0</b> Máximo: <b>1024</b>
container_id	String	ID da instância de container Mínimo: <b>0</b> Máximo: <b>128</b>
container_name	String	Nome do container Mínimo: <b>0</b> Máximo: <b>256</b>
package_path	String	Caminho do pacote Mínimo: <b>0</b> Máximo: <b>1024</b>
is_embedded	Integer	Se deve exibir um pacote aninhado Mínimo: <b>0</b> Máximo: <b>2147483647</b>
record_time	Long	Tempo de verificação Mínimo: <b>0</b> Máximo: <b>4070880000000</b>

## Exemplo de solicitações

Os primeiros 10 servidores cujo nome de middleware é log4j-core-2.8.2.jar e o tipo é host são consultados por padrão.

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

## Exemplo de respostas

**Código de status: 200**

ListJarPackageHostInfo

```
{  
  "data_list" : [ {
```

```
"agent_id" :
"2d0fe7824005bf001220ad9d892e86f8af44a7d3608dab11165008ce439d3583",
"catalogue" : "util",
"container_id" : "",
"file_name" : "rt.jar",
"file_type" : "jar",
"gid" : 0,
"hash" : "04bf14e3b1da55d95561ca78cb29caa909410051dbe047e91ad6f5c1dedb8d6d",
"host_id" : "103ed820-62e5-4754-b0f8-3e47b6dd49d2",
"host_ip" : "192.168.1.76",
"host_name" : "Do not delete the test.",
"mode" : "-rw-----",
"name" : "Java Runtime Environment",
"path" : "/CloudResetPwdUpdateAgent/depend/jre/lib/rt.jar",
"pid" : 1614,
"proc_path" : "/CloudResetPwdUpdateAgent/depend/jre/bin/java",
"record_time" : 1690513169986,
"uid" : 0,
"version" : "1.8.0_252",
"size" : 128,
"container_name" : "aaaa",
"package_path" : "/CloudResetPwdUpdateAgent/depend/jre/bin/java",
"is_embedded" : 0
} ],
"total_num" : 1
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListJarPackageHostInfoSolution {

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

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

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

```
request.withEnterpriseProjectId("<enterprise_project_id>");
request.withFileName("<file_name>");
request.withCategory("<category>");
request.withHostName("<host_name>");
request.withHostIp("<host_ip>");
request.withLimit(<limit>);
request.withOffset(<offset>);
request.withPartMatch(<part_match>);
try {
    ListJarPackageHostInfoResponse response =
client.listJarPackageHostInfo(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListJarPackageHostInfoRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.file_name = "<file_name>"
        request.category = "<category>"
        request.host_name = "<host_name>"
        request.host_ip = "<host_ip>"
        request.limit = <limit>
        request.offset = <offset>
        request.part_match = <PartMatch>
        response = client.list_jar_package_host_info(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
```

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

## Go

```
package main

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

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

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

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

    request := &model.ListJarPackageHostInfoRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        request.FileName = "<file_name>"
        categoryRequest:= "<category>"
        request.Category = &categoryRequest
        hostNameRequest:= "<host_name>"
        request.HostName = &hostNameRequest
        hostIpRequest:= "<host_ip>"
        request.HostIp = &hostIpRequest
        limitRequest:= int32(<limit>)
        request.Limit = &limitRequest
        offsetRequest:= int32(<offset>)
        request.Offset = &offsetRequest
        partMatchRequest:= <part_match>
        request.PartMatch = &partMatchRequest
        response, err := client.ListJarPackageHostInfo(request)
        if err == nil {
            fmt.Printf("%+v\n", response)
        } else {
            fmt.Println(err)
        }
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	ListJarPackageHostInfo

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.2 Prevenção contra ransomware

### 3.2.1 Consulta dos servidores protegidos contra ransomware

#### Função

Essa API é usada para consultar a lista de servidores protegidos contra ransomware. Essa API precisa ser usada em conjunto com o Cloud Backup and Recovery (CBR). Certifique-se de que o site tenha CBR antes de usar APIs relacionadas a ransomware.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/ransomware/server

Tabela 3-85 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-86** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é <b>0</b> . Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
limit	Não	Integer	Número de registros exibidos em cada página. Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>
host_name	Não	String	Nome de servidor
os_type	Não	String	Tipo de SO. Seu valor pode ser: <ul style="list-style-type: none"><li>● Linux</li><li>● Windows</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>
host_ip	Não	String	Endereço IP do servidor Mínimo: <b>0</b> Máximo: <b>256</b>
host_status	Não	String	Status do servidor. Seu valor pode ser: <ul style="list-style-type: none"><li>● Se nenhum parâmetro for transferido, ele indicará todos os itens.<ul style="list-style-type: none"><li>– ACTIVE</li><li>– SHUTOFF</li></ul></li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>



Parâmetro	Obrigatório	Tipo	Descrição
last_days	Não	Integer	Número de dias no intervalo de tempo de consulta. Para consultar registros nos últimos sete dias, defina last_days=7. Se esse parâmetro não for especificado, os eventos e backups existentes no último dia serão consultados por padrão. Mínimo: <b>1</b> Máximo: <b>30</b>

## Parâmetros de solicitação

**Tabela 3-87** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-88** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total Mínimo: <b>0</b> Máximo: <b>2097152</b>

Parâmetro	Tipo	Descrição
data_list	Array of <b>ProtectionServerInfo</b> objects	Consultar os servidores protegidos contra ransomware. Comprimento da matriz: <b>0-10241</b>

**Tabela 3-89** ProtectionServerInfo

Parâmetro	Tipo	Descrição
host_id	String	ID de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
agent_id	String	ID do agente Mínimo: <b>0</b> Máximo: <b>128</b>
host_name	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
host_ip	String	EIP Mínimo: <b>0</b> Máximo: <b>128</b>
private_ip	String	Endereço IP privado Mínimo: <b>0</b> Máximo: <b>128</b>
os_type	String	Tipo de SO. Seu valor pode ser: <ul style="list-style-type: none"><li>● Linux</li><li>● Windows</li></ul> Mínimo: <b>0</b> Máximo: <b>128</b>
os_name	String	Nome de SO Mínimo: <b>0</b> Máximo: <b>128</b>
host_status	String	Status do servidor. As opções são as seguintes: <ul style="list-style-type: none"><li>● ACTIVE</li><li>● SHUTOFF</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>

Parâmetro	Tipo	Descrição
ransom_protection_status	String	Status de proteção contra ransomware. As opções são as seguintes: <ul style="list-style-type: none"> <li>● closed</li> <li>● opened</li> <li>● opening: a função está sendo ativada.</li> <li>● closing: a função está sendo desativada.</li> </ul> Mínimo: <b>0</b> Máximo: <b>128</b>
agent_version	String	Versão do agente Mínimo: <b>1</b> Máximo: <b>128</b>
protect_status	String	Status de proteção. Seu valor pode ser: <ul style="list-style-type: none"> <li>● closed</li> <li>● opened: proteção ativada</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>
group_id	String	ID do grupo de servidores Mínimo: <b>1</b> Máximo: <b>128</b>
group_name	String	Nome do grupo de servidores Mínimo: <b>1</b> Máximo: <b>128</b>
protect_policy_id	String	ID da política Mínimo: <b>1</b> Máximo: <b>128</b>
protect_policy_name	String	Nome da política de proteção Mínimo: <b>1</b> Máximo: <b>128</b>
backup_error	<b>backup_error</b> object	Mensagem de erro de backup
backup_protection_status	String	Se deve ativar o backup. As opções são as seguintes: <ul style="list-style-type: none"> <li>● failed_to_turn_on_backup: o backup não pode ser ativado.</li> <li>● closed</li> <li>● opened</li> </ul> Mínimo: <b>0</b> Máximo: <b>128</b>

Parâmetro	Tipo	Descrição
count_protect_event	Integer	Número de eventos de proteção Mínimo: <b>0</b> Máximo: <b>2097152</b>
count_backuped	Integer	Backups existentes Mínimo: <b>0</b> Máximo: <b>2097152</b>
agent_status	String	Status do agente Mínimo: <b>1</b> Máximo: <b>128</b>
version	String	Edição do HSS. Seu valor pode ser: <ul style="list-style-type: none"> <li>● hss.version.null</li> <li>● hss.version.basic: edição básica</li> <li>● hss.version.advanced: edição profissional</li> <li>● hss.version.enterprise: edição empresarial</li> <li>● hss.version.premium: edição premium</li> <li>● hss.version.wtp: edição WTP</li> <li>● hss.version.container.enterprise: edição de container</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>
host_source	String	Indica o tipo de servidor. As opções são as seguintes: <ul style="list-style-type: none"> <li>● ecs</li> <li>● outside: servidores locais</li> <li>● workspace: área de trabalho na nuvem</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>
vault_id	String	ID do cofre Mínimo: <b>0</b> Máximo: <b>128</b>
vault_name	String	Nome do cofre Mínimo: <b>0</b> Máximo: <b>128</b>
vault_size	Integer	Capacidade total, em GB. Mínimo: <b>0</b> Máximo: <b>2097152</b>

Parâmetro	Tipo	Descrição
vault_used	Integer	Capacidade usada, em MB. Mínimo: <b>0</b> Máximo: <b>2097152</b>
vault_allocated	Integer	Capacidade alocada do servidor vinculado, em GB. Mínimo: <b>0</b> Máximo: <b>2097152</b>
vault_charging_mode	String	Modo de repositório, o valor pode ser post_paid (pagamento por uso) ou pre_paid. Mínimo: <b>0</b> Máximo: <b>128</b>
vault_status	String	O status do cofre pode ser: <ul style="list-style-type: none"><li>● available</li><li>● lock</li><li>● frozen</li><li>● deleting</li><li>● error</li></ul> Mínimo: <b>0</b> Máximo: <b>128</b>
backup_policy_id	String	Especifica o ID da política de backup. Se esse parâmetro estiver vazio, a política de backup não será vinculada. Se esse parâmetro não estiver vazio, verifique se a política de backup está ativada com base no campo backup_policy_enabled. Mínimo: <b>1</b> Máximo: <b>128</b>
backup_policy_name	String	Nome da política de backup Mínimo: <b>1</b> Máximo: <b>128</b>
backup_policy_enabled	Boolean	Se a política está ativada
resources_num	Integer	Servidores vinculados Mínimo: <b>0</b> Máximo: <b>2097152</b>

Tabela 3-90 backup\_error

Parâmetro	Tipo	Descrição
error_code	Integer	Código de erro. As opções são as seguintes: <ul style="list-style-type: none"><li>● 0: nenhuma informação de erro.</li><li>● 1: o backup não pode ser ativado porque outro cofre foi vinculado.</li><li>● 2: o número de cofres de backup excede o limite superior.</li><li>● 3: uma exceção ocorre quando a API do CBR é chamada.</li></ul> Mínimo: <b>0</b> Máximo: <b>128</b>
error_description	String	Descrição do erro Mínimo: <b>1</b> Máximo: <b>128</b>

## Exemplo de solicitações

Consultar a lista de servidores de proteção contra ransomware. Se o parâmetro limit não for definido, 10 registros serão retornados por padrão.

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

## Exemplo de respostas

### Código de status: 200

Lista de servidores protegidos contra ransomware

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

```
"protect_policy_name" : "tst",  
"protect_status" : "opened"  
} ]  
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;  
import com.huaweicloud.sdk.hss.v5.region.HssRegion;  
import com.huaweicloud.sdk.hss.v5.*;  
import com.huaweicloud.sdk.hss.v5.model.*;  
  
public class ListProtectionServerSolution {  
  
    public static void main(String[] args) {  
        // The AK and SK used for authentication are hard-coded or stored in  
plaintext, which has great security risks. It is recommended that the AK and SK  
be stored in ciphertext in configuration files or environment variables and  
decrypted during use to ensure security.  
        // In this example, AK and SK are stored in environment variables for  
authentication. Before running this example, set environment variables  
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
        String ak = System.getenv("CLOUD_SDK_AK");  
        String sk = System.getenv("CLOUD_SDK_SK");  
  
        ICredential auth = new BasicCredentials()  
            .withAk(ak)  
            .withSk(sk);  
  
        HssClient client = HssClient.newBuilder()  
            .withCredential(auth)  
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))  
            .build();  
  
        ListProtectionServerRequest request = new ListProtectionServerRequest();  
        request.withEnterpriseProjectId("<enterprise_project_id>");  
        request.withOffset("<offset>");  
        request.withLimit("<limit>");  
        request.withHostName("<host_name>");  
        request.withOsType("<os_type>");  
        request.withHostIp("<host_ip>");  
        request.withHostStatus("<host_status>");  
        request.withLastDays("<last_days>");  
        try {  
            ListProtectionServerResponse response =  
client.listProtectionServer(request);  
            System.out.println(response.toString());  
        } catch (ConnectionException e) {  
            e.printStackTrace();  
        } catch (RequestTimeoutException e) {  
            e.printStackTrace();  
        } catch (ServiceResponseException e) {  
            e.printStackTrace();  
            System.out.println(e.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 huaweicloudsdkhss.v5.region.hss_region import HssRegion  
from huaweicloudsdkcore.exceptions import exceptions  
from huaweicloudsdkhss.v5 import *  
  
if __name__ == "__main__":  
    # The AK and SK used for authentication are hard-coded or stored in  
    plaintext, which has great security risks. It is recommended that the AK and SK  
    be stored in ciphertext in configuration files or environment variables and  
    decrypted during use to ensure security.  
    # In this example, AK and SK are stored in environment variables for  
    authentication. Before running this example, set environment variables  
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak = __import__('os').getenv("CLOUD_SDK_AK")  
    sk = __import__('os').getenv("CLOUD_SDK_SK")  
  
    credentials = BasicCredentials(ak, sk) \  
  
    client = HssClient.new_builder() \  
        .with_credentials(credentials) \  
        .with_region(HssRegion.value_of("<YOUR REGION>")) \  
        .build()  
  
    try:  
        request = ListProtectionServerRequest()  
        request.enterprise_project_id = "<enterprise_project_id>"  
        request.offset = <offset>  
        request.limit = <limit>  
        request.host_name = "<host_name>"  
        request.os_type = "<os_type>"  
        request.host_ip = "<host_ip>"  
        request.host_status = "<host_status>"  
        request.last_days = <last_days>  
        response = client.list_protection_server(request)  
        print(response)  
    except exceptions.ClientRequestException as e:  
        print(e.status_code)  
        print(e.request_id)  
        print(e.error_code)  
        print(e.error_msg)
```

## Go

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in  
    plaintext, which has great security risks. It is recommended that the AK and SK  
    be stored in ciphertext in configuration files or environment variables and  
    decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for  
    authentication. Before running this example, set environment variables  
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")
```



```
sk := os.Getenv("CLOUD_SDK_SK")

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

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

request := &model.ListProtectionServerRequest{
    enterpriseProjectIdRequest:= "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    offsetRequest:= int32(<offset>)
    request.Offset = &offsetRequest
    limitRequest:= int32(<limit>)
    request.Limit = &limitRequest
    hostNameRequest:= "<host_name>"
    request.HostName = &hostNameRequest
    osTypeRequest:= "<os_type>"
    request.OsType = &osTypeRequest
    hostIpRequest:= "<host_ip>"
    request.HostIp = &hostIpRequest
    hostStatusRequest:= "<host_status>"
    request.HostStatus = &hostStatusRequest
    lastDaysRequest:= int32(<last_days>)
    request.LastDays = &lastDaysRequest
    response, err := client.ListProtectionServer(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia [Código de amostra no API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de servidores protegidos contra ransomware

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.2.2 Consulta da lista de políticas de proteção contra ransomware

### Função

Essa API é usada para consultar a lista de políticas de proteção contra ransomware.

## Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

## URI

GET /v5/{project\_id}/ransomware/protection/policy

**Tabela 3-91** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-92** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é <b>0</b> . Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
limit	Não	Integer	Número de registros exibidos em cada página. Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>
policy_name	Não	String	Nome da política Mínimo: <b>0</b> Máximo: <b>128</b>

Parâmetro	Obrigatório	Tipo	Descrição
protect_policy_id	Não	String	ID da política Mínimo: <b>0</b> Máximo: <b>128</b>
operating_system	Não	String	SOs suportados pela política. As opções são as seguintes: <ul style="list-style-type: none"> <li>● Windows</li> <li>● Linux</li> </ul> Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de solicitação

**Tabela 3-93** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-94** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total de políticas Mínimo: <b>0</b> Máximo: <b>2097152</b>

Parâmetro	Tipo	Descrição
data_list	Array of <b>ProtectionPolicyInfo</b> objects	Consultar a lista de políticas. Comprimento da matriz: <b>0–10241</b>

**Tabela 3-95** ProtectionPolicyInfo

Parâmetro	Tipo	Descrição
policy_id	String	ID da política Mínimo: <b>0</b> Máximo: <b>128</b>
policy_name	String	Nome da política Mínimo: <b>0</b> Máximo: <b>128</b>
protection_mode	String	Ação. Seu valor pode ser: <ul style="list-style-type: none"> <li>● alarm_and_isolation: relatar um alarme e isolar.</li> <li>● alarm_only: relatar apenas alarmes.</li> </ul> Mínimo: <b>0</b> Máximo: <b>128</b>
bait_protection_status	String	Se deve ativar a proteção de honeypot. Por padrão, a proteção está ativada. Seu valor pode ser: <ul style="list-style-type: none"> <li>● opened</li> <li>● closed</li> </ul> Mínimo: <b>0</b> Máximo: <b>128</b>
deploy_mode	String	Se deve ativar a proteção de honeypot. As opções são as seguintes. Por padrão, a proteção dinâmica de honeypot está desativada. <ul style="list-style-type: none"> <li>● opened</li> <li>● closed</li> </ul> Mínimo: <b>0</b> Máximo: <b>128</b>
protection_directory	String	Diretório protegido Mínimo: <b>1</b> Máximo: <b>128</b>

Parâmetro	Tipo	Descrição
protection_type	String	Tipo de arquivo protegido, por exemplo, .docx, .txt e .avi. Mínimo: <b>0</b> Máximo: <b>128</b>
exclude_directory	String	(Opcional) Diretório excluído Mínimo: <b>1</b> Máximo: <b>128</b>
runtime_detection_status	String	Se devem ser realizadas verificações de tempo de execução. As opções são as seguintes. Atualmente, ele só pode ser desativado. Este campo está reservado. <ul style="list-style-type: none"> <li>● opened</li> <li>● closed</li> </ul> Mínimo: <b>0</b> Máximo: <b>128</b>
runtime_detection_directory	String	Diretório a ser verificado durante a execução. Este campo está reservado. Mínimo: <b>1</b> Máximo: <b>128</b>
count_associated_server	Integer	Número de servidores vinculados Mínimo: <b>0</b> Máximo: <b>2097152</b>
operating_system	String	Tipo de SO. <ul style="list-style-type: none"> <li>● Linux</li> <li>● Windows</li> </ul> Mínimo: <b>0</b> Máximo: <b>128</b>
process_whitelist	Array of <a href="#">TrustProcessInfo</a> objects	Lista branca do processo Comprimento da matriz: <b>0–20</b>
default_policy	Integer	Indica se a política é a política padrão. As opções são as seguintes: <ul style="list-style-type: none"> <li>● 0: política não padrão</li> <li>● 1: política padrão</li> </ul> Mínimo: <b>0</b> Máximo: <b>10</b>

**Tabela 3-96** TrustProcessInfo

Parâmetro	Tipo	Descrição
path	String	Indica o caminho do processo. Mínimo: <b>0</b> Máximo: <b>128</b>
hash	String	Hash do processo Mínimo: <b>0</b> Máximo: <b>128</b>

## Exemplo de solicitações

Consultar a lista de políticas de proteção contra ransomware. Se o limite não for especificado, 10 registros serão retornados por padrão.

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

## Exemplo de respostas

**Código de status: 200**

Lista de políticas de proteção

```
{
  "total_num" : 1,
  "data_list" : [ {
    "bait_protection_status" : "opened",
    "exclude_directory" : "/opt",
    "count_associated_server" : 0,
    "operating_system" : "Linux",
    "protection_mode" : "alarm_only",
    "policy_id" : "4117d16-074b-41ae-b7d7-9cc25ee258",
    "policy_name" : "test",
    "protection_directory" : "/dd",
    "protection_type" : "docx",
    "runtime_detection_status" : "closed"
  } ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

```
public class ListProtectionPolicySolution {

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

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

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

        ListProtectionPolicyRequest request = new ListProtectionPolicyRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withOffset("<offset>");
        request.withLimit("<limit>");
        request.withPolicyName("<policy_name>");
        request.withProtectPolicyId("<protect_policy_id>");
        request.withOperatingSystem("<operating_system>");
        try {
            ListProtectionPolicyResponse response =
client.listProtectionPolicy(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

    client = HssClient.new_builder() \
```

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

try:
    request = ListProtectionPolicyRequest()
    request.enterprise_project_id = "<enterprise_project_id>"
    request.offset = <offset>
    request.limit = <limit>
    request.policy_name = "<policy_name>"
    request.protect_policy_id = "<protect_policy_id>"
    request.operating_system = "<operating_system>"
    response = client.list_protection_policy(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ListProtectionPolicyRequest{}
    enterpriseProjectIdRequest := "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    offsetRequest := int32(<offset>)
    request.Offset = &offsetRequest
    limitRequest := int32(<limit>)
    request.Limit = &limitRequest
    policyNameRequest := "<policy_name>"
    request.PolicyName = &policyNameRequest
    protectPolicyIdRequest := "<protect_policy_id>"
    request.ProtectPolicyId = &protectPolicyIdRequest
    operatingSystemRequest := "<operating_system>"
    request.OperatingSystem = &operatingSystemRequest
    response, err := client.ListProtectionPolicy(request)
    if err == nil {
```



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

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de políticas de proteção

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.2.3 Modificação das políticas de proteção contra ransomware

### Função

Essa API é usada para modificar as políticas de proteção contra ransomware.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

PUT /v5/{project\_id}/ransomware/protection/policy

**Tabela 3-97** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-98** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>

## Parâmetros de solicitação

**Tabela 3-99** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-100** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
policy_id	Sim	String	ID da política Mínimo: <b>0</b> Máximo: <b>128</b>
policy_name	Sim	String	Nome da política Mínimo: <b>0</b> Máximo: <b>128</b>

Parâmetro	Obrigatório	Tipo	Descrição
protection_mode	Sim	String	Ação. Seu valor pode ser: <ul style="list-style-type: none"> <li>● alarm_and_isolation: relatar um alarme e isolar.</li> <li>● alarm_only: relatar apenas alarmes.</li> </ul> Mínimo: <b>0</b> Máximo: <b>128</b>
bait_protection_status	Não	String	Se deve ativar a proteção de honeypot. Por padrão, a proteção está ativada. Seu valor pode ser: <ul style="list-style-type: none"> <li>● opened</li> <li>● closed</li> </ul> Mínimo: <b>0</b> Máximo: <b>128</b>
protection_directory	Sim	String	Diretório protegido. Separe vários diretórios com ponto e vírgula (;). Você pode configurar até 20 diretórios. Mínimo: <b>1</b> Máximo: <b>128</b>
protection_type	Sim	String	Tipo de arquivo protegido, por exemplo, .docx, .txt e .avi. Mínimo: <b>1</b> Máximo: <b>128</b>
exclude_directory	Não	String	(Opcional) Diretório excluído. Separe vários diretórios com ponto e vírgula (;). Você pode configurar até 20 diretórios. Mínimo: <b>1</b> Máximo: <b>128</b>
agent_id_list	Não	Array of strings	Especifica os IDs dos agentes para os quais a política de proteção contra ransomware está ativada. Mínimo: <b>1</b> Máximo: <b>128</b> Comprimento da matriz: <b>0-10000</b>

Parâmetro	Obrigatório	Tipo	Descrição
operating_system	Sim	String	SOs suportados pela política. As opções são as seguintes: <ul style="list-style-type: none"><li>● Windows</li><li>● Linux</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>
runtime_detection_status	Não	String	Se devem ser realizadas verificações de tempo de execução. As opções são as seguintes. Atualmente, ele só pode ser desativado. Este campo está reservado. <ul style="list-style-type: none"><li>● opened</li><li>● closed</li></ul> Mínimo: <b>0</b> Máximo: <b>128</b>
process_whitelist	Não	Array of <b>TrustProcessInfo</b> objects	Lista branca do processo Comprimento da matriz: <b>0–20</b>

**Tabela 3-101** TrustProcessInfo

Parâmetro	Obrigatório	Tipo	Descrição
path	Não	String	Indica o caminho do processo. Mínimo: <b>0</b> Máximo: <b>128</b>
hash	Não	String	Hash do processo Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Modificar a política de proteção contra ransomware. Definir o tipo de SO como Linux, o ID da política de proteção como 0253edfd-30e7-439d-8f3f-17c54c997064 e a ação de proteção apenas como alerta.

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

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

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

Modificar a política de proteção contra ransomware. Definir o tipo de SO como Linux, o ID da política de proteção como 0253edfd-30e7-439d-8f3f-17c54c997064 e a ação de proteção apenas como alerta.

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

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

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

public class UpdateProtectionPolicySolution {

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

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

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

        UpdateProtectionPolicyRequest request = new
        UpdateProtectionPolicyRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        UpdateProtectionPolicyInfoRequestInfo body = new
```

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

## Python

Modificar a política de proteção contra ransomware. Definir o tipo de SO como Linux, o ID da política de proteção como 0253edfd-30e7-439d-8f3f-17c54c997064 e a ação de proteção apenas como alerta.

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = UpdateProtectionPolicyRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        listAgentIdListbody = [
            ""
```

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

## Go

Modificar a política de proteção contra ransomware. Definir o tipo de SO como Linux, o ID da política de proteção como 0253edfd-30e7-439d-8f3f-17c54c997064 e a ação de proteção apenas como alerta.

```
package main

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

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

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

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

    request := &model.UpdateProtectionPolicyRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        var listAgentIdListbody = []string{
            "",
        }
    }
    runtimeDetectionStatusUpdateProtectionPolicyInfoRequestInfo:= "closed"
    excludeDirectoryUpdateProtectionPolicyInfoRequestInfo:= ""
    baitProtectionStatusUpdateProtectionPolicyInfoRequestInfo:= "opened"
```

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

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Bem-sucedido

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.2.4 Ativação da prevenção contra ransomware

### Função

Para ativar a proteção contra ransomware, certifique-se de que o CBR esteja disponível na região. A prevenção contra ransomware funciona com o CBR.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

POST /v5/{project\_id}/ransomware/protection/open



**Tabela 3-102** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-103** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>

## Parâmetros de solicitação

**Tabela 3-104** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-105** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
operating_system	Sim	String	SOs do servidor a ser protegido. As opções são as seguintes: <ul style="list-style-type: none"><li>● Windows</li><li>● Linux</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>
ransom_protection_status	Sim	String	Se a proteção contra ransomware está ativada. Seu valor pode ser: <ul style="list-style-type: none"><li>● closed</li><li>● opened. Se esse parâmetro estiver ativado, protection_policy_id ou create_protection_policy deverá ser especificado.</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>
protection_policy_id	Não	String	ID da política de proteção contra ransomware. Se você selecionar uma política existente, esse parâmetro será obrigatório. Mínimo: <b>0</b> Máximo: <b>64</b>
create_protection_policy	Não	<b>ProtectionProxyInfoRequestInfo</b> object	Crie uma política de proteção. Para uma nova política de proteção, deixe protection_policy_id em branco e especifique create_protection_policy.
backup_protection_status	Sim	String	Se deve fazer backup dos dados no servidor. Seu valor pode ser: <ul style="list-style-type: none"><li>● closed</li><li>● opened. Se o backup do servidor estiver ativado, backup_cycle será obrigatório.</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>
backup_resources	Não	<b>BackupResources</b> object	Este parâmetro é obrigatório quando a função de backup está ativada. Se este parâmetro estiver vazio, o cofre vinculado ao HSS_projectid é compatível.

Parâmetro	Obrigatório	Tipo	Descrição
backup_policy_id	Não	String	ID da política de backup Mínimo: <b>0</b> Máximo: <b>64</b>
backup_cycle	Não	<b>UpdateBackupPolicyRequestInfo</b> object	Política de backup.
agent_id_list	Sim	Array of strings	IDs de agentes em que a proteção está ativada Mínimo: <b>0</b> Máximo: <b>64</b> Comprimento da matriz: <b>0-24</b>
host_id_list	Sim	Array of strings	IDs dos servidores em que a proteção está ativada Mínimo: <b>0</b> Máximo: <b>64</b> Comprimento da matriz: <b>0-24</b>

**Tabela 3-106** ProtectionProxyInfoRequestInfo

Parâmetro	Obrigatório	Tipo	Descrição
policy_id	Não	String	ID da política. Este parâmetro é opcional para uma nova política. Mínimo: <b>0</b> Máximo: <b>64</b>
policy_name	Não	String	Nome da política. Este parâmetro é obrigatório quando você cria uma política de proteção. Mínimo: <b>0</b> Máximo: <b>64</b>
protection_mode	Não	String	Ação de proteção. Este parâmetro é obrigatório quando você cria uma política de proteção. As opções são as seguintes: <ul style="list-style-type: none"> <li>● alarm_and_isolation: relatar um alarme e isolar.</li> <li>● alarm_only: relatar apenas alarmes.</li> </ul> Mínimo: <b>0</b> Máximo: <b>64</b>

Parâmetro	Obrigatório	Tipo	Descrição
bait_protection_status	Não	String	Se deve ativar a proteção de honeypot. Este parâmetro é obrigatório quando você cria uma política de proteção. As opções são as seguintes. Por padrão, a proteção de honeypot está ativada. <ul style="list-style-type: none"><li>● opened</li><li>● closed</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>
protection_directory	Não	String	Diretório protegido. Este parâmetro é obrigatório quando você cria uma política de proteção. Mínimo: <b>0</b> Máximo: <b>64</b>
protection_type	Não	String	Tipo de proteção. Este parâmetro é obrigatório quando você cria uma política de proteção. Mínimo: <b>0</b> Máximo: <b>64</b>
exclude_directory	Não	String	(Opcional) Diretório excluído Mínimo: <b>0</b> Máximo: <b>64</b>
runtime_detection_status	Não	String	(Opcional) Se as verificações de tempo de execução devem ser executadas. As opções são as seguintes. Atualmente, ele só pode ser desativado. Este campo está reservado. <ul style="list-style-type: none"><li>● opened</li><li>● closed</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>
operating_system	Não	String	Sistema operacional. Este parâmetro é obrigatório quando você cria uma política de proteção. Seu valor pode ser: <ul style="list-style-type: none"><li>● Windows</li><li>● Linux</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>

Parâmetro	Obrigatório	Tipo	Descrição
process_whitelist	Não	Array of <b>TrustProcessInfo</b> objects	Lista branca do processo Comprimento da matriz: <b>0–20</b>

**Tabela 3-107** TrustProcessInfo

Parâmetro	Obrigatório	Tipo	Descrição
path	Não	String	Indica o caminho do processo. Mínimo: <b>0</b> Máximo: <b>128</b>
hash	Não	String	Hash do processo Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-108** BackupResources

Parâmetro	Obrigatório	Tipo	Descrição
vault_id	Não	String	Selecione o ID do cofre a ser vinculado. O valor não pode ser vazio. Mínimo: <b>0</b> Máximo: <b>64</b>
resource_list	Não	Array of <b>ResourceInfo</b> objects	Lista de servidores para os quais a função de backup precisa ser ativada Comprimento da matriz: <b>0–20</b>

**Tabela 3-109** ResourceInfo

Parâmetro	Obrigatório	Tipo	Descrição
host_id	Não	String	ID de servidor Mínimo: <b>0</b> Máximo: <b>128</b>

Parâmetro	Obrigatório	Tipo	Descrição
history_backup_status	Não	String	Se deve ativar o status de backup depende de error_message ou o status dos servidores disponíveis. Se error_message estiver vazio, o backup não será ativado e o valor desse campo será fechado. Se error_message não estiver vazio, o valor deste campo será aberto.  Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-110** UpdateBackupPolicyRequestInfo1

Parâmetro	Obrigatório	Tipo	Descrição
enabled	Não	Boolean	Se a política está ativada. O valor padrão é <b>true</b> .
policy_id	Não	String	ID da política. Este parâmetro é obrigatório se a proteção de backup estiver ativada.  Mínimo: <b>1</b> Máximo: <b>256</b>
operation_definition	Não	<b>OperationDefinitionRequestInfo</b> object	Parâmetro de agendamento.
trigger	Não	<b>BackupTriggerRequestInfo1</b> object	Regra de agendamento de tempo para a política.

**Tabela 3-111** OperationDefinitionRequestInfo

Parâmetro	Obrigatório	Tipo	Descrição
day_backups	Não	Integer	Número máximo de backups diários retidos. O último backup de cada dia é salvo a longo prazo. Esse parâmetro não é afetado pelo número máximo de backups retidos. O valor varia de 0 a 100. Se este parâmetro for especificado, o fuso horário deve ser configurado. Valor mínimo: 0. Valor máximo: 100 Mínimo: <b>0</b> Máximo: <b>100</b>
max_backups	Não	Integer	Número máximo de backups automatizados que podem ser retidos para um objeto. O valor pode ser -1 ou varia de 0 a 99999. Se o valor for definido como -1, os backups não serão apagados mesmo que o limite de quantidade de backups retidos configurado seja excedido. Se esse parâmetro e retention_duration_days forem deixados em branco ao mesmo tempo, os backups serão retidos permanentemente. Valor mínimo: 1. Valor máximo: 99999. Valor padrão: -1 Mínimo: <b>-1</b> Máximo: <b>99999</b>
month_backups	Não	Integer	Número máximo de backups mensais retidos. O último backup de cada mês é salvo a longo prazo. Esse parâmetro não é afetado pelo número máximo de backups retidos. O valor varia de 0 a 100. Se este parâmetro for especificado, o fuso horário deve ser configurado. Valor mínimo: 0. Valor máximo: 100 Mínimo: <b>0</b> Máximo: <b>100</b>

Parâmetro	Obrigatório	Tipo	Descrição
retention_duration_days	Não	Integer	Duração da retenção de um backup, em dias. O valor máximo é 99999. Se o valor for definido como -1, os backups não serão apagados mesmo que a duração de retenção configurada seja excedida. Se este parâmetro e max_backups forem deixados em branco ao mesmo tempo, os backups serão retidos permanentemente. Valor mínimo: 1. Valor máximo: 99999. Valor padrão: -1 Mínimo: <b>-1</b> Máximo: <b>99999</b>
timezone	Não	String	Fuso horário em que o usuário está localizado, por exemplo, UTC +08:00. Defina esse parâmetro somente depois de configurar qualquer um dos parâmetros day_backups, week_backups, month_backups e year_backups. Mínimo: <b>0</b> Máximo: <b>256</b>
week_backups	Não	Integer	Número máximo de backups semanais retidos. O último backup de cada semana é salvo a longo prazo. Este parâmetro pode ser efetivo junto com o número máximo de backups retidos especificado por max_backups. O valor varia de 0 a 100. Se este parâmetro for especificado, o fuso horário deve ser configurado. Mínimo: <b>0</b> Máximo: <b>100</b>



Parâmetro	Obrigatório	Tipo	Descrição
year_backups	Não	Integer	Número máximo de backups anuais retidos. O último backup de cada ano é salvo a longo prazo. Este parâmetro pode ser efetivo junto com o número máximo de backups retidos especificado por max_backups. O valor varia de 0 a 100. Se este parâmetro for especificado, o fuso horário deve ser configurado. Valor mínimo: 0. Valor máximo: 100  Mínimo: <b>0</b> Máximo: <b>100</b>

**Tabela 3-112** BackupTriggerRequestInfo1

Parâmetro	Obrigatório	Tipo	Descrição
properties	Não	<b>BackupTriggerPropertiesRequestInfo1</b> object	Regra de tempo para execução da política. Este parâmetro é obrigatório se a função de backup estiver ativada com proteção contra ransomware.

**Tabela 3-113** BackupTriggerPropertiesRequestInfo1

Parâmetro	Obrigatório	Tipo	Descrição
pattern	Não	Array of strings	<p>Regra de agendamento. Este parâmetro é obrigatório se a função de backup estiver ativada com proteção contra ransomware. Um máximo de 24 regras podem ser configuradas. A regra de agendamento está em conformidade com iCalendar RFC 2445, mas suporta apenas os parâmetros <b>FREQ</b>, <b>BYDAY</b>, <b>BYHOUR</b>, <b>BYMINUTE</b> e <b>INTERVAL</b>. <b>FREQ</b> pode ser definido apenas como <b>WEEKLY</b> ou <b>DAILY</b>. <b>BYDAY</b> pode ser definido como <b>MO</b>, <b>TU</b>, <b>WE</b>, <b>TH</b>, <b>FR</b>, <b>SA</b> ou <b>SU</b> (sete dias por semana). <b>BYHOUR</b> varia de 0 a 23 horas. <b>BYMINUTE</b> varia de 0 minutos a 59 minutos. O intervalo de agendamento não deve ser inferior a 1 hora. Um máximo de 24 pontos de tempo são permitidos em um dia. Por exemplo, se o horário de agendamento for 14:00 de segunda a domingo, defina a regra de agendamento da seguinte forma: <b>FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00</b>. Para iniciar o agendamento às 14:00 todos os dias, a regra é a seguinte: <b>FREQ=DAILY;INTERVAL=1;BYHOUR=14;BYMINUTE=00'</b></p> <p>Mínimo: <b>1</b> Máximo: <b>256</b> Comprimento da matriz: <b>0–24</b></p>

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Ativar a proteção contra ransomware para o servidor. O tipo de SO é Linux, o ID do servidor de destino é 71a15ecc-049f-4cca-bd28-5e90aca1817f, e o ID do agente do servidor de destino

é c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8. O backup do servidor está desativado.

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

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

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

Ativar a proteção contra ransomware para o servidor. O tipo de SO é Linux, o ID do servidor de destino é 71a15ecc-049f-4cca-bd28-5e90aca1817f, e o ID do agente do servidor de destino é c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8. O backup do servidor está desativado.

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

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

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

public class StartProtectionSolution {

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

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

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

StartProtectionRequest request = new StartProtectionRequest();
request.withEnterpriseProjectId("<enterprise_project_id>");
ProtectionInfoRequestInfo body = new ProtectionInfoRequestInfo();
List<String> listbodyHostIdList = new ArrayList<>();
listbodyHostIdList.add("71a15ecc-049f-4cca-bd28-5e90aca1817f");
List<String> listbodyAgentIdList = new ArrayList<>();

listbodyAgentIdList.add("c9bed5397db449ebdfba15e85fcfc36acce125c68954daf5cab0528bab59bd8");

ProtectionProxyInfoRequestInfo createProtectionPolicybody = new
ProtectionProxyInfoRequestInfo();
createProtectionPolicybody.withPolicyName("test111")
    .withProtectionMode("alarm_only")
    .withBaitProtectionStatus("opened")
    .withProtectionDirectory("/etc/test")
    .withProtectionType("docx")
    .withExcludeDirectory("");
body.withHostIdList(listbodyHostIdList);
body.withAgentIdList(listbodyAgentIdList);
body.withBackupProtectionStatus("closed");
body.withCreateProtectionPolicy(createProtectionPolicybody);
body.withProtectionPolicyId("");
body.withRansomProtectionStatus("opened");
body.withOperatingSystem("Linux");
request.withBody(body);
try {
    StartProtectionResponse response = client.startProtection(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

Ativar a proteção contra ransomware para o servidor. O tipo de SO é Linux, o ID do servidor de destino é 71a15ecc-049f-4cca-bd28-5e90aca1817f, e o ID do agente do servidor de destino é c9bed5397db449ebdfba15e85fcfc36acce125c68954daf5cab0528bab59bd8. O backup do servidor está desativado.

```
# coding: utf-8

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

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
    be stored in ciphertext in configuration files or environment variables and
```

```
decrypted during use to ensure security.
# In this example, AK and SK are stored in environment variables for
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak = __import__('os').getenv("CLOUD_SDK_AK")
sk = __import__('os').getenv("CLOUD_SDK_SK")

credentials = BasicCredentials(ak, sk) \

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

try:
    request = StartProtectionRequest()
    request.enterprise_project_id = "<enterprise_project_id>"
    listHostIdListbody = [
        "71a15ecc-049f-4cca-bd28-5e90aca1817f"
    ]
    listAgentIdListbody = [
        "c9bed5397db449ebdfba15e85fcfc36acceel25c68954daf5cab0528bab59bd8"
    ]
    createProtectionPolicybody = ProtectionProxyInfoRequestInfo(
        policy_name="test111",
        protection_mode="alarm_only",
        bait_protection_status="opened",
        protection_directory="/etc/test",
        protection_type="docx",
        exclude_directory=""
    )
    request.body = ProtectionInfoRequestInfo(
        host_id_list=listHostIdListbody,
        agent_id_list=listAgentIdListbody,
        backup_protection_status="closed",
        create_protection_policy=createProtectionPolicybody,
        protection_policy_id="",
        ransom_protection_status="opened",
        operating_system="Linux"
    )
    response = client.start_protection(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

Ativar a proteção contra ransomware para o servidor. O tipo de SO é Linux, o ID do servidor de destino é 71a15ecc-049f-4cca-bd28-5e90aca1817f, e o ID do agente do servidor de destino é c9bed5397db449ebdfba15e85fcfc36acceel25c68954daf5cab0528bab59bd8. O backup do servidor está desativado.

```
package main

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

func main() {
    // The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
```

```
be stored in ciphertext in configuration files or environment variables and
decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")

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

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

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

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Proteção contra ransomware ativada.

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.2.5 Desativação da prevenção contra ransomware

### Função

Esta API é usada para desativar a prevenção contra ransomware.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

POST /v5/{project\_id}/ransomware/protection/close

Tabela 3-114 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

Tabela 3-115 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>

## Parâmetros de solicitação

**Tabela 3-116** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-117** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
host_id_list	Sim	Array of strings	IDs de servidores em que a proteção contra ransomware precisa ser desativada Mínimo: <b>0</b> Máximo: <b>64</b> Comprimento da matriz: <b>0–20</b>
agent_id_list	Sim	Array of strings	IDs de agentes em que a prevenção contra ransomware precisa ser desativada Mínimo: <b>0</b> Máximo: <b>64</b> Comprimento da matriz: <b>0–20</b>
close_protection_type	Sim	String	Tipo de proteção desativada. As opções são as seguintes: <ul style="list-style-type: none"><li>● close_anti: a prevenção contra ransomware está desativada.</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>

## Parâmetros de resposta

Nenhum



## Exemplo de solicitações

Desativar a proteção contra ransomware para o servidor. O ID do servidor de destino é 71a15ecc-049f-4cca-bd28-5e90aca1817f, e o ID do agente do servidor de destino é c9bed5397db449ebdfba15e85fcfc36accee954daf5cab0528bab59bd8.

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

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

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

Desativar a proteção contra ransomware para o servidor. O ID do servidor de destino é 71a15ecc-049f-4cca-bd28-5e90aca1817f, e o ID do agente do servidor de destino é c9bed5397db449ebdfba15e85fcfc36accee954daf5cab0528bab59bd8.

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

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

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

public class StopProtectionSolution {

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

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

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

```
StopProtectionRequest request = new StopProtectionRequest();
request.withEnterpriseProjectId("<enterprise_project_id>");
CloseProtectionInfoRequestInfo body = new
CloseProtectionInfoRequestInfo();
List<String> listbodyAgentIdList = new ArrayList<>();

listbodyAgentIdList.add("c9bed5397db449ebdfba15e85fcfc36accee954daf5cab0528bab59bd8");

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

## Python

Desativar a proteção contra ransomware para o servidor. O ID do servidor de destino é 71a15ecc-049f-4cca-bd28-5e90aca1817f, e o ID do agente do servidor de destino é c9bed5397db449ebdfba15e85fcfc36accee954daf5cab0528bab59bd8.

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = StopProtectionRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        listAgentIdListbody = [
            "c9bed5397db449ebdfba15e85fcfc36accee954daf5cab0528bab59bd8"
        ]
```

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

## Go

Desativar a proteção contra ransomware para o servidor. O ID do servidor de destino é 71a15ecc-049f-4cca-bd28-5e90aca1817f, e o ID do agente do servidor de destino é c9bed5397db449ebdfba15e85fcfc36accee954daf5cab0528bab59bd8.

```
package main

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

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

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

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

    request := &model.StopProtectionRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        var listAgentIdListbody = []string{
            "c9bed5397db449ebdfba15e85fcfc36accee954daf5cab0528bab59bd8",
        }
        var listHostIdListbody = []string{
            "71a15ecc-049f-4cca-bd28-5e90aca1817f",
        }
        request.Body = &model.CloseProtectionInfoRequestInfo{
            CloseProtectionType: "close_anti",
            AgentIdList: listAgentIdListbody,
            HostIdList: listHostIdListbody,
        }
    }
```

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

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Proteção contra ransomware desativada.

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.2.6 Consulta da política de backup vinculada ao cofre de proteção do HSS

### Função

Essa API é usada para consultar a política de backup vinculada ao cofre de proteção do HSS. Certifique-se de que um cofre de proteção contra ransomware tenha sido comprado no CBR. Esse cofre é nomeado no formato HSS\_projectid.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/backup/policy

Tabela 3-118 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-119** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>

## Parâmetros de solicitação

**Tabela 3-120** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-121** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
enabled	Boolean	Se a política está ativada
id	String	ID da política Mínimo: <b>1</b> Máximo: <b>128</b>

Parâmetro	Tipo	Descrição
name	String	Nome da política Mínimo: <b>1</b> Máximo: <b>128</b>
operation_type	String	Tipo de backup. Seu valor pode ser: <ul style="list-style-type: none"> <li>● backup</li> <li>● replication</li> </ul> Mínimo: <b>1</b> Máximo: <b>128</b>
operation_definition	<b>OperationDefinitionInfo</b> object	Atributo de política. Regra reservada.
trigger	<b>BackupTriggerInfo</b> object	Regra de agendamento da política de backup

**Tabela 3-122** OperationDefinitionInfo

Parâmetro	Tipo	Descrição
day_backups	Integer	Número máximo de backups diários retidos. O último backup de cada dia é salvo a longo prazo. Esse parâmetro não é afetado pelo número máximo de backups retidos. O valor varia de 0 a 100. Se este parâmetro for especificado, o fuso horário deve ser configurado. Valor mínimo: 0. Valor máximo: 100 Mínimo: <b>0</b> Máximo: <b>100</b>
max_backups	Integer	Número máximo de backups automatizados que podem ser retidos para um objeto. O valor pode ser -1 ou varia de 0 a 99999. Se o valor for definido como -1, os backups não serão apagados mesmo que o limite de quantidade de backups retidos configurado seja excedido. Se esse parâmetro e retention_duration_days forem deixados em branco ao mesmo tempo, os backups serão retidos permanentemente. Valor mínimo: 1. Valor máximo: 99999. Valor padrão: -1 Mínimo: <b>-1</b> Máximo: <b>99999</b>

Parâmetro	Tipo	Descrição
month_backups	Integer	Número máximo de backups mensais retidos. O último backup de cada mês é salvo a longo prazo. Esse parâmetro não é afetado pelo número máximo de backups retidos. O valor varia de 0 a 100. Se esse parâmetro for especificado, o fuso horário deverá ser configurado. Valor mínimo: 0. Valor máximo: 100 Mínimo: <b>0</b> Máximo: <b>100</b>
retention_duration_days	Integer	Duração da retenção de um backup, em dias. O valor máximo é 99999. Se o valor for definido como -1, os backups não serão apagados mesmo que a duração de retenção configurada seja excedida. Se este parâmetro e max_backups forem deixados em branco ao mesmo tempo, os backups serão retidos permanentemente. Valor mínimo: 1. Valor máximo: 99999. Valor padrão: -1 Mínimo: <b>-1</b> Máximo: <b>99999</b>
timezone	String	Fuso horário em que o usuário está localizado, por exemplo, UTC+08:00. Defina esse parâmetro somente depois de configurar qualquer um dos parâmetros day_backups, week_backups, month_backups e year_backups. Mínimo: <b>0</b> Máximo: <b>256</b>
week_backups	Integer	Número máximo de backups semanais retidos. O último backup de cada semana é salvo a longo prazo. Este parâmetro pode ser efetivo junto com o número máximo de backups retidos especificado por max_backups. O valor varia de 0 a 100. Se este parâmetro for especificado, o fuso horário deve ser configurado. Mínimo: <b>0</b> Máximo: <b>100</b>
year_backups	Integer	Número máximo de backups anuais retidos. O último backup de cada ano é salvo a longo prazo. Este parâmetro pode ser efetivo junto com o número máximo de backups retidos especificado por max_backups. O valor varia de 0 a 100. Se este parâmetro for especificado, o fuso horário deve ser configurado. Valor mínimo: 0. Valor máximo: 100 Mínimo: <b>0</b> Máximo: <b>100</b>

Tabela 3-123 BackupTriggerInfo

Parâmetro	Tipo	Descrição
id	String	ID do agendador Mínimo: <b>0</b> Máximo: <b>256</b>
name	String	Nome do agendador Mínimo: <b>0</b> Máximo: <b>256</b>
type	String	Tipo de agendador. Atualmente, apenas o tempo pode ser configurado. Mínimo: <b>0</b> Máximo: <b>256</b>
properties	<b>BackupTriggerPropertiesInfo</b> object	Atributo do agendador

Tabela 3-124 BackupTriggerPropertiesInfo

Parâmetro	Tipo	Descrição
pattern	Array of strings	Política de agendamento. O valor contém um máximo de 10.240 caracteres e está em conformidade com iCalendar RFC 2445. No entanto, apenas <b>FREQ</b> , <b>BYDAY</b> , <b>BYHOUR</b> e <b>BYMINUTE</b> são suportados. <b>FREQ</b> pode ser definido como apenas <b>WEEKLY</b> ou <b>DAILY</b> . <b>BYDAY</b> pode ser definido para os sete dias em uma semana ( <b>MO</b> , <b>TU</b> , <b>WE</b> , <b>TH</b> , <b>FR</b> , <b>SA</b> e <b>SU</b> ). <b>BYHOUR</b> pode ser definido de 0 a 23 horas. <b>BYMINUTE</b> pode ser definido de 0 a 59 minutos. O intervalo entre os pontos de tempo não pode ser inferior a uma hora. Vários pontos de tempo de backup podem ser definidos em uma política de backup e até 24 pontos de tempo podem ser definidos para um dia. Mínimo: <b>0</b> Máximo: <b>256</b> Comprimento da matriz: <b>0-24</b>
start_time	String	Hora de início do agendador. Exemplo: 2020-01-08 09:59:49 Mínimo: <b>0</b> Máximo: <b>256</b>



## Exemplo de solicitações

Essa API é usada para consultar a política de backup vinculada ao cofre.

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

## Exemplo de respostas

**Código de status: 200**

Informações sobre a política de backup

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ShowBackupPolicyInfoSolution {

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

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

```
        .withSk(sk);

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

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

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

## Go

```
package main

import (
```

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

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Informações sobre a política de backup

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.2.7 Modificação da política de backup vinculada ao cofre

### Função

Essa API é usada para modificar a política de backup vinculada ao cofre.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

PUT /v5/{project\_id}/backup/policy

**Tabela 3-125** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-126** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>

## Parâmetros de solicitação

**Tabela 3-127** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-128** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
enabled	Não	Boolean	Se a política está ativada. O valor padrão é <b>true</b> .
policy_id	Sim	String	ID da política de backup Mínimo: <b>1</b> Máximo: <b>256</b>
operation_definition	Não	<b>OperationDefinitionRequestInfo</b> object	Parâmetro de agendamento.
trigger	Não	<b>BackupTriggerRequestInfo</b> object	Regra de agendamento de tempo para a política

**Tabela 3-129** OperationDefinitionRequestInfo

Parâmetro	Obrigatório	Tipo	Descrição
day_backups	Não	Integer	Número máximo de backups diários retidos. O último backup de cada dia é salvo a longo prazo. Esse parâmetro não é afetado pelo número máximo de backups retidos. O valor varia de 0 a 100. Se este parâmetro for especificado, o fuso horário deve ser configurado. Valor mínimo: 0. Valor máximo: 100 Mínimo: <b>0</b> Máximo: <b>100</b>
max_backups	Não	Integer	Número máximo de backups automatizados que podem ser retidos para um objeto. O valor pode ser -1 ou varia de 0 a 99999. Se o valor for definido como -1, os backups não serão apagados mesmo que o limite de quantidade de backups retidos configurado seja excedido. Se esse parâmetro e retention_duration_days forem deixados em branco ao mesmo tempo, os backups serão retidos permanentemente. Valor mínimo: 1. Valor máximo: 99999. Valor padrão: -1 Mínimo: <b>-1</b> Máximo: <b>99999</b>
month_backups	Não	Integer	Número máximo de backups mensais retidos. O último backup de cada mês é salvo a longo prazo. Esse parâmetro não é afetado pelo número máximo de backups retidos. O valor varia de 0 a 100. Se este parâmetro for especificado, o fuso horário deve ser configurado. Valor mínimo: 0. Valor máximo: 100 Mínimo: <b>0</b> Máximo: <b>100</b>

Parâmetro	Obrigatório	Tipo	Descrição
retention_duration_days	Não	Integer	Duração da retenção de um backup, em dias. O valor máximo é 99999. Se o valor for definido como -1, os backups não serão apagados mesmo que a duração de retenção configurada seja excedida. Se este parâmetro e max_backups forem deixados em branco ao mesmo tempo, os backups serão retidos permanentemente. Valor mínimo: 1. Valor máximo: 99999. Valor padrão: -1 Mínimo: <b>-1</b> Máximo: <b>99999</b>
timezone	Não	String	Fuso horário em que o usuário está localizado, por exemplo, UTC +08:00. Defina esse parâmetro somente depois de configurar qualquer um dos parâmetros day_backups, week_backups, month_backups e year_backups. Mínimo: <b>0</b> Máximo: <b>256</b>
week_backups	Não	Integer	Número máximo de backups semanais retidos. O último backup de cada semana é salvo a longo prazo. Este parâmetro pode ser efetivo junto com o número máximo de backups retidos especificado por max_backups. O valor varia de 0 a 100. Se este parâmetro for especificado, o fuso horário deve ser configurado. Mínimo: <b>0</b> Máximo: <b>100</b>

Parâmetro	Obrigatório	Tipo	Descrição
year_backups	Não	Integer	Número máximo de backups anuais retidos. O último backup de cada ano é salvo a longo prazo. Este parâmetro pode ser efetivo junto com o número máximo de backups retidos especificado por max_backups. O valor varia de 0 a 100. Se este parâmetro for especificado, o fuso horário deve ser configurado. Valor mínimo: 0. Valor máximo: 100  Mínimo: <b>0</b> Máximo: <b>100</b>

**Tabela 3-130** BackupTriggerRequestInfo

Parâmetro	Obrigatório	Tipo	Descrição
properties	Sim	<b>BackupTriggerPropertiesRequestInfo</b> object	Regra de tempo para a execução da política.



**Tabela 3-131** BackupTriggerPropertiesRequestInfo

Parâmetro	Obrigatório	Tipo	Descrição
pattern	Sim	Array of strings	Regra de agendamento. Um máximo de 24 regras podem ser configuradas. A regra de agendamento está em conformidade com iCalendar RFC 2445, mas suporta apenas os parâmetros <b>FREQ</b> , <b>BYDAY</b> , <b>BYHOUR</b> , <b>BYMINUTE</b> e <b>INTERVAL</b> . <b>FREQ</b> pode ser definido apenas como <b>WEEKLY</b> ou <b>DAILY</b> . <b>BYDAY</b> pode ser definido como <b>MO</b> , <b>TU</b> , <b>WE</b> , <b>TH</b> , <b>FR</b> , <b>SA</b> ou <b>SU</b> (sete dias por semana). <b>BYHOUR</b> varia de 0 a 23 horas. <b>BYMINUTE</b> varia de 0 minutos a 59 minutos. O intervalo de agendamento não deve ser inferior a 1 hora. Um máximo de 24 pontos de tempo são permitidos em um dia. Por exemplo, se o horário de agendamento for 14:00 de segunda a domingo, defina a regra de agendamento da seguinte forma: <b>FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00</b> . Para iniciar o agendamento às 14:00 todos os dias, a regra é a seguinte: <b>FREQ=DAILY;INTERVAL=1;BYHOUR=14;BYMINUTE=00'</b>  Mínimo: <b>1</b> Máximo: <b>256</b> Comprimento da matriz: <b>0-24</b>

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Modificar a política de backup. O ID da política de backup de destino é af4d08ad-2b60-4916-a5cf-8d6a23956dda.

```
PUT https://{endpoint}/v5/{project_id}/backup/policy
{
  "enabled" : true,
```

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

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

Modificar a política de backup. O ID da política de backup de destino é af4d08ad-2b60-4916-a5cf-8d6a23956dda.

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

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

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

public class UpdateBackupPolicyInfoSolution {

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

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

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

```
UpdateBackupPolicyInfoRequest();
request.withEnterpriseProjectId("<enterprise_project_id>");
UpdateBackupPolicyRequestInfo body = new UpdateBackupPolicyRequestInfo();
List<String> listPropertiesPattern = new ArrayList<>();
listPropertiesPattern.add("FREQ=DAILY;INTERVAL=2;BYHOUR=14;BYMINUTE=00");
BackupTriggerPropertiesRequestInfo propertiesTrigger = new
BackupTriggerPropertiesRequestInfo();
propertiesTrigger.withPattern(listPropertiesPattern);
BackupTriggerRequestInfo triggerbody = new BackupTriggerRequestInfo();
triggerbody.withProperties(propertiesTrigger);
OperationDefinitionRequestInfo operationDefinitionbody = new
OperationDefinitionRequestInfo();
operationDefinitionbody.withDayBackups(0)
    .withMaxBackups(-1)
    .withMonthBackups(0)
    .withRetentionDurationDays(5)
    .withTimezone("UTC+08:00")
    .withWeekBackups(0)
    .withYearBackups(0);
body.withTrigger(triggerbody);
body.withOperationDefinition(operationDefinitionbody);
body.withPolicyId("af4d08ad-2b60-4916-a5cf-8d6a23956dda");
body.withEnabled(true);
request.withBody(body);
try {
    UpdateBackupPolicyInfoResponse response =
client.updateBackupPolicyInfo(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

Modificar a política de backup. O ID da política de backup de destino é af4d08ad-2b60-4916-a5cf-8d6a23956dda.

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
```

```
.with_region(HssRegion.value_of("<YOUR REGION>")) \
.build()

try:
    request = UpdateBackupPolicyInfoRequest()
    request.enterprise_project_id = "<enterprise_project_id>"
    listPatternProperties = [
        "FREQ=DAILY;INTERVAL=2;BYHOUR=14;BYMINUTE=00"
    ]
    propertiesTrigger = BackupTriggerPropertiesRequestInfo(
        pattern=listPatternProperties
    )
    triggerbody = BackupTriggerRequestInfo(
        properties=propertiesTrigger
    )
    operationDefinitionbody = OperationDefinitionRequestInfo(
        day_backups=0,
        max_backups=-1,
        month_backups=0,
        retention_duration_days=5,
        timezone="UTC+08:00",
        week_backups=0,
        year_backups=0
    )
    request.body = UpdateBackupPolicyRequestInfo(
        trigger=triggerbody,
        operation_definition=operationDefinitionbody,
        policy_id="af4d08ad-2b60-4916-a5cf-8d6a23956dda",
        enabled=True
    )
    response = client.update_backup_policy_info(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

Modificar a política de backup. O ID da política de backup de destino é af4d08ad-2b60-4916-a5cf-8d6a23956dda.

```
package main

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

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

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

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

request := &model.UpdateBackupPolicyInfoRequest{
    enterpriseProjectIdRequest:= "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    var listPatternProperties = []string{
        "FREQ=DAILY;INTERVAL=2;BYHOUR=14;BYMINUTE=00",
    }
    propertiesTrigger := &model.BackupTriggerPropertiesRequestInfo{
        Pattern: listPatternProperties,
    }
    triggerbody := &model.BackupTriggerRequestInfo{
        Properties: propertiesTrigger,
    }
    dayBackupsOperationDefinition:= int32(0)
    maxBackupsOperationDefinition:= int32(-1)
    monthBackupsOperationDefinition:= int32(0)
    retentionDurationDaysOperationDefinition:= int32(5)
    timezoneOperationDefinition:= "UTC+08:00"
    weekBackupsOperationDefinition:= int32(0)
    yearBackupsOperationDefinition:= int32(0)
    operationDefinitionbody := &model.OperationDefinitionRequestInfo{
        DayBackups: &dayBackupsOperationDefinition,
        MaxBackups: &maxBackupsOperationDefinition,
        MonthBackups: &monthBackupsOperationDefinition,
        RetentionDurationDays: &retentionDurationDaysOperationDefinition,
        Timezone: &timezoneOperationDefinition,
        WeekBackups: &weekBackupsOperationDefinition,
        YearBackups: &yearBackupsOperationDefinition,
    }
    enabledUpdateBackupPolicyRequestInfo:= true
    request.Body = &model.UpdateBackupPolicyRequestInfo{
        Trigger: triggerbody,
        OperationDefinition: operationDefinitionbody,
        PolicyId: "af4d08ad-2b60-4916-a5cf-8d6a23956dda",
        Enabled: &enabledUpdateBackupPolicyRequestInfo,
    }
    response, err := client.UpdateBackupPolicyInfo(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Modificar uma política de backup.

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.3 Gerenciamento de linha de base

### 3.3.1 Consulta da lista de resultados de detecção de senha fraca

#### Função

Essa API é usada para consultar a lista de resultados de detecção de senhas fracas.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/baseline/weak-password-users

Tabela 3-132 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>20</b> Máximo: <b>64</b>

Tabela 3-133 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Mínimo: <b>0</b> Máximo: <b>64</b>
host_name	Não	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>256</b>
host_ip	Não	String	Endereço IP do servidor Mínimo: <b>0</b> Máximo: <b>256</b>

Parâmetro	Obrigatório	Tipo	Descrição
user_name	Não	String	Nome da conta usando uma senha fraca Mínimo: <b>0</b> Máximo: <b>32</b>
host_id	Não	String	ID do host. Se esse parâmetro não for especificado, todos os hosts de um usuário serão consultados. Mínimo: <b>0</b> Máximo: <b>64</b>
limit	Não	Integer	Número de registros em cada página Mínimo: <b>0</b> Máximo: <b>200</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>

## Parâmetros de solicitação

Tabela 3-134 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token de usuário, que pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de <b>X-Subject-Token</b> no cabeçalho da resposta é o token do usuário. Mínimo: <b>32</b> Máximo: <b>2097152</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-135** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Long	Número total de senhas fracas Mínimo: <b>0</b> Máximo: <b>2147483647</b>
data_list	Array of <b>WeakPwdListInfoResponseInfo</b> objects	Lista de senhas fracas Comprimento da matriz: <b>0–2147483647</b>

**Tabela 3-136** WeakPwdListInfoResponseInfo

Parâmetro	Tipo	Descrição
host_id	String	ID do host Mínimo: <b>0</b> Máximo: <b>64</b>
host_name	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>256</b>
host_ip	String	Endereço IP do servidor (endereço IP privado). Este campo não é excluído para compatibilidade com os usuários. Mínimo: <b>0</b> Máximo: <b>256</b>
private_ip	String	Endereço IP privado de servidor Mínimo: <b>0</b> Máximo: <b>256</b>
public_ip	String	Endereço IP público do servidor Mínimo: <b>0</b> Máximo: <b>256</b>
weak_pwd_accounts	Array of <b>WeakPwdAccountInfoResponseInfo</b> objects	Lista de contas com senhas fracas Comprimento da matriz: <b>0–2147483647</b>



**Tabela 3-137** WeakPwdAccountInfoResponseInfo

Parâmetro	Tipo	Descrição
user_name	String	Nome de contas com senhas fracas Mínimo: <b>0</b> Máximo: <b>32</b>
service_type	String	Tipo de conta. As opções são as seguintes: <ul style="list-style-type: none"> <li>● system</li> <li>● mysql</li> <li>● redis</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>
duration	Integer	Período de validade de uma senha fraca, em dias. Mínimo: <b>0</b> Máximo: <b>2147483647</b>

## Exemplo de solicitações

Consultar a senha fraca de servidores cujo ID de projeto empresarial é xxx. Os dados na primeira página (os primeiros 10 registros) são retornados por padrão.

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

## Exemplo de respostas

**Código de status: 200**

Resultado da verificação de senha fraca

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

```
} ]  
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListWeakPasswordUsersRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.host_name = "<host_name>"
        request.host_ip = "<host_ip>"
        request.user_name = "<user_name>"
        request.host_id = "<host_id>"
        request.limit = <limit>
        request.offset = <offset>
        response = client.list_weak_password_users(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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

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

```
        WithSk(sk).
        Build()

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

    request := &model.ListWeakPasswordUsersRequest{}
    enterpriseProjectIdRequest := "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    hostNameRequest := "<host_name>"
    request.HostName = &hostNameRequest
    hostIpRequest := "<host_ip>"
    request.HostIp = &hostIpRequest
    userNameRequest := "<user_name>"
    request.UserName = &userNameRequest
    hostIdRequest := "<host_id>"
    request.HostId = &hostIdRequest
    limitRequest := int32(<limit>)
    request.Limit = &limitRequest
    offsetRequest := int32(<offset>)
    request.Offset = &offsetRequest
    response, err := client.ListWeakPasswordUsers(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Resultado da verificação de senha fraca

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.3.2 Consulta do relatório de detecção de política de complexidade de senha

#### Função

Essa API é usada para consultar o relatório de detecção de política de complexidade de senha.

## Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

## URI

GET /v5/{project\_id}/baseline/password-complexity

**Tabela 3-138** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-139** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Mínimo: <b>0</b> Máximo: <b>256</b>
host_name	Não	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
host_ip	Não	String	Endereço IP do servidor Mínimo: <b>0</b> Máximo: <b>128</b>
host_id	Não	String	ID do host. Se esse parâmetro não for especificado, todos os hosts de um usuário serão consultados. Mínimo: <b>0</b> Máximo: <b>128</b>
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>0</b> Máximo: <b>200</b> Padrão: <b>10</b>

Parâmetro	Obrigatório	Tipo	Descrição
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>

## Parâmetros de solicitação

Tabela 3-140 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de <b>X-Subject-Token</b> no cabeçalho da resposta é o token do usuário. Mínimo: <b>1</b> Máximo: <b>32768</b>

## Parâmetros de resposta

Código de status: **200**

Tabela 3-141 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Long	Número total de políticas de complexidade de senha Mínimo: <b>0</b> Máximo: <b>2147483647</b>
data_list	Array of <b>PwdPolicyInfo ResponseInfo</b> objects	Lista de detecção de política de complexidade de senha Comprimento da matriz: <b>0-2147483647</b>

**Tabela 3-142** PwdPolicyInfoResponseInfo

Parâmetro	Tipo	Descrição
host_id	String	ID do host Mínimo: <b>0</b> Máximo: <b>64</b>
host_name	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>256</b>
host_ip	String	Endereço IP do servidor (endereço IP privado). Este campo não é excluído para compatibilidade com os usuários. Mínimo: <b>0</b> Máximo: <b>256</b>
private_ip	String	Endereço IP privado de servidor Mínimo: <b>0</b> Máximo: <b>256</b>
public_ip	String	Endereço IP público do servidor Mínimo: <b>0</b> Máximo: <b>256</b>
min_length	Boolean	Indica se o comprimento mínimo da senha atende aos requisitos. Se o valor for true, o comprimento mínimo da senha atende aos requisitos. Se o valor for false, o comprimento mínimo da senha não atende aos requisitos.
uppercase_letter	Boolean	Indica se as letras maiúsculas atendem aos requisitos. Se o valor for true, as letras maiúsculas atendem aos requisitos. Se o valor for false, as letras maiúsculas não atendem aos requisitos.
lowercase_letter	Boolean	Indica se as letras minúsculas atendem aos requisitos. Se o valor for true, as letras minúsculas atendem aos requisitos. Se o valor for false, as letras minúsculas não atendem aos requisitos.
number	Boolean	Indica se o número atende aos requisitos. Se o valor for true, o número atende aos requisitos. Se o valor for false, o número não atende aos requisitos.
special_character	Boolean	Indica se o caractere especial atende aos requisitos. Se o valor for true, o caractere especial atende aos requisitos. Se o valor for false, o caractere especial não atende aos requisitos.

Parâmetro	Tipo	Descrição
suggestion	String	Sugestão de modificação Mínimo: <b>0</b> Máximo: <b>65534</b>

## Exemplo de solicitações

Consultar a complexidade da senha do servidor cujo ID de projeto empresarial é xxx. Os dados na primeira página (os primeiros 10 registros) são retornados por padrão.

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

## Exemplo de respostas

**Código de status: 200**

Relatório de verificação de política de complexidade de senha

```
{  
  "total_num" : 1,  
  "data_list" : [ {  
    "host_id" : "76fa440a-5a08-43fa-ac11-d12183ab3a14",  
    "host_ip" : "192.168.0.59",  
    "private_ip" : "192.168.0.8",  
    "public_ip" : "100.85.85.85",  
    "host_name" : "ecs-6b96",  
    "lowercase_letter" : false,  
    "min_length" : true,  
    "number" : false,  
    "special_character" : false,  
    "suggestion" : "The password should contain at least 3 of the following  
character types: uppercase letters, lowercase letters, digits, and special  
characters. ",  
    "uppercase_letter" : false  
  } ]  
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;  
import com.huaweicloud.sdk.hss.v5.region.HssRegion;  
import com.huaweicloud.sdk.hss.v5.*;  
import com.huaweicloud.sdk.hss.v5.model.*;  
  
public class ListPasswordComplexitySolution {  
    public static void main(String[] args) {
```



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

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

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

ListPasswordComplexityRequest request = new
ListPasswordComplexityRequest();
request.withEnterpriseProjectId("<enterprise_project_id>");
request.withHostName("<host_name>");
request.withHostIp("<host_ip>");
request.withHostId("<host_id>");
request.withLimit(<limit>);
request.withOffset(<offset>);
try {
    ListPasswordComplexityResponse response =
client.listPasswordComplexity(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

```
.build()

try:
    request = ListPasswordComplexityRequest()
    request.enterprise_project_id = "<enterprise_project_id>"
    request.host_name = "<host_name>"
    request.host_ip = "<host_ip>"
    request.host_id = "<host_id>"
    request.limit = <limit>
    request.offset = <offset>
    response = client.list_password_complexity(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ListPasswordComplexityRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        hostNameRequest:= "<host_name>"
        request.HostName = &hostNameRequest
        hostIpRequest:= "<host_ip>"
        request.HostIp = &hostIpRequest
        hostIdRequest:= "<host_id>"
        request.HostId = &hostIdRequest
        limitRequest:= int32(<limit>)
        request.Limit = &limitRequest
        offsetRequest:= int32(<offset>)
        request.Offset = &offsetRequest
        response, err := client.ListPasswordComplexity(request)
        if err == nil {
            fmt.Printf("%+v\n", response)
        } else {
```

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

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Relatório de verificação de política de complexidade de senha

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.3.3 Consulta da lista de resultados da verificação de configuração de segurança do servidor

#### Função

Essa API é usada para consultar a lista de resultados da verificação de configuração de segurança do servidor de um usuário.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/baseline/risk-configs

Tabela 3-143 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

Tabela 3-144 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Mínimo: <b>0</b> Máximo: <b>256</b>
check_name	Não	String	Nome da linha de base, por exemplo, SSH, CentOS 7 e Windows. Mínimo: <b>0</b> Máximo: <b>256</b>
group_id	Não	String	Indica o ID do grupo de políticas. Mínimo: <b>0</b> Máximo: <b>128</b>
severity	Não	String	Nível de risco. Seu valor pode ser: <ul style="list-style-type: none"><li>● Security</li><li>● Low</li><li>● Medium</li><li>● High</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
standard	Não	String	Tipo padrão. Seu valor pode ser: <ul style="list-style-type: none"><li>● cn_standard: padrão de conformidade DJCP MLPS</li><li>● hw_standard: padrão de prática de segurança na nuvem</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
host_id	Não	String	ID do host Mínimo: <b>0</b> Máximo: <b>128</b>
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é <b>10</b> . Mínimo: <b>0</b> Máximo: <b>200</b> Padrão: <b>10</b>

Parâmetro	Obrigatório	Tipo	Descrição
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>

## Parâmetros de solicitação

Tabela 3-145 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de <b>X-Subject-Token</b> no cabeçalho da resposta é o token do usuário. Mínimo: <b>1</b> Máximo: <b>32768</b>

## Parâmetros de resposta

**Código de status: 200**

Tabela 3-146 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Long	Número total de registros Mínimo: <b>0</b> Máximo: <b>2147483647</b>
data_list	Array of <b>SecurityCheckInfoResponseInfo</b> objects	Lista de resultados da verificação de configuração do servidor Comprimento da matriz: <b>0-2147483647</b>

**Tabela 3-147** SecurityCheckInfoResponseInfo

Parâmetro	Tipo	Descrição
severity	String	Nível de risco. Seu valor pode ser: <ul style="list-style-type: none"><li>● Low</li><li>● Medium</li><li>● High</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
check_name	String	Nome da linha de base, por exemplo, SSH, CentOS 7 e Windows. Mínimo: <b>0</b> Máximo: <b>256</b>
check_type	String	Tipo de linha de base. Os valores de check_type e check_name são os mesmos para servidores Linux. Por exemplo, ambos podem ser definidos como SSH ou CentOS 7. Para servidores Windows, os valores de check_type e check_name são diferentes. Por exemplo, check_type pode ser definido como Windows Server 2019 R2 ou Windows Server 2016 R2. Mínimo: <b>0</b> Máximo: <b>256</b>
standard	String	Tipo padrão. Seu valor pode ser: <ul style="list-style-type: none"><li>● cn_standard: padrão de conformidade DJCP MLPS</li><li>● hw_standard: padrão de prática de segurança na nuvem</li></ul> Mínimo: <b>1</b> Máximo: <b>16</b>
check_rule_num	Integer	Indica o número total de itens de verificação do tipo de verificação de configuração atual (linha de base). Por exemplo, se o tipo padrão da linha de base do SSH for hw_standard, a segurança do servidor fornecerá 17 itens de verificação, mas apenas cinco itens de verificação da linha de base do SSH serão detectados em todos os servidores. Portanto, o valor de check_rule_num é 5. Todos os itens de verificação são verificados em um servidor. O valor de check_rule_num é 17. Mínimo: <b>0</b> Máximo: <b>2097152</b>

Parâmetro	Tipo	Descrição
failed_rule_num	Integer	Número de itens de verificação com falha. Se um servidor falhar ao passar um item de verificação em check_rule_num, o item será contado em failed_rule_num. Mínimo: <b>0</b> Máximo: <b>2097152</b>
host_num	Integer	O número de servidores nos quais a detecção de linha de base atual é executada. Mínimo: <b>0</b> Máximo: <b>2097152</b>
scan_time	Long	Hora da última detecção (ms) Mínimo: <b>0</b> Máximo: <b>2097152</b>
check_type_desc	String	Descrição do tipo de linha de base, incluindo os padrões para os itens de verificação e os problemas que podem ser auditados. Mínimo: <b>0</b> Máximo: <b>65534</b>

## Exemplo de solicitações

Essa API é usada para consultar a lista de verificação de configuração de linha de base do servidor cujo ID de projeto empresarial é xxx. Os dados na primeira página (os primeiros 10 registros) são retornados por padrão.

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

## Exemplo de respostas

**Código de status: 200**

Resultado da verificação da configuração de segurança do servidor

```
{
  "total_num" : 1,
  "data_list" : [ {
    "check_name" : "Docker",
    "check_rule_num" : 25,
    "check_type" : "Docker",
    "check_type_desc" : "Configuring security audit of Docker's host
configurations and container-running-related contents based on Docker Container
Security Specifications V1_0.",
    "failed_rule_num" : 20,
    "host_num" : 0,
    "scan_time" : 1661716860935,
    "severity" : "High",
    "standard" : "hw_standard"
  } ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListRiskConfigsSolution {

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

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

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

        ListRiskConfigsRequest request = new ListRiskConfigsRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withCheckName("<check_name>");
        request.withGroupId("<group_id>");
        request.withSeverity("<severity>");
        request.withStandard("<standard>");
        request.withHostId("<host_id>");
        request.withLimit(<limit>);
        request.withOffset(<offset>);
        try {
            ListRiskConfigsResponse response = client.listRiskConfigs(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

### Python

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



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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListRiskConfigsRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.check_name = "<check_name>"
        request.group_id = "<group_id>"
        request.severity = "<severity>"
        request.standard = "<standard>"
        request.host_id = "<host_id>"
        request.limit = <limit>
        request.offset = <offset>
        response = client.list_risk_configs(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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

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

```
client := hss.NewHssClient(  
    hss.HssClientBuilder().  
        WithRegion(region.ValueOf("<YOUR REGION>")).  
        WithCredential(auth).  
        Build())  
  
request := &model.ListRiskConfigsRequest{  
    enterpriseProjectIdRequest:= "<enterprise_project_id>"  
    request.EnterpriseProjectId = &enterpriseProjectIdRequest  
    checkNameRequest:= "<check_name>"  
    request.CheckName = &checkNameRequest  
    groupIdRequest:= "<group_id>"  
    request.GroupId = &groupIdRequest  
    severityRequest:= "<severity>"  
    request.Severity = &severityRequest  
    standardRequest:= "<standard>"  
    request.Standard = &standardRequest  
    hostIdRequest:= "<host_id>"  
    request.HostId = &hostIdRequest  
    limitRequest:= int32(<limit>)  
    request.Limit = &limitRequest  
    offsetRequest:= int32(<offset>)  
    request.Offset = &offsetRequest  
    response, err := client.ListRiskConfigs(request)  
    if err == nil {  
        fmt.Printf("%+v\n", response)  
    } else {  
        fmt.Println(err)  
    }  
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Resultado da verificação da configuração de segurança do servidor

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.3.4 Consulta do resultado da verificação de um item de configuração de segurança

#### Função

Essa API é usada para consultar o resultado da verificação de um item de configuração de segurança especificado.

## Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

## URI

GET /v5/{project\_id}/baseline/risk-config/{check\_name}/detail

**Tabela 3-148** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>20</b> Máximo: <b>64</b>
check_name	Sim	String	Nome da linha de base, por exemplo, SSH, CentOS 7 e Windows. Mínimo: <b>0</b> Máximo: <b>256</b>

**Tabela 3-149** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>64</b>
standard	Sim	String	Tipo padrão. Seu valor pode ser: <ul style="list-style-type: none"><li>● cn_standard: padrão de conformidade DJCP MLPS</li><li>● hw_standard: padrão de prática de segurança na nuvem</li></ul> Mínimo: <b>0</b> Máximo: <b>32</b>
host_id	Não	String	ID do servidor. Se esse parâmetro não for especificado, todos os servidores do usuário serão consultados. Mínimo: <b>0</b> Máximo: <b>64</b>

Parâmetro	Obrigatório	Tipo	Descrição
limit	Não	Integer	Número de registros em cada página. Mínimo: <b>0</b> Máximo: <b>200</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>

## Parâmetros de solicitação

Tabela 3-150 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>32</b> Máximo: <b>2097152</b>

## Parâmetros de resposta

Código de status: **200**

Tabela 3-151 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
severity	String	Nível de risco. Seu valor pode ser: <ul style="list-style-type: none"><li>● Low</li><li>● Medium</li><li>● High</li></ul> Mínimo: <b>0</b> Máximo: <b>65534</b>

Parâmetro	Tipo	Descrição
check_type	String	Tipo de verificação de configuração (linha de base), por exemplo, SSH, CentOS 7, Windows Server 2019 R2, Windows Server 2016 R2 e MySQL5-Windows. Mínimo: <b>0</b> Máximo: <b>256</b>
check_type_desc	String	Descrição do tipo de linha de base, incluindo os padrões para os itens de verificação e os problemas que podem ser auditados. Mínimo: <b>0</b> Máximo: <b>65534</b>
check_rule_num	Integer	Indica o número total de itens de verificação do tipo de verificação de configuração atual (linha de base). Por exemplo, se o tipo padrão da linha de base do SSH for hw_standard, a segurança do servidor fornecerá 17 itens de verificação, mas apenas cinco itens de verificação da linha de base do SSH serão detectados em todos os servidores. Portanto, o valor de check_rule_num é 5. Todos os itens de verificação são verificados em um servidor. O valor de check_rule_num é 17. Mínimo: <b>0</b> Máximo: <b>2147483647</b>
failed_rule_num	Integer	Número de itens de verificação com falha. Se um servidor falhar ao passar um item de verificação em check_rule_num, o item será contado em failed_rule_num. Mínimo: <b>0</b> Máximo: <b>2147483647</b>
passed_rule_num	Integer	Número de itens de verificação aprovados. Se um servidor passar um item de verificação em check_rule_num, o item de verificação será contado em passed_rule_num. Mínimo: <b>0</b> Máximo: <b>2147483647</b>
ignored_rule_num	Integer	Número de itens de verificação ignorados. Se um servidor ignorar um item de verificação em check_rule_num, o item de verificação será contado em ignored_rule_num. Mínimo: <b>0</b> Máximo: <b>2147483647</b>

Parâmetro	Tipo	Descrição
host_num	Long	O número de servidores nos quais a detecção de linha de base atual é executada. Mínimo: <b>0</b> Máximo: <b>2147483647</b>

## Exemplo de solicitações

Essa API é usada para consultar a lista de verificação de configuração cujo nome de linha de base é SSH, o padrão de verificação é o padrão de prática de segurança na nuvem e o ID do projeto empresarial é xxx.

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

## Exemplo de respostas

**Código de status: 200**

Resultado da verificação do item de configuração de segurança

```
{
  "check_rule_num" : 17,
  "check_type_desc" : "This policy checks the basic security configuration items of the SSH service to improve the security of the SSH service.",
  "failed_rule_num" : 15,
  "host_num" : 2,
  "ignored_rule_num" : 1,
  "passed_rule_num" : 14,
  "severity" : "Medium"
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ShowRiskConfigDetailSolution {

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

```
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");

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

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();
ShowRiskConfigDetailRequest request = new ShowRiskConfigDetailRequest();
request.withEnterpriseProjectId("<enterprise_project_id>");
request.withStandard("<standard>");
request.withHostId("<host_id>");
request.withLimit(<limit>);
request.withOffset(<offset>);
try {
    ShowRiskConfigDetailResponse response =
client.showRiskConfigDetail(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ShowRiskConfigDetailRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.standard = "<standard>"
        request.host_id = "<host_id>"
        request.limit = <limit>
```

```
request.offset = <offset>
response = client.show_risk_config_detail(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ShowRiskConfigDetailRequest{}
    enterpriseProjectIdRequest := "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    request.Standard = "<standard>"
    hostIdRequest := "<host_id>"
    request.HostId = &hostIdRequest
    limitRequest := int32(<limit>)
    request.Limit = &limitRequest
    offsetRequest := int32(<offset>)
    request.Offset = &offsetRequest
    response, err := client.ShowRiskConfigDetail(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.



## Códigos de status

Código de status	Descrição
200	Resultado da verificação do item de configuração de segurança

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.3.5 Consulta da lista de verificação de um item de configuração de segurança

### Função

Esta API é usada para consultar a lista de verificação de um item de configuração de segurança especificado.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/baseline/risk-config/{check\_name}/check-rules

**Tabela 3-152** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>20</b> Máximo: <b>64</b>
check_name	Sim	String	Nome da linha de base, por exemplo, SSH, CentOS 7 e Windows. Mínimo: <b>0</b> Máximo: <b>256</b>

**Tabela 3-153** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>64</b>
standard	Sim	String	Tipo padrão. Seu valor pode ser: <ul style="list-style-type: none"> <li>● cn_standard: padrão de conformidade DJCP MLPS</li> <li>● hw_standard: padrão de prática de segurança na nuvem</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>
result_type	Não	String	Tipo de resultado. Seu valor pode ser: <ul style="list-style-type: none"> <li>● safe: o item passou na verificação.</li> <li>● unhandled: o item falhou na verificação e não é ignorado.</li> <li>● ignored: o item falhou na verificação, mas foi ignorado.</li> </ul> Padrão: <b>unhandled</b> Mínimo: <b>0</b> Máximo: <b>64</b>
check_rule_name	Não	String	Nome do item de verificação. A correspondência difusa é suportada. Mínimo: <b>0</b> Máximo: <b>2048</b>
severity	Não	String	Nível de risco. Seu valor pode ser: <ul style="list-style-type: none"> <li>● Security</li> <li>● Low</li> <li>● Medium</li> <li>● High</li> <li>● Critical</li> </ul> Mínimo: <b>0</b> Máximo: <b>255</b>

Parâmetro	Obrigatório	Tipo	Descrição
host_id	Não	String	ID do servidor. Se esse parâmetro não for especificado, todos os servidores do usuário serão consultados. Mínimo: <b>0</b> Máximo: <b>64</b>
limit	Não	Integer	Número de itens por página Mínimo: <b>0</b> Máximo: <b>200</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>

## Parâmetros de solicitação

Tabela 3-154 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>32</b> Máximo: <b>2097152</b>

## Parâmetros de resposta

Código de status: **200**

**Tabela 3-155** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Long	Riscos totais Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b>
data_list	Array of <b>CheckRuleRiskInfoResponseInfo</b> objects	Lista de dados Comprimento da matriz: <b>0–2147483647</b>

**Tabela 3-156** CheckRuleRiskInfoResponseInfo

Parâmetro	Tipo	Descrição
severity	String	Nível de risco. Seu valor pode ser: <ul style="list-style-type: none"><li>● Low</li><li>● Medium</li><li>● High</li></ul> Mínimo: <b>0</b> Máximo: <b>255</b>
check_name	String	Nome da linha de base, por exemplo, SSH, CentOS 7 e Windows. Mínimo: <b>0</b> Máximo: <b>256</b>
check_type	String	Tipo de linha de base. Os valores de check_type e check_name são os mesmos para servidores Linux. Por exemplo, ambos podem ser definidos como SSH ou CentOS 7. Para servidores Windows, os valores de check_type e check_name são diferentes. Por exemplo, check_type pode ser definido como Windows Server 2019 R2 ou Windows Server 2016 R2. Mínimo: <b>0</b> Máximo: <b>256</b>
standard	String	Tipo padrão. Seu valor pode ser: <ul style="list-style-type: none"><li>● cn_standard: padrão de conformidade DJCP MLPS</li><li>● hw_standard: padrão de prática de segurança na nuvem</li></ul> Mínimo: <b>0</b> Máximo: <b>16</b>

Parâmetro	Tipo	Descrição
check_rule_name	String	Nome do item de verificação Mínimo: <b>0</b> Máximo: <b>2048</b>
check_rule_id	String	ID do item de verificação Mínimo: <b>0</b> Máximo: <b>64</b>
host_num	Integer	O número de servidores nos quais a detecção de linha de base atual é executada. Mínimo: <b>0</b> Máximo: <b>2147483647</b>
scan_result	String	Resultado da detecção. Seu valor pode ser: <ul style="list-style-type: none"><li>● pass</li><li>● failed</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>
status	String	Status. Seu valor pode ser: <ul style="list-style-type: none"><li>● safe</li><li>● ignored</li><li>● unhandled</li><li>● fixing</li><li>● fix-failed</li><li>● verifying</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>
enable_fix	Integer	Indica se há suporte para reparo com um clique. 1: sim; 0: não. Mínimo: <b>0</b> Máximo: <b>2147483647</b>
enable_click	Boolean	Indica se os botões reparar, ignorar e verificar do item de verificação podem ser clicados. true: o botão pode ser clicado. false: o botão não pode ser clicado.
rule_params	Array of <a href="#">CheckRuleFixParamInfo</a> objects	Intervalo de parâmetros aplicáveis aos itens de verificação que podem ser corrigidos por transferência de parâmetros. Esse parâmetro é retornado apenas para itens de verificação que oferecem suporte à correção de transferência de parâmetro. Comprimento da matriz: <b>0–2147483647</b>

**Tabela 3-157** CheckRuleFixParamInfo

Parâmetro	Tipo	Descrição
rule_param_id	Integer	ID do parâmetro do item de verificação Mínimo: <b>0</b> Máximo: <b>10</b>
rule_desc	String	Descrição do parâmetro do item de verificação Mínimo: <b>0</b> Máximo: <b>256</b>
default_value	Integer	Valores padrão dos parâmetros do item de verificação Mínimo: <b>0</b> Máximo: <b>2147483647</b>
range_min	Integer	Valor mínimo dos parâmetros do item de verificação Mínimo: <b>0</b> Máximo: <b>2147483647</b>
range_max	Integer	Valor máximo dos parâmetros do item de verificação Mínimo: <b>0</b> Máximo: <b>2147483647</b>

## Exemplo de solicitações

Essa API é usada para consultar os itens de verificação cujo nome de linha de base é SSH, o padrão de verificação é o padrão de prática de segurança na nuvem e o ID do projeto empresarial é xxx.

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

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

## Exemplo de respostas

### Código de status: 200

Lista de verificação do item de configuração de segurança especificado

```
{
  "total_num" : 1,
  "data_list" : [ {
    "check_rule_id" : "1.1",
    "check_rule_name" : "Rule:Ensure that permissions on /etc/ssh/sshd_config are
configured.",
    "check_type" : "SSH",
    "host_num" : 2,
    "standard" : "hw_standard",
    "scan_result" : "failed",
    "severity" : "High",
    "status" : "unhandled",
```

```
"enable_fix" : 1,
"enable_click" : true,
"rule_params" : [ {
  "rule_param_id" : 1,
  "rule_desc" : "Set the timeout duration.",
  "default_value" : 5,
  "range_min" : 1,
  "range_max" : 10
}, {
  "rule_param_id" : 2,
  "rule_desc" : "Set the number of restarts.",
  "default_value" : 10,
  "range_min" : 1,
  "range_max" : 20
} ]
} ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

Essa API é usada para consultar os itens de verificação cujo nome de linha de base é SSH, o padrão de verificação é o padrão de prática de segurança na nuvem e o ID do projeto empresarial é xxx.

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

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

public class ListRiskConfigCheckRulesSolution {

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

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

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

        ListRiskConfigCheckRulesRequest request = new
        ListRiskConfigCheckRulesRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withStandard("<standard>");
        request.withResultType("<result_type>");
        request.withCheckRuleName("<check_rule_name>");
    }
}
```

```
request.withSeverity("<severity>");
request.withHostId("<host_id>");
request.withLimit("<limit>");
request.withOffset("<offset>");
try {
    ListRiskConfigCheckRulesResponse response =
client.listRiskConfigCheckRules(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

Essa API é usada para consultar os itens de verificação cujo nome de linha de base é SSH, o padrão de verificação é o padrão de prática de segurança na nuvem e o ID do projeto empresarial é xxx.

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListRiskConfigCheckRulesRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.standard = "<standard>"
        request.result_type = "<result_type>"
        request.check_rule_name = "<check_rule_name>"
        request.severity = "<severity>"
        request.host_id = "<host_id>"
        request.limit = <limit>
        request.offset = <offset>
        response = client.list_risk_config_check_rules(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
```



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

## Go

Essa API é usada para consultar os itens de verificação cujo nome de linha de base é SSH, o padrão de verificação é o padrão de prática de segurança na nuvem e o ID do projeto empresarial é xxx.

```
package main

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

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

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

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

    request := &model.ListRiskConfigCheckRulesRequest{}
    enterpriseProjectIdRequest := "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    request.Standard = "<standard>"
    resultTypeRequest := "<result_type>"
    request.ResultType = &resultTypeRequest
    checkRuleNameRequest := "<check_rule_name>"
    request.CheckRuleName = &checkRuleNameRequest
    severityRequest := "<severity>"
    request.Severity = &severityRequest
    hostIdRequest := "<host_id>"
    request.HostId = &hostIdRequest
    limitRequest := int32(<limit>)
    request.Limit = &limitRequest
    offsetRequest := int32(<offset>)
    request.Offset = &offsetRequest
    response, err := client.ListRiskConfigCheckRules(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de verificação do item de configuração de segurança especificado

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.3.6 Consulta da lista de servidores afetados de um item de configuração de segurança

#### Função

Essa API é usada para consultar a lista de servidores afetados de um item de configuração de segurança especificado.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/baseline/risk-config/{check\_name}/hosts

**Tabela 3-158** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>20</b> Máximo: <b>64</b>
check_name	Sim	String	Nome da linha de base, por exemplo, SSH, CentOS 7 e Windows. Mínimo: <b>0</b> Máximo: <b>256</b>

**Tabela 3-159** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>64</b>
standard	Sim	String	Tipo padrão. Seu valor pode ser: <ul style="list-style-type: none"><li>● cn_standard: padrão de conformidade DJCP MLPS</li><li>● hw_standard: padrão de prática de segurança na nuvem</li></ul> Mínimo: <b>0</b> Máximo: <b>32</b>
host_name	Não	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>256</b>
host_ip	Não	String	Endereço IP do servidor Mínimo: <b>0</b> Máximo: <b>256</b>
limit	Não	Integer	Número de itens por página Mínimo: <b>0</b> Máximo: <b>200</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>

## Parâmetros de solicitação

**Tabela 3-160** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>32</b> Máximo: <b>2097152</b>

## Parâmetros de resposta

**Código de status: 200****Tabela 3-161** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Long	Quantidade total de dados afetados pela verificação de configuração Mínimo: <b>0</b> Máximo: <b>2147483647</b>
data_list	Array of <b>SecurityCheckHostInfoResponseInfo</b> objects	Lista de dados Comprimento da matriz: <b>0–2147483647</b>

**Tabela 3-162** SecurityCheckHostInfoResponseInfo

Parâmetro	Tipo	Descrição
host_id	String	ID do host Mínimo: <b>0</b> Máximo: <b>64</b>
host_name	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>256</b>

Parâmetro	Tipo	Descrição
host_public_ip	String	Endereço IP público do servidor Mínimo: <b>0</b> Máximo: <b>128</b>
host_private_ip	String	Endereço IP privado de servidor Mínimo: <b>0</b> Máximo: <b>256</b>
scan_time	Long	Tempo de verificação (ms) Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b>
failed_num	Integer	Número de itens de risco Mínimo: <b>0</b> Máximo: <b>2147483647</b>
passed_num	Integer	Número de itens passados Mínimo: <b>0</b> Máximo: <b>2147483647</b>

## Exemplo de solicitações

Essa API é usada para consultar a lista de servidores afetados cujo nome de linha de base é SSH, o padrão de verificação é o padrão de prática de segurança na nuvem e o ID do projeto empresarial é xxx.

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

## Exemplo de respostas

**Código de status: 200**

Servidores afetados pelo item de configuração de segurança

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

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

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

public class ListRiskConfigHostsSolution {

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

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

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

        ListRiskConfigHostsRequest request = new ListRiskConfigHostsRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withStandard("<standard>");
        request.withHostName("<host_name>");
        request.withHostIp("<host_ip>");
        request.withLimit(<limit>);
        request.withOffset(<offset>);
        try {
            ListRiskConfigHostsResponse response =
client.listRiskConfigHosts(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListRiskConfigHostsRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.standard = "<standard>"
        request.host_name = "<host_name>"
        request.host_ip = "<host_ip>"
        request.limit = <limit>
        request.offset = <offset>
        response = client.list_risk_config_hosts(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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

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

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

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

```
enterpriseProjectIdRequest:= "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
request.Standard = "<standard>"
hostNameRequest:= "<host_name>"
request.HostName = &hostNameRequest
hostIpRequest:= "<host_ip>"
request.HostIp = &hostIpRequest
limitRequest:= int32(<limit>)
request.Limit = &limitRequest
offsetRequest:= int32(<offset>)
request.Offset = &offsetRequest
response, err := client.ListRiskConfigHosts(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Servidores afetados pelo item de configuração de segurança

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.3.7 Consulta do relatório de um item de verificação em uma verificação de configuração de segurança

### Função

Essa API é usada para consultar o relatório de um item de verificação em uma verificação de configuração de segurança.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/baseline/check-rule/detail



**Tabela 3-163** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>20</b> Máximo: <b>64</b>

**Tabela 3-164** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Mínimo: <b>0</b> Máximo: <b>64</b>
check_name	Sim	String	Nome da linha de base, por exemplo, SSH, CentOS 7 e Windows. Mínimo: <b>0</b> Máximo: <b>255</b>
check_type	Sim	String	Tipo de linha de base. Os valores de check_type e check_name são os mesmos para servidores Linux. Por exemplo, ambos podem ser definidos como SSH ou CentOS 7. Para servidores Windows, os valores de check_type e check_name são diferentes. Por exemplo, check_type pode ser definido como Windows Server 2019 R2 ou Windows Server 2016 R2. Mínimo: <b>0</b> Máximo: <b>255</b>
check_rule_id	Sim	String	ID do item de verificação, que pode ser obtido a partir dos dados de retorno desta API: /v5/{project_id}/baseline/risk-config/{check_name}/check-rules Mínimo: <b>0</b> Máximo: <b>255</b>

Parâmetro	Obrigatório	Tipo	Descrição
standard	Sim	String	Tipo padrão. Seu valor pode ser: <ul style="list-style-type: none"><li>● cn_standard: padrão de conformidade DJCP MLPS</li><li>● hw_standard: padrão de prática de segurança na nuvem</li></ul> Mínimo: <b>0</b> Máximo: <b>32</b>
host_id	Não	String	ID do host Mínimo: <b>0</b> Máximo: <b>64</b>

## Parâmetros de solicitação

Tabela 3-165 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token de usuário, que pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de <b>X-Subject-Token</b> no cabeçalho da resposta é o token do usuário. Mínimo: <b>32</b> Máximo: <b>2097152</b>

## Parâmetros de resposta

Código de status: **200**

Tabela 3-166 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
description	String	Descrição do item de verificação atual (regra de detecção). Mínimo: <b>0</b> Máximo: <b>2048</b>

Parâmetro	Tipo	Descrição
reference	String	Base para a configuração do item de verificação (regra) Mínimo: <b>0</b> Máximo: <b>255</b>
audit	String	Descrição da auditoria do item de verificação (regra) Mínimo: <b>0</b> Máximo: <b>65534</b>
remediation	String	Sugestões de modificação para o item de verificação (regra) Mínimo: <b>0</b> Máximo: <b>65534</b>
check_info_list	Array of <b>CheckRuleCheckCaseResponseInfo</b> objects	Casos de teste Comprimento da matriz: <b>0–2147483647</b>

**Tabela 3-167** CheckRuleCheckCaseResponseInfo

Parâmetro	Tipo	Descrição
check_description	String	Descrição do caso de teste Mínimo: <b>0</b> Máximo: <b>65534</b>
current_value	String	Resultado atual Mínimo: <b>0</b> Máximo: <b>65534</b>
suggest_value	String	Resultado esperado Mínimo: <b>0</b> Máximo: <b>65534</b>

## Exemplo de solicitações

Essa API é usada para consultar o relatório dos itens de verificação de configuração cujo nome de linha de base é SSH, o ID do item de verificação é 1.12, o padrão de verificação é o padrão de prática de segurança de nuvem e o ID do projeto empresarial é xxx.

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

## Exemplo de respostas

### Código de status: 200

#### Relatório de verificação de item de configuração

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ShowCheckRuleDetailSolution {

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

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

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ShowCheckRuleDetailRequest request = new ShowCheckRuleDetailRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
    }
}
```

```
request.withCheckName("<check_name>");
request.withCheckType("<check_type>");
request.withCheckRuleId("<check_rule_id>");
request.withStandard("<standard>");
request.withHostId("<host_id>");
try {
    ShowCheckRuleDetailResponse response =
client.showCheckRuleDetail(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.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 huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ShowCheckRuleDetailRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.check_name = "<check_name>"
        request.check_type = "<check_type>"
        request.check_rule_id = "<check_rule_id>"
        request.standard = "<standard>"
        request.host_id = "<host_id>"
        response = client.show_check_rule_detail(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ShowCheckRuleDetailRequest{}
    enterpriseProjectIdRequest := "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    request.CheckName = "<check_name>"
    request.CheckType = "<check_type>"
    request.CheckRuleId = "<check_rule_id>"
    request.Standard = "<standard>"
    hostIdRequest := "<host_id>"
    request.HostId = &hostIdRequest
    response, err := client.ShowCheckRuleDetail(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Relatório de verificação de item de configuração

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.3.8 Ignoração, cancelamento da ignoração, reparação ou verificação dos itens de verificação de configuração com falha

#### Função

Ignorar, cancelar a ignorar, reparar ou verificar os itens de verificação de configuração com falha.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

PUT /v5/{project\_id}/baseline/check-rule/action

Tabela 3-168 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>20</b> Máximo: <b>64</b>

Tabela 3-169 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>64</b>
host_id	Não	String	ID do servidor. Se esse parâmetro não for especificado, todos os servidores do usuário serão consultados. Mínimo: <b>0</b> Máximo: <b>64</b>

Parâmetro	Obrigatório	Tipo	Descrição
action	Sim	String	Ação. <ul style="list-style-type: none"> <li>● ignore</li> <li>● unignore</li> <li>● fix</li> <li>● verify</li> </ul> Padrão: <b>ignore</b> Mínimo: <b>0</b> Máximo: <b>32</b>

## Parâmetros de solicitação

**Tabela 3-170** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando uma API do IAM. O valor de X-Subject-Token no cabeçalho de resposta é o token do usuário. Mínimo: <b>32</b> Máximo: <b>2097152</b>

**Tabela 3-171** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
check_rules	Não	Array of <b>CheckRuleKeyInfoRequestInfo</b> objects	Lista de IDs de itens de verificação Comprimento da matriz: <b>0–2147483647</b>

**Tabela 3-172** CheckRuleKeyInfoRequestInfo

Parâmetro	Obrigatório	Tipo	Descrição
check_name	Não	String	Nome da linha de base, por exemplo, SSH, CentOS 7 e Windows. Mínimo: <b>0</b> Máximo: <b>256</b>



Parâmetro	Obrigatório	Tipo	Descrição
check_rule_id	Não	String	ID do item de verificação, que pode ser obtido a partir dos dados de retorno desta API: /v5/{project_id}/baseline/risk-config/{check_name}/check-rules Mínimo: <b>0</b> Máximo: <b>64</b>
standard	Não	String	Padrões de linha de base. As opções são as seguintes: <ul style="list-style-type: none"><li>● cn_standard: padrão de conformidade DJCP MLPS</li><li>● hw_standard: padrão de prática de segurança na nuvem</li></ul> Mínimo: <b>0</b> Máximo: <b>16</b>
fix_values	Não	Array of <b>CheckRuleFixValuesInfo</b> objects	Parâmetros de reparo de itens de verificação inseridos pelo usuário Comprimento da matriz: <b>0-10000</b>

Tabela 3-173 CheckRuleFixValuesInfo

Parâmetro	Obrigatório	Tipo	Descrição
rule_param_id	Não	Integer	ID do parâmetro do item de verificação Mínimo: <b>0</b> Máximo: <b>2147483647</b>
fix_value	Não	Integer	Valor do parâmetro do item de verificação Mínimo: <b>0</b> Máximo: <b>2147483647</b>

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

- Essa API é usada para ignorar os itens de verificação de configuração cujo nome de linha de base é SSH, o ID do item de verificação é 1.11, o padrão de verificação é o padrão de prática de segurança na nuvem e o ID do projeto empresarial é xxx. Esta operação se aplica a todos os servidores afetados.

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

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

- Essa API é usada para restaurar os itens de verificação de configuração cujo nome de linha de base é SSH, o ID do item de verificação é 1.11, o padrão de verificação é o padrão de prática de segurança na nuvem e o ID do projeto empresarial é xxx. Esta operação se aplica apenas ao servidor cujo ID é xxx. Os parâmetros de restauração são os seguintes: defina o valor do item de reparo cujo ID é de 1 a 5 e o valor do item de reparo cujo ID é de 2 a 20.

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

```
{
  "check_rules" : [ {
    "check_name" : "SSH",
    "check_rule_id" : "1.11",
    "standard" : "hw_standard",
    "fix_values" : [ {
      "rule_param_id" : 1,
      "fix_value" : 5
    }, {
      "rule_param_id" : 2,
      "fix_value" : 20
    } ]
  } ]
}
```

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

- Essa API é usada para ignorar os itens de verificação de configuração cujo nome de linha de base é SSH, o ID do item de verificação é 1.11, o padrão de verificação é o padrão de prática de segurança na nuvem e o ID do projeto empresarial é xxx. Esta operação se aplica a todos os servidores afetados.

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

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

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

```
public class ChangeCheckRuleActionSolution {

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

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

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

        ChangeCheckRuleActionRequest request = new
        ChangeCheckRuleActionRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withHostId("<host_id>");
        request.withAction("<action>");
        CheckRuleIdListRequestInfo body = new CheckRuleIdListRequestInfo();
        List<CheckRuleKeyInfoRequestInfo> listbodyCheckRules = new
        ArrayList<>();
        listbodyCheckRules.add(
            new CheckRuleKeyInfoRequestInfo()
                .withCheckName("SSH")
                .withCheckRuleId("1.11")
                .withStandard("hw_standard")
        );
        body.withCheckRules(listbodyCheckRules);
        request.withBody(body);
        try {
            ChangeCheckRuleActionResponse response =
            client.changeCheckRuleAction(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrMsg());
        }
    }
}
```

- Essa API é usada para restaurar os itens de verificação de configuração cujo nome de linha de base é SSH, o ID do item de verificação é 1.11, o padrão de verificação é o padrão de prática de segurança na nuvem e o ID do projeto empresarial é xxx. Esta operação se aplica apenas ao servidor cujo ID é xxx. Os parâmetros de restauração são os seguintes: defina o valor do item de reparo cujo ID é de 1 a 5 e o valor do item de reparo cujo ID é de 2 a 20.

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

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

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

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

public class ChangeCheckRuleActionSolution {

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

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

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

        ChangeCheckRuleActionRequest request = new
        ChangeCheckRuleActionRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withHostId("<host_id>");
        request.withAction("<action>");
        CheckRuleIdListRequestInfo body = new CheckRuleIdListRequestInfo();
        List<CheckRuleFixValuesInfo> listCheckRulesFixValues = new
        ArrayList<>();
        listCheckRulesFixValues.add(
            new CheckRuleFixValuesInfo()
                .withRuleParamId(1)
                .withFixValue(5)
        );
        listCheckRulesFixValues.add(
            new CheckRuleFixValuesInfo()
                .withRuleParamId(2)
                .withFixValue(20)
        );
        List<CheckRuleKeyInfoRequestInfo> listbodyCheckRules = new
        ArrayList<>();
        listbodyCheckRules.add(
            new CheckRuleKeyInfoRequestInfo()
                .withCheckName("SSH")
                .withCheckRuleId("1.11")
                .withStandard("hw_standard")
                .withFixValues(listCheckRulesFixValues)
        );
        body.withCheckRules(listbodyCheckRules);
        request.withBody(body);
        try {
            ChangeCheckRuleActionResponse response =
            client.changeCheckRuleAction(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
        }
    }
}
```

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

## Python

- Essa API é usada para ignorar os itens de verificação de configuração cujo nome de linha de base é SSH, o ID do item de verificação é 1.11, o padrão de verificação é o padrão de prática de segurança na nuvem e o ID do projeto empresarial é xxx. Esta operação se aplica a todos os servidores afetados.

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ChangeCheckRuleActionRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.host_id = "<host_id>"
        request.action = "<action>"
        listCheckRulesbody = [
            CheckRuleKeyInfoRequestInfo(
                check_name="SSH",
                check_rule_id="1.11",
                standard="hw_standard"
            )
        ]
        request.body = CheckRuleIdListRequestInfo(
            check_rules=listCheckRulesbody
        )
        response = client.change_check_rule_action(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

- Essa API é usada para restaurar os itens de verificação de configuração cujo nome de linha de base é SSH, o ID do item de verificação é 1.11, o padrão de verificação é o padrão de prática de segurança na nuvem e o ID do projeto empresarial é xxx. Esta operação se aplica apenas ao servidor cujo ID é xxx. Os parâmetros de restauração são os seguintes: defina o valor do item de reparo cujo ID é de 1 a 5 e o valor do item de reparo cujo ID é de 2 a 20.

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ChangeCheckRuleActionRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.host_id = "<host_id>"
        request.action = "<action>"
        listFixValuesCheckRules = [
            CheckRuleFixValuesInfo(
                rule_param_id=1,
                fix_value=5
            ),
            CheckRuleFixValuesInfo(
                rule_param_id=2,
                fix_value=20
            )
        ]
        listCheckRulesbody = [
            CheckRuleKeyInfoRequestInfo(
                check_name="SSH",
                check_rule_id="1.11",
                standard="hw_standard",
                fix_values=listFixValuesCheckRules
            )
        ]
        request.body = CheckRuleIdListRequestInfo(
            check_rules=listCheckRulesbody
        )
        response = client.change_check_rule_action(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

- Essa API é usada para ignorar os itens de verificação de configuração cujo nome de linha de base é SSH, o ID do item de verificação é 1.11, o padrão de verificação é o padrão de prática de segurança na nuvem e o ID do projeto empresarial é xxx. Esta operação se aplica a todos os servidores afetados.

```
package main

import (
```

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

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

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

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

    request := &model.ChangeCheckRuleActionRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        hostIdRequest:= "<host_id>"
        request.HostId = &hostIdRequest
        request.Action = "<action>"
        checkNameCheckRules:= "SSH"
        checkRuleIdCheckRules:= "1.11"
        standardCheckRules:= "hw_standard"
        var listCheckRulesbody = []model.CheckRuleKeyInfoRequestInfo{
            {
                CheckName: &checkNameCheckRules,
                CheckRuleId: &checkRuleIdCheckRules,
                Standard: &standardCheckRules,
            },
        }
        request.Body = &model.CheckRuleIdListRequestInfo{
            CheckRules: &listCheckRulesbody,
        }
        response, err := client.ChangeCheckRuleAction(request)
        if err == nil {
            fmt.Printf("%+v\n", response)
        } else {
            fmt.Println(err)
        }
    }
}
```

- Essa API é usada para restaurar os itens de verificação de configuração cujo nome de linha de base é SSH, o ID do item de verificação é 1.11, o padrão de verificação é o padrão de prática de segurança na nuvem e o ID do projeto empresarial é xxx. Esta operação se aplica apenas ao servidor cujo ID é xxx. Os parâmetros de restauração são os seguintes: defina o valor do item de reparo cujo ID é de 1 a 5 e o valor do item de reparo cujo ID é de 2 a 20.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
```

```
hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/
region"
)

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

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

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

    request := &model.ChangeCheckRuleActionRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        hostIdRequest:= "<host_id>"
        request.HostId = &hostIdRequest
        request.Action = "<action>"
        ruleParamIdFixValues:= int32(1)
        fixValueFixValues:= int32(5)
        ruleParamIdFixValues1:= int32(2)
        fixValueFixValues1:= int32(20)
        var listFixValuesCheckRules = []model.CheckRuleFixValuesInfo{
            {
                RuleParamId: &ruleParamIdFixValues,
                FixValue: &fixValueFixValues,
            },
            {
                RuleParamId: &ruleParamIdFixValues1,
                FixValue: &fixValueFixValues1,
            },
        }
        checkNameCheckRules:= "SSH"
        checkRuleIdCheckRules:= "1.11"
        standardCheckRules:= "hw_standard"
        var listCheckRulesbody = []model.CheckRuleKeyInfoRequestInfo{
            {
                CheckName: &checkNameCheckRules,
                CheckRuleId: &checkRuleIdCheckRules,
                Standard: &standardCheckRules,
                FixValues: &listFixValuesCheckRules,
            },
        }
        request.Body = &model.CheckRuleIdListRequestInfo{
            CheckRules: &listCheckRulesbody,
        }
        response, err := client.ChangeCheckRuleAction(request)
        if err == nil {
            fmt.Printf("%v\n", response)
        } else {
            fmt.Println(err)
        }
    }
}
```



## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Execução concluída

## Códigos de erro

Consulte [Códigos de erro](#).

# 3.4 Gerenciamento de cotas

## 3.4.1 Consulta de informações de cota

### Função

Essa API é usada para consultar informações de cotas.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/billing/quotas

**Tabela 3-174** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>128</b>

**Tabela 3-175** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>
version	Não	String	Edição do HSS. Seu valor pode ser: <ul style="list-style-type: none"> <li>● hss.version.null</li> <li>● hss.version.basic: edição básica</li> <li>● hss.version.advanced: edição profissional</li> <li>● hss.version.enterprise: edição empresarial</li> <li>● hss.version.premium: edição premium</li> <li>● hss.version.wtp: edição WTP</li> <li>● hss.version.container.enterprise : edição de container</li> </ul> Mínimo: <b>1</b> Máximo: <b>64</b>
charging_mode	Não	String	Modo de cobrança. Seu valor pode ser: <ul style="list-style-type: none"> <li>● packet_cycle: anual/mensal</li> <li>● on_demand: pagamento por uso</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>

## Parâmetros de solicitação

**Tabela 3-176** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>32</b> Máximo: <b>4096</b>
region	Não	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-177** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
data_list	Array of <b>ResourceQuotasInfo</b> objects	Lista de estatísticas de cota Comprimento da matriz: <b>0–200</b>

**Tabela 3-178** ResourceQuotasInfo

Parâmetro	Tipo	Descrição
version	String	Edição do HSS. Seu valor pode ser: <ul style="list-style-type: none"> <li>● hss.version.null</li> <li>● hss.version.basic: edição básica</li> <li>● hss.version.advanced: edição profissional</li> <li>● hss.version.enterprise: edição empresarial</li> <li>● hss.version.premium: edição premium</li> <li>● hss.version.wtp: edição WTP</li> <li>● hss.version.container.enterprise: edição de container</li> </ul> Mínimo: <b>1</b> Máximo: <b>64</b>
total_num	Integer	Cotas totais Mínimo: <b>0</b> Máximo: <b>2000000</b>
used_num	Integer	Cotas usadas Mínimo: <b>0</b> Máximo: <b>2000000</b>
available_num	Integer	Cotas totais Mínimo: <b>0</b> Máximo: <b>2000000</b>
available_resources_list	Array of <a href="#">AvailableResourceIdsInfo</a> objects	Lista de recursos disponíveis Comprimento da matriz: <b>0–200</b>

**Tabela 3-179** AvailableResourceIdsInfo

Parâmetro	Tipo	Descrição
resource_id	String	ID do recurso Mínimo: <b>1</b> Máximo: <b>256</b>
current_time	String	Hora atual Mínimo: <b>1</b> Máximo: <b>64</b>

Parâmetro	Tipo	Descrição
shared_quota	String	Se as cotas são compartilhadas. Seu valor pode ser: <ul style="list-style-type: none"><li>● shared</li><li>● unshared</li></ul> Mínimo: 1 Máximo: 64

## Exemplo de solicitações

Essa API é usada para consultar cotas da edição básica em todos os projetos empresariais.

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

## Exemplo de respostas

**Código de status: 200**

Lista de estatísticas de cota

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ShowResourceQuotasSolution {

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

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

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

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();
ShowResourceQuotasRequest request = new ShowResourceQuotasRequest();
request.withEnterpriseProjectId("<enterprise_project_id>");
request.withVersion("<version>");
request.withChargingMode("<charging_mode>");
try {
    ShowResourceQuotasResponse response =
client.showResourceQuotas(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.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 huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ShowResourceQuotasRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.version = "<version>"
        request.charging_mode = "<charging_mode>"
```

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

## Go

```
package main

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

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

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

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

    request := &model.ShowResourceQuotasRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        versionRequest:= "<version>"
        request.Version = &versionRequest
        chargingModeRequest:= "<charging_mode>"
        request.ChargingMode = &chargingModeRequest
    }
    response, err := client.ShowResourceQuotas(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de estatísticas de cota

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.4.2 Consulta de detalhes da cota

### Função

Essa API é usada para consultar detalhes da cota.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/billing/quotas-detail

**Tabela 3-180** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-181** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>



Parâmetro	Obrigatório	Tipo	Descrição
version	Não	String	Edição do HSS. Seu valor pode ser: <ul style="list-style-type: none"> <li>● hss.version.null</li> <li>● hss.version.basic: edição básica</li> <li>● hss.version.advanced: edição profissional</li> <li>● hss.version.enterprise: edição empresarial</li> <li>● hss.version.premium: edição premium</li> <li>● hss.version.wtp: edição WTP</li> <li>● hss.version.container.enterprise : edição de container</li> </ul> Mínimo: <b>1</b> Máximo: <b>64</b>
category	Não	String	Tipo. Seu valor pode ser: <ul style="list-style-type: none"> <li>● host_resource</li> <li>● container_resource</li> </ul> Mínimo: <b>1</b> Máximo: <b>64</b>
quota_status	Não	String	Status da cota. Pode ser: <ul style="list-style-type: none"> <li>● QUOTA_STATUS_NORMAL <ul style="list-style-type: none"> <li>– QUOTA_STATUS_EXPIRED</li> <li>– QUOTA_STATUS_FREEZE</li> </ul> </li> </ul> Mínimo: <b>1</b> Máximo: <b>64</b>
used_status	Não	String	Status de uso. Pode ser: <ul style="list-style-type: none"> <li>● USED_STATUS_IDLE</li> <li>● USED_STATUS_USED</li> </ul> Mínimo: <b>1</b> Máximo: <b>64</b>
host_name	Não	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>128</b>

Parâmetro	Obrigatório	Tipo	Descrição
resource_id	Não	String	Especifica o ID do recurso da cota do HSS. Mínimo: <b>0</b> Máximo: <b>128</b>
charging_mode	Não	String	Modo de cobrança. Seu valor pode ser: <ul style="list-style-type: none"><li>● packet_cycle: anual/mensal</li><li>● on_demand: pagamento por uso</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
limit	Não	Integer	Número de itens por página Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>

## Parâmetros de solicitação

Tabela 3-182 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>32</b> Máximo: <b>4096</b>
region	Não	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

Código de status: 200

Tabela 3-183 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
packet_cycle_num	Integer	Cotas anuais/mensais Mínimo: 0 Máximo: <b>10000000</b>
on_demand_num	Integer	Cotas de pagamento por uso Mínimo: 0 Máximo: <b>10000000</b>
used_num	Integer	Cotas usadas Mínimo: 0 Máximo: <b>10000000</b>
idle_num	Integer	Cotas ociosas Mínimo: 0 Máximo: <b>10000000</b>
normal_num	Integer	Cotas normais Mínimo: 0 Máximo: <b>10000000</b>
expired_num	Integer	Cotas expiradas Mínimo: 0 Máximo: <b>10000000</b>
freeze_num	Integer	Cotas congeladas Mínimo: 0 Máximo: <b>10000000</b>
quota_statistics_list	Array of <b>QuotaStatisticsResponseInfo</b> objects	Lista de estatísticas de cota Comprimento da matriz: <b>0-200</b>
total_num	Integer	Cotas totais Mínimo: 0 Máximo: <b>10000000</b>
data_list	Array of <b>QuotaResourcesResponseInfo</b> objects	Lista de cotas Comprimento da matriz: <b>0-200</b>

**Tabela 3-184** QuotaStatisticsResponseInfo

Parâmetro	Tipo	Descrição
version	String	Flavor do recurso. Seu valor pode ser: <ul style="list-style-type: none"> <li>● hss.version.basic: edição básica</li> <li>● hss.version.advanced: edição profissional</li> <li>● hss.version.enterprise: edição empresarial</li> <li>● hss.version.premium: edição premium</li> <li>● hss.version.wtp: edição WTP</li> <li>● hss.version.container: edição de container</li> </ul> Mínimo: <b>1</b> Máximo: <b>64</b>
total_num	Integer	Cotas totais Mínimo: <b>0</b> Máximo: <b>10000000</b>

**Tabela 3-185** QuotaResourcesResponseInfo

Parâmetro	Tipo	Descrição
resource_id	String	ID de recurso de uma cota de HSS Mínimo: <b>0</b> Máximo: <b>256</b>
version	String	Flavor do recurso. Seu valor pode ser: <ul style="list-style-type: none"> <li>● hss.version.basic: edição básica</li> <li>● hss.version.advanced: edição profissional</li> <li>● hss.version.enterprise: edição empresarial</li> <li>● hss.version.premium: edição premium</li> <li>● hss.version.wtp: edição WTP</li> <li>● hss.version.container: edição de container</li> </ul> Mínimo: <b>1</b> Máximo: <b>64</b>
quota_status	String	Status da cota. Pode ser: <ul style="list-style-type: none"> <li>● normal</li> <li>● expired</li> <li>● freeze</li> </ul> Mínimo: <b>1</b> Máximo: <b>64</b>

Parâmetro	Tipo	Descrição
used_status	String	Status de uso. Seu valor pode ser: <ul style="list-style-type: none"><li>● idle</li><li>● used</li></ul> Mínimo: <b>1</b> Máximo: <b>64</b>
host_id	String	ID do host Mínimo: <b>1</b> Máximo: <b>64</b>
host_name	String	Nome de servidor Mínimo: <b>1</b> Máximo: <b>128</b>
charging_mode	String	Modo de cobrança. Seu valor pode ser: <ul style="list-style-type: none"><li>● packet_cycle: anual/mensal</li><li>● on_demand: pagamento por uso</li></ul> Mínimo: <b>1</b> Máximo: <b>64</b>
tags	Array of <b>TagInfo</b> objects	Tag Comprimento da matriz: <b>0–2097152</b>
expire_time	Long	Tempo de expiração. O valor -1 indica que o recurso não expirará. Mínimo: <b>0</b> Máximo: <b>2147483647</b>
shared_quota	String	Se as cotas são compartilhadas. Seu valor pode ser: <ul style="list-style-type: none"><li>● shared</li><li>● unshared</li></ul> Mínimo: <b>1</b> Máximo: <b>64</b>
enterprise_project_id	String	ID do projeto empresarial Mínimo: <b>0</b> Máximo: <b>256</b>
enterprise_project_name	String	Nome do projeto empresarial Mínimo: <b>0</b> Máximo: <b>256</b>

**Tabela 3-186** TagInfo

Parâmetro	Tipo	Descrição
key	String	Chave. Pode conter até 128 caracteres Unicode. O key não pode ser deixado em branco. Mínimo: <b>1</b> Máximo: <b>128</b>
value	String	Valor. Cada valor de tag pode conter um máximo de 255 caracteres Unicode. Mínimo: <b>1</b> Máximo: <b>255</b>

## Exemplo de solicitações

Essa API é usada para consultar detalhes de cotas em todos os projetos empresariais.

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

## Exemplo de respostas

### Código de status: 200

Detalhes da cota

```
{
  "data_list" : [ {
    "charging_mode" : "packet_cycle",
    "expire_time" : -1,
    "host_id" : "71a15ecc-049f-4cca-bd28-5e90aca1817f",
    "host_name" : "zhangxiaodong2",
    "quota_status" : "normal",
    "resource_id" : "af4d08ad-2b60-4916-a5cf-8d6a23956dda",
    "shared_quota" : "shared",
    "tags" : [ {
      "key" : "Service",
      "value" : "HSS"
    } ],
    "used_status" : "used",
    "version" : "hss.version.wtp"
  } ],
  "expired_num" : 0,
  "freeze_num" : 0,
  "idle_num" : 20,
  "normal_num" : 60,
  "on_demand_num" : 0,
  "packet_cycle_num" : 60,
  "quota_statistics_list" : [ {
    "total_num" : 8,
    "version" : "hss.version.basic"
  } ],
  "total_num" : 60,
  "used_num" : 40
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

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

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

public class ListQuotasDetailSolution {

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

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

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

        ListQuotasDetailRequest request = new ListQuotasDetailRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withVersion("<version>");
        request.withCategory("<category>");
        request.withQuotaStatus("<quota_status>");
        request.withUsedStatus("<used_status>");
        request.withHostName("<host_name>");
        request.withResourceId("<resource_id>");
        request.withChargingMode("<charging_mode>");
        request.withLimit("<limit>");
        request.withOffset("<offset>");
        try {
            ListQuotasDetailResponse response = client.listQuotasDetail(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.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 huaweicloudsdkhss.v5.region.hss_region import HssRegion
```

```
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListQuotasDetailRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.version = "<version>"
        request.category = "<category>"
        request.quota_status = "<quota_status>"
        request.used_status = "<used_status>"
        request.host_name = "<host_name>"
        request.resource_id = "<resource_id>"
        request.charging_mode = "<charging_mode>"
        request.limit = <limit>
        request.offset = <offset>
        response = client.list_quotas_detail(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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

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



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

request := &model.ListQuotasDetailRequest{}
enterpriseProjectIdRequest := "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
versionRequest := "<version>"
request.Version = &versionRequest
categoryRequest := "<category>"
request.Category = &categoryRequest
quotaStatusRequest := "<quota_status>"
request.QuotaStatus = &quotaStatusRequest
usedStatusRequest := "<used_status>"
request.UsedStatus = &usedStatusRequest
hostNameRequest := "<host_name>"
request.HostName = &hostNameRequest
resourceIdRequest := "<resource_id>"
request.ResourceId = &resourceIdRequest
chargingModeRequest := "<charging_mode>"
request.ChargingMode = &chargingModeRequest
limitRequest := int32(<limit>)
request.Limit = &limitRequest
offsetRequest := int32(<offset>)
request.Offset = &offsetRequest
response, err := client.ListQuotasDetail(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia [Código de amostra no API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Detalhes da cota

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.4.3 Criação de uma cota de pedidos por HSS

#### Função

O modo de cobrança só pode ser anual/mensal quando uma cota de pedido é criada pelo HSS.

## Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

## URI

POST /v5/{project\_id}/quotas/orders

**Tabela 3-187** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Mínimo: <b>0</b> Máximo: <b>512</b>

**Tabela 3-188** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de solicitação

**Tabela 3-189** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>0</b> Máximo: <b>4096</b>
Content-Type	Não	String	Valor padrão: application/json; charset=utf-8 Mínimo: <b>0</b> Máximo: <b>128</b>

Parâmetro	Obrigatório	Tipo	Descrição
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>32</b>

**Tabela 3-190** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
resource_spec_code	Sim	String	Especificações <ul style="list-style-type: none"> <li>● hss.version.basic: edição básica</li> <li>● hss.version.advanced: edição profissional</li> <li>● hss.version.enterprise: edição empresarial</li> <li>● hss.version.premium: edição premium</li> <li>● hss.version.wtp: edição WTP</li> <li>● hss.version.container.enterprise : edição de container</li> </ul> Mínimo: <b>0</b> Máximo: <b>128</b>
period_type	Sim	Integer	Tipo de período de assinatura. <ul style="list-style-type: none"> <li>● 2: mês</li> <li>● 3: ano</li> </ul> Mínimo: <b>0</b> Máximo: <b>100</b>
period_num	Sim	Integer	Número de períodos de assinatura Mínimo: <b>0</b> Máximo: <b>1000</b>
is_auto_renew	Não	Boolean	Se deve oferecer suporte à renovação automática. As opções são true (sim) e false (não). O valor padrão é false.
is_auto_pay	Não	Boolean	Se deve suportar o pagamento automático. As opções são true (sim) e false (não). O valor padrão é false.
subscription_num	Sim	Integer	Quantidade de assinatura Mínimo: <b>0</b> Máximo: <b>500</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-191** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
order_id	String	ID do pedido Mínimo: <b>0</b> Máximo: <b>256</b>

## Exemplo de solicitações

Criar um pedido de cota de edição empresarial do HSS. As informações do pedido são as seguintes. O modo de cobrança é anual/mensal. A quantidade é 1. O período de assinatura é 1. O tipo de período de assinatura é mensal. A renovação automática está desativada. O pedido será pago automaticamente.

```
POST https://{endpoint}/v5/{project_id}/quotas/orders
{
  "resource_spec_code" : "hss.version.enterprise",
  "subscription_num" : 1,
  "period_num" : 1,
  "period_type" : 2,
  "is_auto_renew" : 0,
  "is_auto_pay" : 1
}
```

## Exemplo de respostas

**Código de status: 200**

Informações sobre pedidos

```
{
  "order_id" : "CS2404171733"
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

Criar um pedido de cota de edição empresarial do HSS. As informações do pedido são as seguintes. O modo de cobrança é anual/mensal. A quantidade é 1. O período de assinatura é 1. O tipo de período de assinatura é mensal. A renovação automática está desativada. O pedido será pago automaticamente.

```
package com.huaweicloud.sdk.test;
import com.huaweicloud.sdk.core.auth.ICredential;
```

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

public class CreateQuotasOrderSolution {

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

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

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        CreateQuotasOrderRequest request = new CreateQuotasOrderRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        CreateQuotasOrderRequestInfo body = new CreateQuotasOrderRequestInfo();
        body.withSubscriptionNum(1);
        body.withIsAutoPay(1);
        body.withIsAutoRenew(0);
        body.withPeriodNum(1);
        body.withPeriodType(2);
        body.withResourceSpecCode("hss.version.enterprise");
        request.withBody(body);
        try {
            CreateQuotasOrderResponse response =
client.createQuotasOrder(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Criar um pedido de cota de edição empresarial do HSS. As informações do pedido são as seguintes. O modo de cobrança é anual/mensal. A quantidade é 1. O período de assinatura é 1. O tipo de período de assinatura é mensal. A renovação automática está desativada. O pedido será pago automaticamente.

```
# coding: utf-8
from huaweicloudsdkcore.auth.credentials import BasicCredentials
```

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = CreateQuotasOrderRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.body = CreateQuotasOrderRequestInfo(
            subscription_num=1,
            is_auto_pay=1,
            is_auto_renew=0,
            period_num=1,
            period_type=2,
            resource_spec_code="hss.version.enterprise"
        )
        response = client.create_quotas_order(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Criar um pedido de cota de edição empresarial do HSS. As informações do pedido são as seguintes. O modo de cobrança é anual/mensal. A quantidade é 1. O período de assinatura é 1. O tipo de período de assinatura é mensal. A renovação automática está desativada. O pedido será pago automaticamente.

```
package main

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

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

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

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

request := &model.CreateQuotasOrderRequest{}
enterpriseProjectIdRequest := "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
isAutoPayCreateQuotasOrderRequestInfo := 1
isAutoRenewCreateQuotasOrderRequestInfo := 0
request.Body = &model.CreateQuotasOrderRequestInfo{
    SubscriptionNum: int32(1),
    IsAutoPay: &isAutoPayCreateQuotasOrderRequestInfo,
    IsAutoRenew: &isAutoRenewCreateQuotasOrderRequestInfo,
    PeriodNum: int32(1),
    PeriodType: int32(2),
    ResourceSpecCode: "hss.version.enterprise",
}
response, err := client.CreateQuotasOrder(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia [Código de amostra no API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Informações sobre pedidos

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.4.4 Consulta de informações sobre produtos e ofertas

### Função

Esta API é usada para consultar informações sobre produtos e ofertas.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

## URI

GET /v5/{project\_id}/product/productdata/offering-infos

**Tabela 3-192** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>128</b>

**Tabela 3-193** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>
site_code	Não	String	Informações do site. <ul style="list-style-type: none"><li>● HWC_CN: China continental</li><li>● HWC_HK: internacional</li><li>● HWC_EU: Europa</li></ul> Padrão: <b>HWC_CN</b> Mínimo: <b>1</b> Máximo: <b>256</b>



## Parâmetros de solicitação

**Tabela 3-194** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>32</b> Máximo: <b>4096</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

**Código de status: 200****Tabela 3-195** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
[items]	Array of <b>ResourceProductDataObjectInfo</b> objects	Lista de dados de oferta

**Tabela 3-196** ResourceProductDataObjectInfo

Parâmetro	Tipo	Descrição
charging_mode	String	Modos de cobrança <ul style="list-style-type: none"><li>● packet_cycle: anual/mensal</li><li>● on_demand: pagamento por uso</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
is_auto_renew	Boolean	Se deve ativar a renovação automática.

Parâmetro	Tipo	Descrição
version_info	Map<String,Array<ShowPeriodResponseInfo>>	<p>Informações da edição. O valor da chave é a edição do HSS. Seu valor pode ser:</p> <ul style="list-style-type: none"> <li>● hss.version.basic: edição básica</li> <li>● hss.version.advanced: edição profissional</li> <li>● hss.version.enterprise: edição empresarial</li> <li>● hss.version.premium: edição premium</li> <li>● hss.version.wtp: edição WTP</li> <li>● hss.version.container.enterprise: edição de container</li> </ul>

**Tabela 3-197** ShowPeriodResponseInfo

Parâmetro	Tipo	Descrição
period_vals	String	<p>Cadeia de valores da duração necessária. Vários valores são separados por vírgulas (.). Por exemplo: 1,2,3,4,5,6,7,8,9</p> <p>Mínimo: 1 Máximo: 32</p>
period_unit	String	<p>Unidade de duração necessária</p> <ul style="list-style-type: none"> <li>● year: ano</li> <li>● month: mês</li> <li>● day: dia</li> </ul> <p>Mínimo: 1 Máximo: 32</p>

## Exemplo de solicitações

Nenhum

## Exemplo de respostas

**Código de status: 200**

Resposta bem-sucedida

```
{
  "data_list" : [ {
    "charging_mode" : "packet_cycle",
    "is_auto_renew" : false,
    "version_info" : {
      "hss.version.enterprise" : [ {
        "period_vals" : "1,2,3,4,5,6,7,8,9",
        "period_unit" : "month"
      }, {
        "period_vals" : "1,2,3,5",
```

```
        "period_unit" : "year"
    } ],
    "hss.version.premium" : [ {
        "period_vals" : "1,2,3,4,5,6,7,8,9",
        "period_unit" : "month"
    }, {
        "period_vals" : "1,2,3,5",
        "period_unit" : "year"
    } ]
    }
}, {
    "charging_mode" : "on_demand",
    "is_auto_renew" : false,
    "version_info" : {
        "hss.version.enterprise" : [ {
            "period_vals" : "1,2,3,4,5,6,7,8,9",
            "period_unit" : "month"
        }, {
            "period_vals" : "1,2,3,5",
            "period_unit" : "year"
        } ]
    }
} ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ShowProductdataOfferingInfosSolution {

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

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

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

        ShowProductdataOfferingInfosRequest request = new
        ShowProductdataOfferingInfosRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withSiteCode("<site_code>");
    }
}
```

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

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ShowProductdataOfferingInfosRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.site_code = "<site_code>"
        response = client.show_productdata_offering_infos(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ShowProductdataOfferingInfosRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        siteCodeRequest:= "<site_code>"
        request.SiteCode = &siteCodeRequest
    }
    response, err := client.ShowProductdataOfferingInfos(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Resposta bem-sucedida

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.5 Gerenciamento de containers

## 3.5.1 Consulta da lista de nós de container

### Função

Essa API é usada para consultar a lista de nós de container.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/container/nodes

**Tabela 3-198** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-199** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é <b>0</b> . Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
limit	Não	Integer	Número de registros exibidos em cada página. Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>

Parâmetro	Obrigatório	Tipo	Descrição
host_name	Não	String	Nome do nó. Mínimo: <b>0</b> Máximo: <b>128</b>
agent_status	Não	String	Status de agente. Pode ser: <ul style="list-style-type: none"><li>● not_installed</li><li>● online</li><li>● offline</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
protect_status	Não	String	Status de proteção. Seu valor pode ser: <ul style="list-style-type: none"><li>● closed</li><li>● opened</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
container_tags	Não	String	Rótulo, que é usado para identificar o container do CCE e os nós autoconstruídos. <ul style="list-style-type: none"><li>● cce: nós do CCE</li><li>● self: nós autoconstruídos</li><li>● other: outros nós</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>

## Parâmetros de solicitação

**Tabela 3-200** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>

Parâmetro	Obrigatório	Tipo	Descrição
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

Código de status: **200**

Tabela 3-201 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total de nós de container Mínimo: <b>0</b> Máximo: <b>65535</b>
data_list	Array of <a href="#">ContainerNodeInfo</a> objects	Lista de nós de container Comprimento da matriz: <b>0–65535</b>

Tabela 3-202 ContainerNodeInfo

Parâmetro	Tipo	Descrição
agent_id	String	ID do agente Mínimo: <b>0</b> Máximo: <b>64</b>
host_id	String	ID de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
host_name	String	Nome do nó Mínimo: <b>0</b> Máximo: <b>128</b>
host_status	String	Status do servidor. As opções são as seguintes: <ul style="list-style-type: none"><li>● ACTIVE</li><li>● SHUTOFF</li><li>● BUILDING</li><li>● ERROR</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>



Parâmetro	Tipo	Descrição
agent_status	String	Status de agente. Pode ser: <ul style="list-style-type: none"> <li>● not_installed</li> <li>● online</li> <li>● offline</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>
protect_status	String	Status de proteção. Seu valor pode ser: <ul style="list-style-type: none"> <li>● closed</li> <li>● opened</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>
protect_interrupt	Boolean	Se a proteção foi interrompida
container_tags	String	Rótulo, que é usado para identificar o container do CCE e os nós autoconstruídos. <ul style="list-style-type: none"> <li>● cce: nós do CCE</li> <li>● self: nós autoconstruídos</li> <li>● other: outros nós</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>
private_ip	String	Endereço IP privado Mínimo: <b>0</b> Máximo: <b>128</b>
public_ip	String	Endereço IP elástico (EIP) Mínimo: <b>0</b> Máximo: <b>128</b>
resource_id	String	ID da cota de HSS (UUID) Mínimo: <b>0</b> Máximo: <b>128</b>
group_name	String	ID do grupo de servidores Mínimo: <b>1</b> Máximo: <b>128</b>
enterprise_project_name	String	Nome do projeto empresarial Mínimo: <b>0</b> Máximo: <b>256</b>

Parâmetro	Tipo	Descrição
detect_result	String	Resultado da verificação do servidor. As opções são as seguintes: <ul style="list-style-type: none"><li>● undetected</li><li>● clean: nenhum risco é detectado.</li><li>● risk: os riscos são detectados.</li><li>● scanning</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
asset	Integer	Riscos de ativos Mínimo: <b>0</b> Máximo: <b>2097152</b>
vulnerability	Integer	Vulnerabilidades Mínimo: <b>0</b> Máximo: <b>2097152</b>
intrusion	Integer	Riscos de intrusão Mínimo: <b>0</b> Máximo: <b>2097152</b>
policy_group_id	String	ID do grupo de políticas Mínimo: <b>1</b> Máximo: <b>128</b>
policy_group_name	String	Nome do grupo de políticas Mínimo: <b>1</b> Máximo: <b>128</b>

## Exemplo de solicitações

Essa API é usada para consultar a lista de nós de container. Se o parâmetro limit não for definido, 10 registros serão retornados por padrão.

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

## Exemplo de respostas

**Código de status: 200**

Resposta bem-sucedida

```
{
  "total_num" : 1,
  "data_list" : [ {
    "agent_id" : "2d0fe7824005bf001220ad9d892e86f8af44xxxxxxxxxxxx",
    "agent_status" : "online",
    "host_id" : "host_id",
    "host_name" : "host_name",
```

```
"host_status" : "ACTIVE",
"protect_status" : "opened",
"protect_interrupt" : false,
"private_ip" : "192.168.0.114",
"public_ip" : "100.85.218.122",
"resource_id" : "ef5eb4fd-7376-48ac-886f-16fd057776f3",
"group_name" : "as(All projects)",
"enterprise_project_name" : "default",
"detect_result" : "risk",
"asset" : 0,
"vulnerability" : 14,
"intrusion" : 0,
"policy_group_id" : "ce4d5e95-0cbf-4102-9c77-ef1bcb6b35aa",
"policy_group_name" : "tenant_linux_enterprise_default_policy_group (All
projects)"
} ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListContainerNodesSolution {

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

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

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

        ListContainerNodesRequest request = new ListContainerNodesRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withOffset("<offset>");
        request.withLimit("<limit>");
        request.withHostName("<host_name>");
        request.withAgentStatus("<agent_status>");
        request.withProtectStatus("<protect_status>");
        request.withContainerTags("<container_tags>");
        try {
            ListContainerNodesResponse response =
                client.listContainerNodes(request);
        }
    }
}
```

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

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListContainerNodesRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.offset = <offset>
        request.limit = <limit>
        request.host_name = "<host_name>"
        request.agent_status = "<agent_status>"
        request.protect_status = "<protect_status>"
        request.container_tags = "<container_tags>"
        response = client.list_container_nodes(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

```
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in  
    plaintext, which has great security risks. It is recommended that the AK and SK  
    be stored in ciphertext in configuration files or environment variables and  
    decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for  
    authentication. Before running this example, set environment variables  
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        Build()  
  
    client := hss.NewHssClient(  
        hss.HssClientBuilder().  
            WithRegion(region.ValueOf("<YOUR REGION>")).  
            WithCredential(auth).  
            Build()  
    )  
  
    request := &model.ListContainerNodesRequest{  
        enterpriseProjectIdRequest:= "<enterprise_project_id>"  
        request.EnterpriseProjectId = &enterpriseProjectIdRequest  
        offsetRequest:= int32(<offset>)  
        request.Offset = &offsetRequest  
        limitRequest:= int32(<limit>)  
        request.Limit = &limitRequest  
        hostNameRequest:= "<host_name>"  
        request.HostName = &hostNameRequest  
        agentStatusRequest:= "<agent_status>"  
        request.AgentStatus = &agentStatusRequest  
        protectStatusRequest:= "<protect_status>"  
        request.ProtectStatus = &protectStatusRequest  
        containerTagsRequest:= "<container_tags>"  
        request.ContainerTags = &containerTagsRequest  
        response, err := client.ListContainerNodes(request)  
        if err == nil {  
            fmt.Printf("%+v\n", response)  
        } else {  
            fmt.Println(err)  
        }  
    }  
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Resposta bem-sucedida

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.6 Gerenciamento de eventos

### 3.6.1 Consulta da lista de endereços IP bloqueados

#### Função

Essa API é usada para consultar a lista de endereços IP bloqueados.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/event/blocked-ip

**Tabela 3-203** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>20</b> Máximo: <b>64</b>

**Tabela 3-204** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como all_granted_eps. Mínimo: <b>0</b> Máximo: <b>64</b>
last_days	Não	Integer	Número de dias a serem consultados. Este parâmetro é exclusivo manualmente com <b>begin_time</b> e <b>end_time</b> . Mínimo: <b>1</b> Máximo: <b>30</b>
host_name	Não	String	Nome de servidor Mínimo: <b>1</b> Máximo: <b>64</b>

Parâmetro	Obrigatório	Tipo	Descrição
src_ip	Não	String	Endereço IP de origem do ataque
intercept_status	Não	String	Status da interceptação. As opções são as seguintes: <ul style="list-style-type: none"> <li>● intercepted</li> <li>● canceled (desbloqueado)</li> <li>● cancelling</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
limit	Não	Integer	Número de registros exibidos em cada página. Mínimo: <b>10</b> Máximo: <b>1000</b> Padrão: <b>10</b>

## Parâmetros de solicitação

Tabela 3-205 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-206** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total
data_list	Array of <a href="#">BlockedIpResponseInfo</a> objects	Detalhes do endereço IP bloqueado Comprimento da matriz: <b>0–100</b>

**Tabela 3-207** BlockedIpResponseInfo

Parâmetro	Tipo	Descrição
host_id	String	ID do host
host_name	String	Nome de servidor
src_ip	String	Endereço IP de origem do ataque
login_type	String	Tipo de logon. As opções são as seguintes: <ul style="list-style-type: none"><li>● "mysql" # serviço MySQL</li><li>● "rdp" # serviço RDP</li><li>● "ssh" # serviço SSH</li><li>● "vsftp" # serviço vsftp</li></ul>
intercept_num	Integer	Blocos Mínimo: <b>0</b> Máximo: <b>2147483647</b>
intercept_status	String	Status da interceptação. As opções são as seguintes: <ul style="list-style-type: none"><li>● intercepted</li><li>● canceled (desbloqueado)</li><li>● cancelling</li></ul>
block_time	Long	Hora de início da interceptação, em milissegundos. Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b>
latest_time	Long	Último tempo de interceptação, em milissegundos. Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b>



## Exemplo de solicitações

Consultar os 10 primeiros endereços IP bloqueados.

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

## Exemplo de respostas

**Código de status: 200**

Lista de endereços IP bloqueados

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

```
ListBlockedIpRequest request = new ListBlockedIpRequest();
request.withEnterpriseProjectId("<enterprise_project_id>");
request.withLastDays(<last_days>);
request.withHostName("<host_name>");
request.withSrcIp("<src_ip>");
request.withInterceptStatus("<intercept_status>");
request.withOffset(<offset>);
request.withLimit(<limit>);
try {
    ListBlockedIpResponse response = client.listBlockedIp(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListBlockedIpRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.last_days = <last_days>
        request.host_name = "<host_name>"
        request.src_ip = "<src_ip>"
        request.intercept_status = "<intercept_status>"
        request.offset = <offset>
        request.limit = <limit>
        response = client.list_blocked_ip(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ListBlockedIpRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        lastDaysRequest:= int32(<last_days>)
        request.LastDays = &lastDaysRequest
        hostNameRequest:= "<host_name>"
        request.HostName = &hostNameRequest
        srcIpRequest:= "<src_ip>"
        request.SrcIp = &srcIpRequest
        interceptStatusRequest:= "<intercept_status>"
        request.InterceptStatus = &interceptStatusRequest
        offsetRequest:= int32(<offset>)
        request.Offset = &offsetRequest
        limitRequest:= int32(<limit>)
        request.Limit = &limitRequest
        response, err := client.ListBlockedIp(request)
        if err == nil {
            fmt.Printf("%+v\n", response)
        } else {
            fmt.Println(err)
        }
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia [Código de amostra no API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de endereços IP bloqueados

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.6.2 Desbloqueio de um endereço IP bloqueado

### Função

Esta API é usada para desbloquear um endereço IP bloqueado.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

PUT /v5/{project\_id}/event/blocked-ip

**Tabela 3-208** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>20</b> Máximo: <b>64</b>

**Tabela 3-209** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como all_granted_eps. Mínimo: <b>0</b> Máximo: <b>64</b>

## Parâmetros de solicitação

**Tabela 3-210** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-211** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
data_list	Não	Array of <b>BlockedIpRequestInfo</b> objects	Lista de endereços IP a serem desbloqueados Comprimento da matriz: <b>1–100</b>

**Tabela 3-212** BlockedIpRequestInfo

Parâmetro	Obrigatório	Tipo	Descrição
host_id	Sim	String	ID do host
src_ip	Sim	String	Endereço IP de origem do ataque
login_type	Sim	String	Tipo de logon. As opções são as seguintes: <ul style="list-style-type: none"><li>● "mysql" # serviço MySQL</li><li>● "rdp" # serviço RDP</li><li>● "ssh" # serviço SSH</li><li>● "vsftp" # serviço vsftp</li></ul>

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Remover o endereço IP bloqueado 192.168.1.6 do host af423efds-214432fgsdaf-gfdsaggbvf no modo SSH.

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

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

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

Remover o endereço IP bloqueado 192.168.1.6 do host af423efds-214432fgsdaf-gfdsaggbvf no modo SSH.

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

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

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

public class ChangeBlockedIpSolution {

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

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

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();
        ChangeBlockedIpRequest request = new ChangeBlockedIpRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
```

```
ChangeBlockedIpRequestInfo body = new ChangeBlockedIpRequestInfo();
List<BlockedIpRequestInfo> listbodyDataList = new ArrayList<>();
listbodyDataList.add(
    new BlockedIpRequestInfo()
        .withHostId("af423efds-214432fgsdaf-gfdsaggbvf")
        .withSrcIp("192.168.1.6")
        .withLoginType("ssh")
);
body.withDataList(listbodyDataList);
request.withBody(body);
try {
    ChangeBlockedIpResponse response = client.changeBlockedIp(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

Remover o endereço IP bloqueado 192.168.1.6 do host af423efds-214432fgsdaf-gfdsaggbvf no modo SSH.

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ChangeBlockedIpRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        listDataListbody = [
            BlockedIpRequestInfo(
                host_id="af423efds-214432fgsdaf-gfdsaggbvf",
                src_ip="192.168.1.6",
                login_type="ssh"
            )
        ]
        request.body = ChangeBlockedIpRequestInfo(
            data_list=listDataListbody
```

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

## Go

Remover o endereço IP bloqueado 192.168.1.6 do host af423efds-214432fgsdaf-gfdsaggbvf no modo SSH.

```
package main

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

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

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

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

    request := &model.ChangeBlockedIpRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        var listDataListbody = []model.BlockedIpRequestInfo{
            {
                HostId: "af423efds-214432fgsdaf-gfdsaggbvf",
                SrcIp: "192.168.1.6",
                LoginType: "ssh",
            },
        },
    }
    request.Body = &model.ChangeBlockedIpRequestInfo{
        DataList: &listDataListbody,
    }
    response, err := client.ChangeBlockedIp(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```



## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Resposta bem-sucedida

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.6.3 Consulta da lista de arquivos isolados

#### Função

Esta API é usada para consultar a lista de arquivos isolados.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/event/isolated-file

Tabela 3-213 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>20</b> Máximo: <b>64</b>

Tabela 3-214 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como all_granted_eps. Mínimo: <b>0</b> Máximo: <b>64</b>
file_path	Não	String	Caminho do arquivo
host_name	Não	String	Nome de servidor Mínimo: <b>1</b> Máximo: <b>64</b>
private_ip	Não	String	Endereço IP privado de servidor Mínimo: <b>1</b> Máximo: <b>256</b>
public_ip	Não	String	Endereço IP público do servidor Mínimo: <b>1</b> Máximo: <b>256</b>
file_hash	Não	String	O valor de hash calculado usando o algoritmo SHA256.
asset_value	Não	String	Importância de ativo. As opções são as seguintes: <ul style="list-style-type: none"><li>● important</li><li>● common</li><li>● test</li></ul> Mínimo: <b>0</b> Máximo: <b>128</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
limit	Não	Integer	Número de registros exibidos em cada página. Mínimo: <b>10</b> Máximo: <b>1000</b> Padrão: <b>10</b>

## Parâmetros de solicitação

Tabela 3-215 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

Código de status: **200**

Tabela 3-216 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total
data_list	Array of <b>IsolatedFileResponseInfo</b> objects	Detalhes do arquivo isolado Comprimento da matriz: <b>0-100</b>

Tabela 3-217 IsolatedFileResponseInfo

Parâmetro	Tipo	Descrição
os_type	String	Tipo de SO. Seu valor pode ser: <ul style="list-style-type: none"><li>● Linux</li><li>● Windows</li></ul>
host_id	String	ID do host
host_name	String	Nome de servidor

Parâmetro	Tipo	Descrição
file_hash	String	Hash de arquivo
file_path	String	Caminho do arquivo
file_attr	String	Atributo de arquivo
isolation_status	String	Status de isolamento. As opções são as seguintes: <ul style="list-style-type: none"><li>● isolated</li><li>● restored</li><li>● isolating</li><li>● restoring</li></ul>
private_ip	String	Endereço IP privado de servidor
public_ip	String	Endereço IP elástico
asset_value	String	Importância dos ativos
update_time	Integer	Hora em que a lista branca de eventos é atualizada, em milissegundos.
agent_version	String	Versão do agente
isolate_source	String	Fonte de isolamento. As opções são as seguintes: <ul style="list-style-type: none"><li>● event: evento de alarme de segurança</li><li>● antivirus: verificação e remoção de vírus</li></ul>
event_name	String	Nome do evento
agent_event_info	<b>IsolateEventResponseInfo</b> object	Detalhes do evento de isolamento
antivirus_result_info	<b>AntivirusResultDetailInfo</b> object	Resultados da verificação e remoção de vírus

**Tabela 3-218** IsolateEventResponseInfo

Parâmetro	Tipo	Descrição
event_id	String	ID do evento

Parâmetro	Tipo	Descrição
event_class_id	String	<p>Categoria do evento. Seu valor pode ser:</p> <ul style="list-style-type: none"> <li>● container_1001: namespace do container</li> <li>● container_1002: porta aberta do container</li> <li>● container_1003: opção de segurança de container</li> <li>● container_1004: diretório de montagem do container</li> <li>● containerescape_0001: chamada de sistema de alto risco</li> <li>● containerescape_0002: ataque de Shocker</li> <li>● containerescape_0003: ataque de Dirty Cow</li> <li>● containerescape_0004: escape do arquivo do container</li> <li>● dockerfile_001: modificação do arquivo de container protegido definido pelo usuário</li> <li>● dockerfile_002: modificação de arquivos executáveis no sistema de arquivos de container</li> <li>● dockerproc_001: processo de container anormal</li> <li>● fileprotect_0001: escalonamento de privilégio de arquivo</li> <li>● fileprotect_0002: alteração do arquivo de chave</li> <li>● fileprotect_0003: alteração do caminho do AuthorizedKeysFile</li> <li>● fileprotect_0004: alteração do diretório de arquivos</li> <li>● login_0001: tentativa de ataque de força bruta</li> <li>● login_0002: ataque de força bruta foi bem-sucedido</li> <li>● login_1001: logon bem-sucedido</li> <li>● login_1002: logon remoto</li> <li>● login_1003: senha fraca</li> <li>● malware_0001: mudança de shell</li> <li>● malware_0002: shell reverso</li> <li>● malware_1001: programa malicioso</li> <li>● procdet_0001: comportamento anormal do processo</li> <li>● procdet_0002: escalonamento de privilégio do processo</li> <li>● procreport_0001: comando de alto risco</li> <li>● user_1001: alteração de conta</li> <li>● user_1002: conta insegura</li> </ul>

Parâmetro	Tipo	Descrição
		<ul style="list-style-type: none"> <li>● vmescape_0001: comando sensível executado na VM</li> <li>● vmescape_0002: arquivo sensível acessado pelo processo de virtualização</li> <li>● vmescape_0003: acesso anormal à porta de VM</li> <li>● webshell_0001: web shell</li> <li>● network_1001: mineração</li> <li>● network_1002: ataques DDoS</li> <li>● network_1003: verificação maliciosa</li> <li>● network_1004: ataque em áreas sensíveis</li> <li>● ransomware_0001: ataque de ransomware</li> <li>● ransomware_0002: ataque de ransomware</li> <li>● ransomware_0003: ataque de ransomware</li> <li>● fileless_0001: injeção de processo</li> <li>● fileless_0002: injeção de biblioteca dinâmica</li> <li>● fileless_0003: alteração na configuração da chave</li> <li>● fileless_0004: alteração na variável de ambiente</li> <li>● fileless_0005: processo de arquivo de memória</li> <li>● fileless_0006: sequestro de VDSO</li> <li>● crontab_1001: tarefa crontab suspeita</li> <li>● vul_exploit_0001: exploração da vulnerabilidade do Redis</li> <li>● vul_exploit_0002: exploração da vulnerabilidade de Hadoop</li> <li>● vul_exploit_0003: exploração da vulnerabilidade de MySQL</li> <li>● rootkit_0001: arquivo de rootkit suspeito</li> <li>● rootkit_0002: módulo de kernel suspeito</li> <li>● RASP_0004: upload de web shell</li> <li>● RASP_0018: web shell sem arquivo</li> <li>● blockexec_001: ataque de ransomware conhecido</li> <li>● hips_0001: Windows Defender desativado</li> <li>● hips_0002: ferramenta de hacker suspeita</li> <li>● hips_0003: comportamento suspeito de criptografia de ransomware</li> <li>● hips_0004: criação de conta oculta</li> <li>● hips_0005: senha do usuário e leitura de credenciais</li> <li>● hips_0006: exportação suspeita de arquivos SAM</li> <li>● hips_0007: exclusão suspeita de cópia de sombra</li> </ul>

Parâmetro	Tipo	Descrição
		<ul style="list-style-type: none"> <li>● hips_0008: exclusão de arquivo de backup</li> <li>● hips_0009: registro de ransomware suspeito</li> <li>● hips_0010: processo anormal suspeito</li> <li>● hips_0011: verificação suspeita</li> <li>● hips_0012: script de ransomware suspeito em execução</li> <li>● hips_0013: execução suspeita do comando de mineração</li> <li>● hips_0014: desativação suspeita da central de segurança do Windows</li> <li>● hips_0015: comportamento suspeito de desativar o serviço de firewall</li> <li>● hips_0016: desativação suspeita de recuperação automática do sistema</li> <li>● hips_0017: execução de arquivo executável em Office</li> <li>● hips_0018: criação de arquivo anormal com macros em Office</li> <li>● hips_0019: operação de registro suspeita</li> <li>● hips_0020: execução remota de código do Confluence</li> <li>● hips_0021: execução remota de código de MSDT</li> <li>● portscan_0001: verificação de porta comum</li> <li>● portscan_0002: verificação de porta secreta</li> <li>● k8s_1001: exclusão de eventos do Kubernetes</li> <li>● k8s_1002: criações de pods privilegiados</li> <li>● k8s_1003: shell interativo usado no pod</li> <li>● k8s_1004: pod criado com diretório sensível</li> <li>● k8s_1005: pod criado com a rede do servidor</li> <li>● k8s_1006: pod criado com espaço de PID do host</li> <li>● k8s_1007: falha de autenticação quando pods comuns acessam o servidor da API</li> <li>● k8s_1008: acesso ao servidor de API do pod comum usando cURL</li> <li>● k8s_1009: exec no espaço de gerenciamento do sistema</li> <li>● k8s_1010: pod criado no espaço de gerenciamento</li> <li>● k8s_1011: criação de pod estático</li> <li>● k8s_1012: criação de DaemonSet</li> <li>● k8s_1013: criação de tarefa de cluster agendada</li> <li>● k8s_1014: operação em segredos</li> </ul>

Parâmetro	Tipo	Descrição
		<ul style="list-style-type: none"> <li>● k8s_1015: enumeração de operação permitida</li> <li>● k8s_1016: RoleBinding ou ClusterRoleBinding de alto privilégio</li> <li>● k8s_1017: criação de ServiceAccount</li> <li>● k8s_1018: criação de Cronjob</li> <li>● k8s_1019: shell interativo usado para exec em pods</li> <li>● k8s_1020: acesso não autorizado ao servidor da API</li> <li>● k8s_1021: acesso ao servidor de API com curl</li> <li>● k8s_1022: vulnerabilidade de entrada</li> <li>● k8s_1023: ataque man-in-the-middle (MITM)</li> <li>● k8s_1024: worm, mineração ou cavalo de Troia</li> <li>● k8s_1025: exclusão de evento de K8s</li> <li>● k8s_1026: SelfSubjectRulesReview</li> <li>● imgblock_0001: bloqueio de imagem com base na lista branca</li> <li>● imgblock_0002: bloqueio de imagem com base na lista negra</li> <li>● imgblock_0003: bloqueio de tags de imagem com base na lista branca</li> <li>● imgblock_0004: bloqueio de tags de imagem com base na lista negra</li> <li>● imgblock_0005: criação de container bloqueada com base na lista branca</li> <li>● imgblock_0006: criação de container bloqueada com base na lista negra</li> <li>● imgblock_0007: bloqueio de container mount proc</li> <li>● imgblock_0008: bloqueio de container seccomp unconfined</li> <li>● imgblock_0009: bloqueio de privilégios de container</li> <li>● imgblock_0010: bloqueio de recursos do container</li> </ul>



Parâmetro	Tipo	Descrição
event_type	Integer	<p>Tipo de evento. Seu valor pode ser:</p> <ul style="list-style-type: none"><li>● 1001: malware comum</li><li>● 1002: vírus</li><li>● 1003: worm</li><li>● 1004: cavalo de Troia</li><li>● 1005: rede de bots</li><li>● 1006: backdoor</li><li>● 1010: Rootkit</li><li>● 1011: ransomware</li><li>● 1012: ferramenta de hacker</li><li>● 1015: web shell</li><li>● 1016: mineração</li><li>● 1017: shell reverso</li><li>● 2001: exploração de vulnerabilidade comum</li><li>● 2012: execução remota de código</li><li>● 2047: exploração da vulnerabilidade do Redis</li><li>● 2048: exploração da vulnerabilidade de Hadoop</li><li>● 2049: exploração da vulnerabilidade de MySQL</li><li>● 3002: escalonamento de privilégios de arquivo</li><li>● 3003: escalonamento de privilégio de processo</li><li>● 3004: alteração crítica de arquivo</li><li>● 3005: alteração de arquivo/diretório</li><li>● 3007: comportamento anormal do processo</li><li>● 3015: execução de comandos de alto risco</li><li>● 3018: shell anormal</li><li>● 3027: tarefa crontab suspeita</li><li>● 3029: proteção do sistema desativada</li><li>● 3030: exclusão de backup</li><li>● 3031: operações de registro suspeitas</li><li>● 3036: bloqueio de imagem de container</li><li>● 4002: ataque de força bruta</li><li>● 4004: logon anormal</li><li>● 4006: contas inválidas</li><li>● 4014: conta adicionada</li><li>● 4020: roubo de senha</li><li>● 6002: verificação de porta</li><li>● 6003: verificação do servidor</li><li>● 13001: exclusão de eventos do Kubernetes</li><li>● 13002: comportamento anormal do pod</li></ul>

Parâmetro	Tipo	Descrição
		<ul style="list-style-type: none"><li>● 13003: enumeração de informações do usuário</li><li>● 13004: vinculação de função de cluster</li></ul>
event_name	String	Nome do evento
severity	String	Nível de ameaça. Seu valor pode ser: <ul style="list-style-type: none"><li>● Security</li><li>● Low</li><li>● Medium</li><li>● High</li><li>● Critical</li></ul>
container_name	String	Nome da instância do container. Esta API está disponível apenas para alarmes de container.
image_name	String	Nome da imagem. Esta API está disponível apenas para alarmes de container.
host_name	String	Nome de servidor
host_id	String	ID do host
private_ip	String	Endereço IP privado de servidor
public_ip	String	Endereço IP elástico
os_type	String	Tipo de SO. Seu valor pode ser: <ul style="list-style-type: none"><li>● Linux</li><li>● Windows</li></ul>
host_status	String	Status do servidor. As opções são as seguintes: <ul style="list-style-type: none"><li>● ACTIVE</li><li>● SHUTOFF</li><li>● BUILDING</li><li>● ERROR</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
agent_status	String	Status de agente. Seu valor pode ser: <ul style="list-style-type: none"><li>● installed</li><li>● not_installed</li><li>● online</li><li>● offline</li><li>● install_failed</li><li>● installing</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>

Parâmetro	Tipo	Descrição
protect_status	String	Status de proteção. Seu valor pode ser: <ul style="list-style-type: none"> <li>● closed</li> <li>● opened</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>
asset_value	String	Importância de ativo. As opções são as seguintes: <ul style="list-style-type: none"> <li>● important</li> <li>● common</li> <li>● test</li> </ul> Mínimo: <b>0</b> Máximo: <b>128</b>
attack_phase	String	Fase de ataque. Seu valor pode ser: <ul style="list-style-type: none"> <li>● reconnaissance</li> <li>● weaponization</li> <li>● delivery</li> <li>● exploit</li> <li>● installation</li> <li>● command_and_control</li> <li>● actions</li> </ul>
attack_tag	String	Tag de ataque. Seu valor pode ser: <ul style="list-style-type: none"> <li>● attack_success</li> <li>● attack_attempt</li> <li>● attack_blocked</li> <li>● abnormal_behavior</li> <li>● collapsible_host</li> <li>● system_vulnerability</li> </ul>
occur_time	Integer	Tempo de ocorrência, com precisão de milissegundos.
handle_time	Integer	Tempo de manipulação, em milissegundos. Esta API está disponível apenas para alarmes manipulados.
handle_status	String	Status de processamento. Seu valor pode ser: <ul style="list-style-type: none"> <li>● unhandled</li> <li>● handled</li> </ul>

Parâmetro	Tipo	Descrição
handle_method	String	Método de manipulação. Esta API está disponível apenas para alarmes manipulados. As opções são as seguintes: <ul style="list-style-type: none"> <li>● mark_as_handled</li> <li>● ignore</li> <li>● add_to_alarm_whitelist</li> <li>● add_to_login_whitelist</li> <li>● isolate_and_kill</li> </ul>
handler	String	Observações. Esta API está disponível apenas para alarmes manipulados.
recommendation	String	Sugestão de tratamento
description	String	Descrição do alarme Mínimo: <b>0</b> Máximo: <b>1024</b>
event_abstract	String	Resumo do alarme Mínimo: <b>0</b> Máximo: <b>512</b>
event_count	Integer	Ocorrências de eventos Mínimo: <b>0</b> Máximo: <b>2147483647</b>

**Tabela 3-219** AntivirusResultDetailInfo

Parâmetro	Tipo	Descrição
result_id	String	O ID de resultado da verificação e remoção de vírus
malware_name	String	Nome do vírus
file_path	String	Caminho do arquivo
file_hash	String	Hash de arquivo
file_size	Integer	Tamanho do arquivo
file_owner	String	Proprietário do arquivo
file_attr	String	Atributo de arquivo
file_ctime	Integer	Tempo de criação do arquivo
file_mtime	Integer	Hora da atualização do arquivo

Parâmetro	Tipo	Descrição
update_time	Integer	Hora em que a lista branca de eventos é atualizada, em milissegundos.
agent_id	String	ID do agente

## Exemplo de solicitações

Consultar os 10 primeiros arquivos isolados.

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

## Exemplo de respostas

**Código de status: 200**

Lista de arquivos isolados

```
{
  "data_list" : [ {
    "file_attr" : "0",
    "file_hash" :
"58693382bc0c9f60ef86e5b37cf3c2f3a9c9ec46936901eaa9131f7ee4a09bde",
    "file_path" : "C:\\Users\\Public\\Public Docker\\system32.exe",
    "os_type" : "Linux",
    "host_id" : "5a41ca47-8ea7-4a65-a8fb-950d03d8638e",
    "host_name" : "ecs-wi-800211",
    "isolation_status" : "isolated",
    "private_ip" : "127.0.0.2",
    "public_ip" : "127.0.0.1",
    "asset_value" : "common",
    "update_time" : 1698304933717,
    "agent_version" : "3.2.10",
    "isolate_source" : "event",
    "event_name" : "Spyware",
    "antivirus_result_info" : {
      "result_id" : "5a41ca47-8ea7-4a65-a8fb-950d03d8638e",
      "malware_name" : "Win32.Virus.Hidrag",
      "file_attr" : "0",
      "file_hash" :
"58693382bc0c9f60ef86e5b37cf3c2f3a9c9ec46936901eaa9131f7ee4a09bde",
      "file_path" : "C:\\Users\\Public\\Public Docker\\system32.exe",
      "file_size" : 58460,
      "file_owner" : "Administrators",
      "file_ctime" : 1700039800,
      "file_mtime" : 1700039800,
      "update_time" : 1698304933717,
      "agent_id" : "5a41ca47-8ea7-4a65-a8fb-950d03d8638e"
    },
    "agent_event_info" : {
      "attack_phase" : "exploit",
      "attack_tag" : "abnormal_behavior",
      "event_class_id" : "lgln_1002",
      "event_id" : "d8a12cf7-6a43-4cd6-92b4-aabf1e917",
      "event_name" : "different locations",
      "event_type" : 4004,
      "handle_status" : "unhandled",
      "host_name" : "xxx",
      "occur_time" : 1661593036627,
      "private_ip" : "127.0.0.1",
      "severity" : "Medium",
```

```
"os_type" : "Linux",
"agent_status" : "online",
"asset_value" : "common",
"protect_status" : "opened",
"host_status" : "ACTIVE",
"description" : "",
"event_abstract" : "",
"image_name" : "image",
"container_name" : "test",
"host_id" : "5a41ca47-8ea7-4a65-a8fb-950d03d8638e",
"public_ip" : "127.0.0.2",
"handle_time" : 1698304933717,
"handle_method" : "ignore",
"recommendation" : "Handling suggestion",
"event_count" : 1
}
} ],
"total_num" : 1
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListIsolatedFileSolution {

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

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

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

        ListIsolatedFileRequest request = new ListIsolatedFileRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withFilePath("<file_path>");
        request.withHostName("<host_name>");
        request.withPrivateIp("<private_ip>");
        request.withPublicIp("<public_ip>");
        request.withFileHash("<file_hash>");
        request.withAssetValue("<asset_value>");
        request.withOffset("<offset>");
    }
}
```

```
request.withLimit(<limit>);
try {
    ListIsolatedFileResponse response = client.listIsolatedFile(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListIsolatedFileRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.file_path = "<file_path>"
        request.host_name = "<host_name>"
        request.private_ip = "<private_ip>"
        request.public_ip = "<public_ip>"
        request.file_hash = "<file_hash>"
        request.asset_value = "<asset_value>"
        request.offset = <offset>
        request.limit = <limit>
        response = client.list_isolated_file(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
```

```
"fmt"  
"github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"  
"github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"  
region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in  
    plaintext, which has great security risks. It is recommended that the AK and SK  
    be stored in ciphertext in configuration files or environment variables and  
    decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for  
    authentication. Before running this example, set environment variables  
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        Build()  
  
    client := hss.NewHssClient(  
        hss.HssClientBuilder().  
            WithRegion(region.ValueOf("<YOUR REGION>")).  
            WithCredential(auth).  
            Build()  
    )  
  
    request := &model.ListIsolatedFileRequest{}  
    enterpriseProjectIdRequest := "<enterprise_project_id>"  
    request.EnterpriseProjectId = &enterpriseProjectIdRequest  
    filePathRequest := "<file_path>"  
    request.FilePath = &filePathRequest  
    hostNameRequest := "<host_name>"  
    request.HostName = &hostNameRequest  
    privateIpRequest := "<private_ip>"  
    request.PrivateIp = &privateIpRequest  
    publicIpRequest := "<public_ip>"  
    request.PublicIp = &publicIpRequest  
    fileHashRequest := "<file_hash>"  
    request.FileHash = &fileHashRequest  
    assetValueRequest := "<asset_value>"  
    request.AssetValue = &assetValueRequest  
    offsetRequest := int32(<offset>)  
    request.Offset = &offsetRequest  
    limitRequest := int32(<limit>)  
    request.Limit = &limitRequest  
    response, err := client.ListIsolatedFile(request)  
    if err == nil {  
        fmt.Printf("%+v\n", response)  
    } else {  
        fmt.Println(err)  
    }  
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia [Código de amostra no API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.



## Códigos de status

Código de status	Descrição
200	Lista de arquivos isolados

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.6.4 Restauração de arquivos isolados

### Função

Essa API é usada para restaurar arquivos isolados.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

PUT /v5/{project\_id}/event/isolated-file

**Tabela 3-220** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>20</b> Máximo: <b>64</b>

**Tabela 3-221** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como all_granted_eps. Mínimo: <b>0</b> Máximo: <b>64</b>

## Parâmetros de solicitação

**Tabela 3-222** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-223** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
data_list	Não	Array of <b>IsolatedFileRequestInfo</b> objects	Lista de arquivos a serem restaurados Comprimento da matriz: <b>0–100</b>

**Tabela 3-224** IsolatedFileRequestInfo

Parâmetro	Obrigatório	Tipo	Descrição
host_id	Não	String	ID do host
file_hash	Não	String	Hash de arquivo
file_path	Não	String	Caminho do arquivo
file_attr	Não	String	Atributo de arquivo

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Cancelar o isolamento do arquivo C:\Users\Public\test.exe no host 5a41ca47-8ea7-4a65-a8fb-950d03d8638e.

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

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

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

Cancelar o isolamento do arquivo C:\Users\Public\test.exe no host 5a41ca47-8ea7-4a65-a8fb-950d03d8638e.

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

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

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

public class ChangeIsolatedFileSolution {

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

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

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
            .build();
        ChangeIsolatedFileRequest request = new ChangeIsolatedFileRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        ChangeIsolatedFileRequestInfo body = new ChangeIsolatedFileRequestInfo();
        List<IsolatedFileRequestInfo> listbodyDataList = new ArrayList<>();
        listbodyDataList.add(
            new IsolatedFileRequestInfo()

```

```
        .withHostId("5a41ca47-8ea7-4a65-a8fb-950d03d8638e")
        .withFileHash("58693382bc0c9f60ef86e5b37cf3c2f3a9c9ec46936901eaa91
31f7ee4a09bde")
        .withFilePath("C:\\Users\\Public\\test.exe")
        .withFileAttr("0")
    );
    body.withDataList(listbodyDataList);
    request.withBody(body);
    try {
        ChangeIsolatedFileResponse response =
client.changeIsolatedFile(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

Cancelar o isolamento do arquivo C:\Users\Public\test.exe no host 5a41ca47-8ea7-4a65-a8fb-950d03d8638e.

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ChangeIsolatedFileRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        listDataListbody = [
            IsolatedFileRequestInfo(
                host_id="5a41ca47-8ea7-4a65-a8fb-950d03d8638e",
file_hash="58693382bc0c9f60ef86e5b37cf3c2f3a9c9ec46936901eaa9131f7ee4a09bde",
                file_path="C:\\Users\\Public\\test.exe",
                file_attr="0"
            )
        ]
        request.body = ChangeIsolatedFileRequestInfo(
```

```
        data_list=listDataListbody
    )
    response = client.change_isolated_file(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

Cancelar o isolamento do arquivo C:\Users\Public\test.exe no host 5a41ca47-8ea7-4a65-a8fb-950d03d8638e.

```
package main

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

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

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

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

    request := &model.ChangeIsolatedFileRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        hostIdDataList:= "5a41ca47-8ea7-4a65-a8fb-950d03d8638e"
        fileHashDataList:=
"58693382bc0c9f60ef86e5b37cf3c2f3a9c9ec46936901eaa9131f7ee4a09bde"
        filePathDataList:= "C:\Users\Public\test.exe"
        fileAttrDataList:= "0"
        var listDataListbody = []model.IsolatedFileRequestInfo{
            {
                HostId: &hostIdDataList,
                FileHash: &fileHashDataList,
                FilePath: &filePathDataList,
                FileAttr: &fileAttrDataList,
            },
        }
        request.Body = &model.ChangeIsolatedFileRequestInfo{
            DataList: &listDataListbody,
        }
        response, err := client.ChangeIsolatedFile(request)
        if err == nil {
            fmt.Printf("%v\n", response)
        }
    }
}
```

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

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Resposta bem-sucedida

## Códigos de erro

Consulte [Códigos de erro](#).

# 3.7 Detecção de intrusão

## 3.7.1 Manipulação de eventos de alarme

### Função

Essa API é usada para manipular eventos de alarme.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

POST /v5/{project\_id}/event/operate

Tabela 3-225 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>20</b> Máximo: <b>64</b>

**Tabela 3-226** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>64</b>
container_name	Não	String	Nome da instância do container
container_id	Não	String	ID do container

## Parâmetros de solicitação

**Tabela 3-227** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-228** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
operate_type	Sim	String	Método de manipulação. Seu valor pode ser: <ul style="list-style-type: none"> <li>● mark_as_handled</li> <li>● ignore</li> <li>● add_to_alarm_whitelist</li> <li>● add_to_login_whitelist</li> <li>● isolate_and_kill</li> <li>● unhandle</li> <li>● do_not_ignore</li> <li>● remove_from_alarm_whitelist</li> <li>● remove_from_login_whitelist</li> <li>● do_not_isolate_or_kill</li> </ul>
handler	Não	String	Observações. Esta API está disponível apenas para alarmes manipulados.
operate_event_list	Sim	Array of <b>OperateEventRequestInfo</b> objects	Lista de eventos operados Comprimento da matriz: <b>0–100</b>
event_white_rule_list	Não	Array of <b>EventWhiteRuleListRequestInfo</b> objects	Lista branca de alarme definida pelo usuário Comprimento da matriz: <b>0–100</b>



**Tabela 3-229** OperateEventRequestInfo

Parâmetro	Obrigatório	Tipo	Descrição
event_class_id	Sim	String	<p>Categoria do evento. Seu valor pode ser:</p> <ul style="list-style-type: none"> <li>● container_1001: namespace do container</li> <li>● container_1002: porta aberta do container</li> <li>● container_1003: opção de segurança de container</li> <li>● container_1004: diretório de montagem do container</li> <li>● containerescape_0001: chamada de sistema de alto risco</li> <li>● containerescape_0002: ataque de Shocker</li> <li>● containerescape_0003: ataque de Dirty Cow</li> <li>● containerescape_0004: escape do arquivo do container</li> <li>● dockerfile_001: modificação do arquivo de container protegido definido pelo usuário</li> <li>● dockerfile_002: modificação de arquivos executáveis no sistema de arquivos de container</li> <li>● dockerproc_001: processo de container anormal</li> <li>● fileprotect_0001: escalonamento de privilégio de arquivo</li> <li>● fileprotect_0002: alteração do arquivo de chave</li> <li>● fileprotect_0003: alteração do caminho do AuthorizedKeysFile</li> <li>● fileprotect_0004: alteração do diretório de arquivos</li> <li>● login_0001: tentativa de ataque com força bruta</li> <li>● login_0002: ataque de força bruta foi bem-sucedido</li> <li>● login_1001: logon bem-sucedido</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
			<ul style="list-style-type: none"> <li>● login_1002: logon remoto</li> <li>● login_1003: senha fraca</li> <li>● malware_0001: mudança de shell</li> <li>● malware_0002: shell reverso</li> <li>● malware_1001: programa malicioso</li> <li>● procdet_0001: comportamento anormal do processo</li> <li>● procdet_0002: escalonamento de privilégio do processo</li> <li>● procreport_0001: comando de alto risco</li> <li>● user_1001: alteração de conta</li> <li>● user_1002: conta insegura</li> <li>● vmescape_0001: comando sensível executado na VM</li> <li>● vmescape_0002: arquivo sensível acessado pelo processo de virtualização</li> <li>● vmescape_0003: acesso anormal à porta de VM</li> <li>● webshell_0001: web shell</li> <li>● network_1001: mineração</li> <li>● network_1002: ataques DDoS</li> <li>● network_1003: verificação maliciosa</li> <li>● network_1004: ataque em áreas sensíveis</li> <li>● ransomware_0001: ataque de ransomware</li> <li>● ransomware_0002: ataque de ransomware</li> <li>● ransomware_0003: ataque de ransomware</li> <li>● fileless_0001: injeção de processo</li> <li>● fileless_0002: injeção de biblioteca dinâmica</li> <li>● fileless_0003: alteração na configuração da chave</li> <li>● fileless_0004: alteração na variável de ambiente</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
			<ul style="list-style-type: none"> <li>● fileless_0005: processo de arquivo de memória</li> <li>● fileless_0006: sequestro de VDSO</li> <li>● crontab_1001: tarefa crontab suspeita</li> <li>● vul_exploit_0001: exploração da vulnerabilidade do Redis</li> <li>● vul_exploit_0002: exploração da vulnerabilidade de Hadoop</li> <li>● vul_exploit_0003: exploração da vulnerabilidade de MySQL</li> <li>● rootkit_0001: arquivo de rootkit suspeito</li> <li>● rootkit_0002: módulo de kernel suspeito</li> <li>● RASP_0004: upload de web shell</li> <li>● RASP_0018: web shell sem arquivo</li> <li>● blockexec_001: ataque de ransomware conhecido</li> <li>● hips_0001: Windows Defender desativado</li> <li>● hips_0002: ferramenta de hacker suspeita</li> <li>● hips_0003: comportamento suspeito de criptografia de ransomware</li> <li>● hips_0004: criação de conta oculta</li> <li>● hips_0005: senha do usuário e leitura de credenciais</li> <li>● hips_0006: exportação suspeita de arquivos SAM</li> <li>● hips_0007: exclusão suspeita de cópia de sombra</li> <li>● hips_0008: exclusão de arquivo de backup</li> <li>● hips_0009: registro de ransomware suspeito</li> <li>● hips_0010: processo anormal suspeito</li> <li>● hips_0011: verificação suspeita</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
			<ul style="list-style-type: none"> <li>● hips_0012: script de ransomware suspeito em execução</li> <li>● hips_0013: execução suspeita do comando de mineração</li> <li>● hips_0014: desativação suspeita da central de segurança do Windows</li> <li>● hips_0015: comportamento suspeito de desativar o serviço de firewall</li> <li>● hips_0016: desativação suspeita de recuperação automática do sistema</li> <li>● hips_0017: execução de arquivo executável em Office</li> <li>● hips_0018: criação de arquivo anormal com macros em Office</li> <li>● hips_0019: operação de registro suspeita</li> <li>● hips_0020: execução remota de código do Confluence</li> <li>● hips_0021: execução remota de código de MSDT</li> <li>● portscan_0001: verificação de porta comum</li> <li>● portscan_0002: verificação de porta secreta</li> <li>● k8s_1001: exclusão de eventos do Kubernetes</li> <li>● k8s_1002: criações de pods privilegiados</li> <li>● k8s_1003: shell interativo usado no pod</li> <li>● k8s_1004: pod criado com diretório sensível</li> <li>● k8s_1005: pod criado com a rede do servidor</li> <li>● k8s_1006: pod criado com espaço de PID do host</li> <li>● k8s_1007: falha de autenticação quando pods comuns acessam o servidor da API</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
			<ul style="list-style-type: none"> <li>● k8s_1008: acesso ao servidor de API do pod comum usando cURL</li> <li>● k8s_1009: exec no espaço de gerenciamento do sistema</li> <li>● k8s_1010: pod criado no espaço de gerenciamento</li> <li>● k8s_1011: criação de pod estático</li> <li>● k8s_1012: criação de DaemonSet</li> <li>● k8s_1013: criação de tarefa de cluster agendada</li> <li>● k8s_1014: operação em segredos</li> <li>● k8s_1015: enumeração de operação permitida</li> <li>● k8s_1016: RoleBinding ou ClusterRoleBinding de alto privilégio</li> <li>● k8s_1017: criação de ServiceAccount</li> <li>● k8s_1018: criação de Cronjob</li> <li>● k8s_1019: shell interativo usado para exec em pods</li> <li>● k8s_1020: acesso não autorizado ao servidor da API</li> <li>● k8s_1021: acesso ao servidor de API com curl</li> <li>● k8s_1022: vulnerabilidade de entrada</li> <li>● k8s_1023: ataque man-in-the-middle (MITM)</li> <li>● k8s_1024: worm, mineração ou cavalo de Troia</li> <li>● k8s_1025: exclusão de evento de K8s</li> <li>● k8s_1026: SelfSubjectRules-Review</li> <li>● imgblock_0001: bloqueio de imagem com base na lista branca</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
			<ul style="list-style-type: none"> <li>● imgblock_0002: bloqueio de imagem com base na lista negra</li> <li>● imgblock_0003: bloqueio de tag de imagem com base na lista branca</li> <li>● imgblock_0004: bloqueio de tag de imagem com base na lista negra</li> <li>● imgblock_0005: criação de container bloqueada com base na lista branca</li> <li>● imgblock_0006: criação de container bloqueada com base na lista negra</li> <li>● imgblock_0007: bloqueio de container mount proc</li> <li>● imgblock_0008: bloqueio de container seccomp unconfined</li> <li>● imgblock_0009: bloqueio de privilégios de container</li> <li>● imgblock_0010: bloqueio de recursos do container</li> </ul>
event_id	Sim	String	ID do evento

Parâmetro	Obrigatório	Tipo	Descrição
event_type	Sim	Integer	<p>Tipo de evento. Seu valor pode ser:</p> <ul style="list-style-type: none"> <li>● 1001: malware comum</li> <li>● 1002: vírus</li> <li>● 1003: worm</li> <li>● 1004: cavalo de Troia</li> <li>● 1005: rede de bots</li> <li>● 1006: backdoor</li> <li>● 1010: Rootkit</li> <li>● 1011: ransomware</li> <li>● 1012: ferramenta de hacker</li> <li>● 1015: web shell</li> <li>● 1016: mineração</li> <li>● 1017: shell reverso</li> <li>● 2001: exploração de vulnerabilidade comum</li> <li>● 2012: execução remota de código</li> <li>● 2047: exploração da vulnerabilidade do Redis</li> <li>● 2048: exploração da vulnerabilidade de Hadoop</li> <li>● 2049: exploração da vulnerabilidade de MySQL</li> <li>● 3002: escalonamento de privilégios de arquivo</li> <li>● 3003: escalonamento de privilégio de processo</li> <li>● 3004: alteração crítica de arquivo</li> <li>● 3005: alteração de arquivo/diretório</li> <li>● 3007: comportamento anormal do processo</li> <li>● 3015: execução de comandos de alto risco</li> <li>● 3018: shell anormal</li> <li>● 3027: tarefa crontab suspeita</li> <li>● 3029: proteção do sistema desativada</li> <li>● 3030: exclusão de backup</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
			<ul style="list-style-type: none"><li>● 3031: operações de registro suspeitas</li><li>● 3036: bloqueio de imagem de container</li><li>● 4002: ataque de força bruta</li><li>● 4004: logon anormal</li><li>● 4006: contas inválidas</li><li>● 4014: conta adicionada</li><li>● 4020: roubo de senha</li><li>● 6002: verificação de porta</li><li>● 6003: verificação do servidor</li><li>● 13001: exclusão de eventos do Kubernetes</li><li>● 13002: comportamento anormal do pod</li><li>● 13003: enumeração de informações do usuário</li><li>● 13004: vinculação de função de cluster</li></ul>
occur_time	Sim	Integer	Tempo de ocorrência, com precisão de milissegundos.
operate_detail_list	Sim	Array of <a href="#">EventDetailRequestInfo</a> objects	Lista de detalhes da operação. Se operate_type estiver definido como add_to_alarm_whitelist ou remove_from_alarm_whitelist, a palavra-chave e o hash serão obrigatórios. Se operate_type for definido como add_to_login_whitelist ou remove_from_login_whitelist, os parâmetros login_ip, private_ip e login_user_name serão obrigatórios. Se operate_type for definido como isolate_and_kill ou do_not_isolate_or_kill, os parâmetros agent_id, file_hash, file_path e process_pid serão obrigatórios. Em outros casos, os parâmetros são opcionais.  Comprimento da matriz: <b>0–100</b>



**Tabela 3-230** EventDetailRequestInfo

Parâmetro	Obrigatório	Tipo	Descrição
agent_id	Não	String	ID do agente
process_pid	Não	Integer	ID do processo
file_hash	Não	String	Hash de arquivo
file_path	Não	String	Caminho do arquivo
file_attr	Não	String	Atributo de arquivo
keyword	Não	String	Palavra-chave de evento de alarme, que é usada somente para a lista branca de alarmes.
hash	Não	String	Hash de evento de alarme, que é usado apenas para a lista branca de alarme.
private_ip	Não	String	Endereço IP privado de servidor
login_ip	Não	String	Endereço IP de origem de logon
login_user_name	Não	String	Nome de usuário de logon
container_id	Não	String	ID do container Mínimo: <b>64</b> Máximo: <b>64</b>
container_name	Não	String	Nome do container Mínimo: <b>1</b> Máximo: <b>128</b>

**Tabela 3-231** EventWhiteRuleListRequestInfo

Parâmetro	Obrigatório	Tipo	Descrição
event_type	Sim	Integer	<p>Tipo de evento. Seu valor pode ser:</p> <ul style="list-style-type: none"> <li>● 1001: malware comum</li> <li>● 1002: vírus</li> <li>● 1003: worm</li> <li>● 1004: cavalo de Troia</li> <li>● 1005: rede de bots</li> <li>● 1006: backdoor</li> <li>● 1010: Rootkit</li> <li>● 1011: ransomware</li> <li>● 1012: ferramenta de hacker</li> <li>● 1015: web shell</li> <li>● 1016: mineração</li> <li>● 1017: shell reverso</li> <li>● 2001: exploração de vulnerabilidade comum</li> <li>● 2012: execução remota de código</li> <li>● 2047: exploração da vulnerabilidade do Redis</li> <li>● 2048: exploração da vulnerabilidade de Hadoop</li> <li>● 2049: exploração da vulnerabilidade de MySQL</li> <li>● 3002: escalonamento de privilégios de arquivo</li> <li>● 3003: escalonamento de privilégio de processo</li> <li>● 3004: alteração crítica de arquivo</li> <li>● 3005: alteração de arquivo/diretório</li> <li>● 3007: comportamento anormal do processo</li> <li>● 3015: execução de comandos de alto risco</li> <li>● 3018: shell anormal</li> <li>● 3027: tarefa crontab suspeita</li> <li>● 3029: proteção do sistema desativada</li> <li>● 3030: exclusão de backup</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
			<ul style="list-style-type: none"> <li>● 3031: operações de registro suspeitas</li> <li>● 3036: bloqueio de imagem de container</li> <li>● 4002: ataque de força bruta</li> <li>● 4004: logon anormal</li> <li>● 4006: contas inválidas</li> <li>● 4014: conta adicionada</li> <li>● 4020: roubo de senha</li> <li>● 6002: verificação de porta</li> <li>● 6003: verificação do servidor</li> <li>● 13001: exclusão de eventos do Kubernetes</li> <li>● 13002: comportamento anormal do pod</li> <li>● 13003: enumeração de informações do usuário</li> <li>● 13004: vinculação de função de cluster</li> </ul>
field_key	Sim	String	<p>Campos da lista branca. As opções são as seguintes:</p> <ul style="list-style-type: none"> <li>● "file/process hash" # hash de processo/arquivo</li> <li>● "file_path"</li> <li>● "process_path"</li> <li>● "login_ip": endereço IP de logon</li> <li>● "reg_key": chave do registro</li> <li>● "process_cmdline": linha de comando do processo</li> <li>● "username"</li> </ul> <p>Mínimo: <b>1</b> Máximo: <b>20</b></p>
field_value	Sim	String	<p>Valor do campo da lista branca</p> <p>Mínimo: <b>1</b> Máximo: <b>128</b></p>

Parâmetro	Obrigatório	Tipo	Descrição
judge_type	Sim	String	<p>Curinga. As opções são as seguintes:</p> <ul style="list-style-type: none"> <li>● "equal"</li> <li>● "contain"</li> </ul> <p>Mínimo: <b>1</b> Máximo: <b>10</b></p>

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Manipular manualmente os alarmes de intrusão cujo tipo de evento de alarme é Rootkit e o ID do evento de alarme é 2a71e1e2-60f4-4d56-b314-2038fdc39de6.

```
POST https://{endpoint}/v5/{project_id}/event/operate?enterprise_project_id=xxx
{
  "operate_type" : "mark_as_handled",
  "handler" : "test",
  "operate_event_list" : [ {
    "event_class_id" : "rootkit_0001",
    "event_id" : "2a71e1e2-60f4-4d56-b314-2038fdc39de6",
    "occur_time" : 1672046760353,
    "event_type" : 1010,
    "operate_detail_list" : [ {
      "agent_id" :
"c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8",
      "file_hash" :
"e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
      "file_path" : "/usr/test",
      "process_pid" : 3123,
      "file_attr" : 33261,
      "keyword" : "file_path=/usr/test",
      "hash" : "e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
      "login_ip" : "127.0.0.1",
      "private_ip" : "127.0.0.2",
      "login_user_name" : "root",
      "container_id" : "containerid",
      "container_name" : "/test"
    } ]
  } ]
}
```

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

Manipular manualmente os alarmes de intrusão cujo tipo de evento de alarme é Rootkit e o ID do evento de alarme é 2a71e1e2-60f4-4d56-b314-2038fdc39de6.

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

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

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

public class ChangeEventSolution {

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

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

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

        ChangeEventRequest request = new ChangeEventRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withContainerName("<container_name>");
        request.withContainerId("<container_id>");
        ChangeEventRequestInfo body = new ChangeEventRequestInfo();
        List<EventDetailRequestInfo> listOperateEventListOperateDetailList = new
ArrayList<>();
        listOperateEventListOperateDetailList.add(
            new EventDetailRequestInfo()
                .withAgentId("c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab
0528bab59bd8")
                .withProcessPid(3123)
                .withFileHash("e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d
43154c5dbc44d")
                .withFilePath("/usr/test")
                .withFileAttr("33261")
                .withKeyword("file_path=/usr/test")
                .withHash("e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d4315
4c5dbc44d")
                .withPrivateIp("127.0.0.2")
                .withLoginIp("127.0.0.1")
                .withLoginUserName("root")
                .withContainerId("containerid")
                .withContainerName("/test")
            );
        List<OperateEventRequestInfo> listbodyOperateEventList = new
ArrayList<>();
        listbodyOperateEventList.add(
            new OperateEventRequestInfo()
```

```
        .withEventClassId("rootkit_0001")
        .withEventId("2a71e1e2-60f4-4d56-b314-2038fdc39de6")
        .withEventType(1010)
        .withOccurTime(1672046760353L)
        .withOperateDetailList(listOperateEventListOperateDetailList)
    );
    body.withOperateEventList(listbodyOperateEventList);
    body.withHandler("test");
    body.withOperateType("mark_as_handled");
    request.withBody(body);
    try {
        ChangeEventResponse response = client.changeEvent(request);
        System.out.println(response.toString());
    } catch (ConnectionException e) {
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
}
```

## Python

Manipular manualmente os alarmes de intrusão cujo tipo de evento de alarme é Rootkit e o ID do evento de alarme é 2a71e1e2-60f4-4d56-b314-2038fdc39de6.

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ChangeEventRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.container_name = "<container_name>"
        request.container_id = "<container_id>"
        listOperateDetailListOperateEventList = [
            EventDetailRequestInfo(
                agent_id="c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8",
                process_pid=3123,
                file_hash="e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
```

```
        file_path="/usr/test",
        file_attr="33261",
        keyword="file_path=/usr/test",

hash="e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
        private_ip="127.0.0.2",
        login_ip="127.0.0.1",
        login_user_name="root",
        container_id="containerid",
        container_name="/test"
    )
]
listOperateEventListbody = [
    OperateEventRequestInfo(
        event_class_id="rootkit_0001",
        event_id="2a71e1e2-60f4-4d56-b314-2038fdc39de6",
        event_type=1010,
        occur_time=1672046760353,
        operate_detail_list=listOperateDetailListOperateEventList
    )
]
request.body = ChangeEventRequestInfo(
    operate_event_list=listOperateEventListbody,
    handler="test",
    operate_type="mark_as_handled"
)
response = client.change_event(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

Manipular manualmente os alarmes de intrusão cujo tipo de evento de alarme é Rootkit e o ID do evento de alarme é 2a71e1e2-60f4-4d56-b314-2038fdc39de6.

```
package main

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

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

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

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

```
Build()

request := &model.ChangeEventRequest{}
enterpriseProjectIdRequest:= "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
containerNameRequest:= "<container_name>"
request.ContainerName = &containerNameRequest
containerIdRequest:= "<container_id>"
request.ContainerId = &containerIdRequest
agentIdOperateDetailList:=
"c9bed5397db449ebdfb15e85fcfc36acceel25c68954daf5cab0528bab59bd8"
processPidOperateDetailList:= int32(3123)
fileHashOperateDetailList:=
"e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d"
filePathOperateDetailList:= "/usr/test"
fileAttrOperateDetailList:= "33261"
keywordOperateDetailList:= "file_path=/usr/test"
hashOperateDetailList:=
"e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d"
privateIpOperateDetailList:= "127.0.0.2"
loginIpOperateDetailList:= "127.0.0.1"
loginUserNameOperateDetailList:= "root"
containerIdOperateDetailList:= "containerid"
containerNameOperateDetailList:= "/test"
var listOperateDetailListOperateEventList = []model.EventDetailRequestInfo{
    {
        AgentId: &agentIdOperateDetailList,
        ProcessPid: &processPidOperateDetailList,
        FileHash: &fileHashOperateDetailList,
        FilePath: &filePathOperateDetailList,
        FileAttr: &fileAttrOperateDetailList,
        Keyword: &keywordOperateDetailList,
        Hash: &hashOperateDetailList,
        PrivateIp: &privateIpOperateDetailList,
        LoginIp: &loginIpOperateDetailList,
        LoginUserName: &loginUserNameOperateDetailList,
        ContainerId: &containerIdOperateDetailList,
        ContainerName: &containerNameOperateDetailList,
    },
}
var listOperateEventListbody = []model.OperateEventRequestInfo{
    {
        EventClassId: "rootkit_0001",
        EventId: "2a71e1e2-60f4-4d56-b314-2038fdc39de6",
        EventType: int32(1010),
        OccurTime: int64(1672046760353),
        OperateDetailList: listOperateDetailListOperateEventList,
    },
}
handlerChangeEventRequestInfo:= "test"
request.Body = &model.ChangeEventRequestInfo{
    OperateEventList: listOperateEventListbody,
    Handler: &handlerChangeEventRequestInfo,
    OperateType: "mark_as_handled",
}
response, err := client.ChangeEvent(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia [Código de amostra no API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.



## Códigos de status

Código de status	Descrição
200	Bem-sucedido
400	Parâmetro inválido.
401	Falha na autenticação.
403	Permissão insuficiente.
404	Recurso não encontrado.
500	Erro de sistema.

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.7.2 Consulta da lista de intrusões detectadas

#### Função

Essa API é usada para consultar a lista de intrusões detectadas.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/event/events

Tabela 3-232 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>20</b> Máximo: <b>64</b>

Tabela 3-233 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
category	Sim	String	Categoria do evento. Seu valor pode ser: <ul style="list-style-type: none"><li>● host: evento de segurança do host</li><li>● container: evento de segurança do container</li></ul> Mínimo: <b>0</b> Máximo: <b>32</b>
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>64</b>
last_days	Não	Integer	Número de dias a serem consultados. Este parâmetro é mutuamente exclusivo com <b>begin_time</b> e <b>end_time</b> . Mínimo: <b>1</b> Máximo: <b>30</b>
host_name	Não	String	Nome de servidor Mínimo: <b>1</b> Máximo: <b>64</b>
host_id	Não	String	ID do host Mínimo: <b>0</b> Máximo: <b>64</b>
private_ip	Não	String	Endereço IP do servidor Mínimo: <b>1</b> Máximo: <b>256</b>
public_ip	Não	String	Endereço IP público do servidor Mínimo: <b>1</b> Máximo: <b>256</b>
container_name	Não	String	Nome da instância do container

Parâmetro	Obrigatório	Tipo	Descrição
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
limit	Não	Integer	Número de registros exibidos em cada página Mínimo: <b>10</b> Máximo: <b>1000</b> Padrão: <b>10</b>

Parâmetro	Obrigatório	Tipo	Descrição
event_types	Não	Array	<p>Tipo de evento. Seu valor pode ser:</p> <ul style="list-style-type: none"> <li>● 1001: malware comum</li> <li>● 1002: vírus</li> <li>● 1003: worm</li> <li>● 1004: cavalo de Troia</li> <li>● 1005: rede de bots</li> <li>● 1006: backdoor</li> <li>● 1010: Rootkit</li> <li>● 1011: ransomware</li> <li>● 1012: ferramenta de hacker</li> <li>● 1015: web shell</li> <li>● 1016: mineração</li> <li>● 1017: shell reverso</li> <li>● 2001: exploração de vulnerabilidade comum</li> <li>● 2012: execução remota de código</li> <li>● 2047: exploração da vulnerabilidade do Redis</li> <li>● 2048: exploração da vulnerabilidade de Hadoop</li> <li>● 2049: exploração da vulnerabilidade de MySQL</li> <li>● 3002: escalonamento de privilégios de arquivo</li> <li>● 3003: escalonamento de privilégio de processo</li> <li>● 3004: alteração crítica de arquivo</li> <li>● 3005: alteração de arquivo/diretório</li> <li>● 3007: comportamento anormal do processo</li> <li>● 3015: execução de comandos de alto risco</li> <li>● 3018: shell anormal</li> <li>● 3026: escalonamento de privilégio de crontab</li> <li>● 3027: tarefa crontab suspeita</li> <li>● 3029: proteção do sistema desativada</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
			<ul style="list-style-type: none"> <li>● 3030: exclusão de backup</li> <li>● 3031: operações de registro suspeitas</li> <li>● 3036: bloqueio de imagem de container</li> <li>● 4002: ataque de força bruta</li> <li>● 4004: logon anormal</li> <li>● 4006: contas inválidas</li> <li>● 4014: conta adicionada</li> <li>● 4020: roubo de senha</li> <li>● 6002: verificação de porta</li> <li>● 6003: verificação do servidor</li> <li>● 13001: exclusão de eventos do Kubernetes</li> <li>● 13002: comportamento anormal do pod</li> <li>● 13003: enumeração de informações do usuário</li> <li>● 13004: vinculação de função de cluster</li> </ul> <p>Mínimo: <b>1000</b>  Máximo: <b>30000</b>  Comprimento da matriz: <b>1–500</b></p>
handle_status	Não	String	<p>Status. Seu valor pode ser:</p> <ul style="list-style-type: none"> <li>● unhandled</li> <li>● handled</li> </ul> <p>Mínimo: <b>1</b>  Máximo: <b>32</b></p>
severity	Não	String	<p>Nível de ameaça. Seu valor pode ser:</p> <ul style="list-style-type: none"> <li>● Security</li> <li>● Low</li> <li>● Medium</li> <li>● High</li> <li>● Critical</li> </ul> <p>Mínimo: <b>1</b>  Máximo: <b>32</b></p>

Parâmetro	Obrigatório	Tipo	Descrição
begin_time	Não	String	Hora de início personalizada de um segmento. O carimbo de data/hora tem precisão de segundos. O <b>begin_time</b> não deve ser mais do que dois dias antes do <b>end_time</b> . Este parâmetro é mutuamente exclusivo com a duração consultada. Mínimo: <b>13</b> Máximo: <b>13</b>
end_time	Não	String	Hora de término personalizada de um segmento. O carimbo de data/hora tem precisão de segundos. O <b>begin_time</b> não deve ser mais do que dois dias antes do <b>end_time</b> . Este parâmetro é mutuamente exclusivo com a duração consultada. Mínimo: <b>13</b> Máximo: <b>13</b>

Parâmetro	Obrigatório	Tipo	Descrição
event_class_ids	Não	Array	<p>ID do evento. Seu valor pode ser:</p> <ul style="list-style-type: none"> <li>● container_1001: namespace do container</li> <li>● container_1002: porta de container ativada</li> <li>● container_1003: opções de segurança de container</li> <li>● container_1004: diretório de montagem de container</li> <li>● containerescape_0001: chamada de sistema de alto risco</li> <li>● containerescape_0002: ataque de shocker</li> <li>● containerescape_0003: ataque de Dirty Cow</li> <li>● containerescape_0004: escape de arquivo de container</li> <li>● dockerfile_001: modificação do arquivo de container protegido definido pelo usuário</li> <li>● dockerfile_002: modificação de arquivos executáveis no sistema de arquivos do container</li> <li>● dockerproc_001: processo de container anormal</li> <li>● fileprotect_0001: escalonamento de privilégios de arquivo</li> <li>● fileprotect_0002: alteração de arquivo-chave</li> <li>● fileprotect_0003: alteração do caminho do arquivo-chave</li> <li>● fileprotect_0004: alteração de arquivo/diretório</li> <li>● av_1002: vírus</li> <li>● av_1003: worm</li> <li>● av_1004: cavalo de Troia</li> <li>● av_1005: rede de bots</li> <li>● av_1006: backdoor</li> <li>● av_1007: spyware</li> <li>● av_1008: adware malicioso</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
			<ul style="list-style-type: none"> <li>● av_1009: phishing</li> <li>● av_1010: Rootkit</li> <li>● av_1011: ransomware</li> <li>● av_1012: ferramenta de hacker</li> <li>● av_1013: grayware</li> <li>● av_1015: web shell</li> <li>● av_1016: software de mineração</li> <li>● login_0001: quebra de força bruta</li> <li>● login_0002: quebra bem-sucedida</li> <li>● login_1001: logon bem-sucedido</li> <li>● login_1002: logon remoto</li> <li>● login_1003: senha fraca</li> <li>● malware_0001: relatório de alteração do shell</li> <li>● malware_0002: relatório de shell reverso</li> <li>● malware_1001: programa malicioso</li> <li>● procdet_0001: detecção de comportamento anormal do processo</li> <li>● procdet_0002: escalonamento de privilégios de processo</li> <li>● crontab_0001: escalonamento de privilégios do script crontab</li> <li>● crontab_0002: escalonamento de privilégios do caminho malicioso</li> <li>● procreport_0001: comandos arriscados</li> <li>● user_1001: alteração de conta</li> <li>● user_1002: conta arriscada</li> <li>● vmescape_0001: execução de comando sensível à VM</li> <li>● vmescape_0002: acesso do processo de virtualização ao arquivo confidencial</li> <li>● vmescape_0003: acesso anormal à porta da VM</li> </ul>



Parâmetro	Obrigatório	Tipo	Descrição
			<ul style="list-style-type: none"> <li>● webshell_0001: web shell</li> <li>● network_1001: mineração maliciosa</li> <li>● network_1002: ataques DDoS</li> <li>● network_1003: verificação maliciosa</li> <li>● network_1004: ataque em áreas sensíveis</li> <li>● ransomware_0001: ataque de ransomware</li> <li>● ransomware_0002: ataque de ransomware</li> <li>● ransomware_0003: ataque de ransomware</li> <li>● fileless_0001: injeção de processo</li> <li>● fileless_0002: injeção de biblioteca dinâmica</li> <li>● fileless_0003: alteração na configuração da chave</li> <li>● fileless_0004: alteração na variável de ambiente</li> <li>● fileless_0005: processo de arquivo de memória</li> <li>● fileless_0006: sequestro de VDSO</li> <li>● crontab_1001: tarefa crontab suspeita</li> <li>● vul_exploit_0001: exploração da vulnerabilidade do Redis</li> <li>● vul_exploit_0002: exploração da vulnerabilidade de Hadoop</li> <li>● vul_exploit_0003: exploração da vulnerabilidade de MySQL</li> <li>● rootkit_0001: arquivo de rootkit suspeito</li> <li>● rootkit_0002: módulo de kernel suspeito</li> <li>● RASP_0004: upload de web shell</li> <li>● RASP_0018: web shell sem arquivo</li> <li>● blockexec_001: ataque de ransomware conhecido</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
			<ul style="list-style-type: none"> <li>● hips_0001: Windows Defender desativado</li> <li>● hips_0002: ferramenta de hacker suspeita</li> <li>● hips_0003: comportamento suspeito de criptografia de ransomware</li> <li>● hips_0004: criação de conta oculta</li> <li>● hips_0005: senha do usuário e leitura de credenciais</li> <li>● hips_0006: exportação suspeita de arquivos SAM</li> <li>● hips_0007: exclusão suspeita de cópia de sombra</li> <li>● hips_0008: exclusão de arquivo de backup</li> <li>● hips_0009: registro de ransomware suspeito</li> <li>● hips_0010: processo anormal suspeito</li> <li>● hips_0011: verificação suspeita</li> <li>● hips_0012: script de ransomware suspeito em execução</li> <li>● hips_0013: execução suspeita do comando de mineração</li> <li>● hips_0014: desativação suspeita da central de segurança do Windows</li> <li>● hips_0015: comportamento suspeito de desativar o serviço de firewall</li> <li>● hips_0016: desativação suspeita de recuperação automática do sistema</li> <li>● hips_0017: execução de arquivo executável em Office</li> <li>● hips_0018: criação de arquivo anormal com macros em Office</li> <li>● hips_0019: operação de registro suspeita</li> <li>● hips_0020: execução remota de código do Confluence</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
			<ul style="list-style-type: none"> <li>● hips_0021: execução remota de código de MSDT</li> <li>● portscan_0001: verificação de porta comum</li> <li>● portscan_0002: verificação de porta secreta</li> <li>● k8s_1001: exclusão de eventos do Kubernetes</li> <li>● k8s_1002: criações de pods privilegiados</li> <li>● k8s_1003: shell interativo usado no pod</li> <li>● k8s_1004: pod criado com diretório sensível</li> <li>● k8s_1005: pod criado com a rede do servidor</li> <li>● k8s_1006: pod criado com espaço de PID do host</li> <li>● k8s_1007: falha de autenticação quando pods comuns acessam o servidor da API</li> <li>● k8s_1008: acesso ao servidor de API do pod comum usando cURL</li> <li>● k8s_1009: exec no espaço de gerenciamento do sistema</li> <li>● k8s_1010: pod criado no espaço de gerenciamento</li> <li>● k8s_1011: criação de pod estático</li> <li>● k8s_1012: criação de DaemonSet</li> <li>● k8s_1013: criação de tarefa de cluster agendada</li> <li>● k8s_1014: operação em segredos</li> <li>● k8s_1015: enumeração de operação permitida</li> <li>● k8s_1016: RoleBinding ou ClusterRoleBinding de alto privilégio</li> <li>● k8s_1017: criação de ServiceAccount</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
			<ul style="list-style-type: none"> <li>● k8s_1018: criação de Cronjob</li> <li>● k8s_1019: shell interativo usado para exec em pods</li> <li>● k8s_1020: acesso não autorizado ao servidor da API</li> <li>● k8s_1021: acesso ao servidor de API com curl</li> <li>● k8s_1022: vulnerabilidade de entrada</li> <li>● k8s_1023: ataque man-in-the-middle (MITM)</li> <li>● k8s_1024: worm, mineração ou cavalo de Troia</li> <li>● k8s_1025: exclusão de evento de K8s</li> <li>● k8s_1026: SelfSubjectRules-Review</li> <li>● imgblock_0001: bloqueio de imagem com base na lista branca</li> <li>● imgblock_0002: bloqueio de imagem com base na lista negra</li> <li>● imgblock_0003: bloqueio de tag de imagem com base na lista branca</li> <li>● imgblock_0004: bloqueio de tags de imagem com base na lista negra</li> <li>● imgblock_0005: criação de container bloqueada com base na lista branca</li> <li>● imgblock_0006: criação de container bloqueada com base na lista negra</li> <li>● imgblock_0007: bloqueio de container mount proc</li> <li>● imgblock_0008: bloqueio de container seccomp unconfined</li> <li>● imgblock_0009: bloqueio de privilégios de container</li> <li>● imgblock_0010: bloqueio de recursos do container</li> </ul> <p>Comprimento da matriz: <b>1–200</b></p>

Parâmetro	Obrigatório	Tipo	Descrição
severity_list	Não	Array	Nível de ameaça. As opções são as seguintes: <ul style="list-style-type: none"> <li>● Security</li> <li>● Low</li> <li>● Medium</li> <li>● High</li> <li>● Critical</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b> Comprimento da matriz: <b>0-5</b>
attack_tag	Não	String	Indica o sinalizador de ataque. As opções são as seguintes: <ul style="list-style-type: none"> <li>● attack_success: sucesso do ataque</li> <li>● attack_attempt: tentativa de ataque</li> <li>● attack_blocked: ataque bloqueado</li> <li>● abnormal_behavior: comportamento anormal</li> <li>● collapsible_host: host comprometido</li> <li>● system_vulnerability: vulnerabilidade do sistema</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>
asset_value	Não	String	Importância de ativo. As opções são as seguintes: <ul style="list-style-type: none"> <li>● important</li> <li>● common</li> <li>● test</li> </ul> Mínimo: <b>0</b> Máximo: <b>128</b>
tag_list	Não	Array	Lista de tags de evento, por exemplo, ["hot event"]. Mínimo: <b>0</b> Máximo: <b>10</b> Comprimento da matriz: <b>0-20</b>

Parâmetro	Obrigatório	Tipo	Descrição
att_ck	Não	String	Estágio de ataque ATT&CK, incluindo: <ul style="list-style-type: none"> <li>● Reconnaissance</li> <li>● Initial Access</li> <li>● Execution</li> <li>● Persistence</li> <li>● Privilege Escalation</li> <li>● Defense Evasion: desvio de defesa</li> <li>● Credential Access</li> <li>● Command and Control</li> <li>● Impact: o dano é afetado.</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>
event_name	Não	String	Nome do alarme Mínimo: <b>1</b> Máximo: <b>128</b>

## Parâmetros de solicitação

**Tabela 3-234** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de <b>X-Subject-Token</b> no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-235** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total de eventos de alarme Mínimo: <b>0</b> Máximo: <b>2147483647</b>
data_list	Array of <b>EventManagementResponseInfo</b> objects	Lista de eventos Comprimento da matriz: <b>0-1000</b>

**Tabela 3-236** EventManagementResponseInfo

Parâmetro	Tipo	Descrição
event_id	String	ID do evento

Parâmetro	Tipo	Descrição
event_class_id	String	<p>Categoria do evento. Seu valor pode ser:</p> <ul style="list-style-type: none"> <li>● container_1001: namespace do container</li> <li>● container_1002: porta aberta do container</li> <li>● container_1003: opção de segurança de container</li> <li>● container_1004: diretório de montagem do container</li> <li>● containerescape_0001: chamada de sistema de alto risco</li> <li>● containerescape_0002: ataque de Shocker</li> <li>● containerescape_0003: ataque de Dirty Cow</li> <li>● containerescape_0004: escape do arquivo do container</li> <li>● dockerfile_001: modificação do arquivo de container protegido definido pelo usuário</li> <li>● dockerfile_002: modificação de arquivos executáveis no sistema de arquivos de container</li> <li>● dockerproc_001: processo de container anormal</li> <li>● fileprotect_0001: escalonamento de privilégio de arquivo</li> <li>● fileprotect_0002: alteração do arquivo de chave</li> <li>● fileprotect_0003: alteração do caminho do AuthorizedKeysFile</li> <li>● fileprotect_0004: alteração do diretório de arquivos</li> <li>● login_0001: tentativa de ataque com força bruta</li> <li>● login_0002: ataque de força bruta foi bem-sucedido</li> <li>● login_1001: logon bem-sucedido</li> <li>● login_1002: logon remoto</li> <li>● login_1003: senha fraca</li> <li>● malware_0001: mudança de shell</li> <li>● malware_0002: shell reverso</li> <li>● malware_1001: programa malicioso</li> <li>● procdet_0001: comportamento anormal do processo</li> <li>● procdet_0002: escalonamento de privilégio do processo</li> <li>● procreport_0001: comando de alto risco</li> <li>● user_1001: alteração de conta</li> <li>● user_1002: conta insegura</li> </ul>



Parâmetro	Tipo	Descrição
		<ul style="list-style-type: none"> <li>● vmescape_0001: comando sensível executado na VM</li> <li>● vmescape_0002: arquivo sensível acessado pelo processo de virtualização</li> <li>● vmescape_0003: acesso anormal à porta de VM</li> <li>● webshell_0001: web shell</li> <li>● network_1001: mineração</li> <li>● network_1002: ataques DDoS</li> <li>● network_1003: verificação maliciosa</li> <li>● network_1004: ataque em áreas sensíveis</li> <li>● ransomware_0001: ataque de ransomware</li> <li>● ransomware_0002: ataque de ransomware</li> <li>● ransomware_0003: ataque de ransomware</li> <li>● fileless_0001: injeção de processo</li> <li>● fileless_0002: injeção de biblioteca dinâmica</li> <li>● fileless_0003: alteração na configuração da chave</li> <li>● fileless_0004: alteração na variável de ambiente</li> <li>● fileless_0005: processo de arquivo de memória</li> <li>● fileless_0006: sequestro de VDSO</li> <li>● crontab_1001: tarefa crontab suspeita</li> <li>● vul_exploit_0001: exploração da vulnerabilidade do Redis</li> <li>● vul_exploit_0002: exploração da vulnerabilidade de Hadoop</li> <li>● vul_exploit_0003: exploração da vulnerabilidade de MySQL</li> <li>● rootkit_0001: arquivo de rootkit suspeito</li> <li>● rootkit_0002: módulo de kernel suspeito</li> <li>● RASP_0004: upload de web shell</li> <li>● RASP_0018: web shell sem arquivo</li> <li>● blockexec_001: ataque de ransomware conhecido</li> <li>● hips_0001: Windows Defender desativado</li> <li>● hips_0002: ferramenta de hacker suspeita</li> <li>● hips_0003: comportamento suspeito de criptografia de ransomware</li> <li>● hips_0004: criação de conta oculta</li> <li>● hips_0005: senha do usuário e leitura de credenciais</li> <li>● hips_0006: exportação suspeita de arquivos SAM</li> <li>● hips_0007: exclusão suspeita de cópia de sombra</li> </ul>

Parâmetro	Tipo	Descrição
		<ul style="list-style-type: none"> <li>● hips_0008: exclusão de arquivo de backup</li> <li>● hips_0009: registro de ransomware suspeito</li> <li>● hips_0010: processo anormal suspeito</li> <li>● hips_0011: verificação suspeita</li> <li>● hips_0012: script de ransomware suspeito em execução</li> <li>● hips_0013: execução suspeita do comando de mineração</li> <li>● hips_0014: desativação suspeita da central de segurança do Windows</li> <li>● hips_0015: comportamento suspeito de desativar o serviço de firewall</li> <li>● hips_0016: desativação suspeita de recuperação automática do sistema</li> <li>● hips_0017: execução de arquivo executável em Office</li> <li>● hips_0018: criação de arquivo anormal com macros em Office</li> <li>● hips_0019: operação de registro suspeita</li> <li>● hips_0020: execução remota de código do Confluence</li> <li>● hips_0021: execução remota de código de MSDT</li> <li>● portscan_0001: verificação de porta comum</li> <li>● portscan_0002: verificação de porta secreta</li> <li>● k8s_1001: exclusão de eventos do Kubernetes</li> <li>● k8s_1002: criações de pods privilegiados</li> <li>● k8s_1003: shell interativo usado no pod</li> <li>● k8s_1004: pod criado com diretório sensível</li> <li>● k8s_1005: pod criado com a rede do servidor</li> <li>● k8s_1006: pod criado com espaço de PID do host</li> <li>● k8s_1007: falha de autenticação quando pods comuns acessam o servidor da API</li> <li>● k8s_1008: acesso ao servidor de API do pod comum usando cURL</li> <li>● k8s_1009: exec no espaço de gerenciamento do sistema</li> <li>● k8s_1010: pod criado no espaço de gerenciamento</li> <li>● k8s_1011: criação de pod estático</li> <li>● k8s_1012: criação de DaemonSet</li> <li>● k8s_1013: criação de tarefa de cluster agendada</li> <li>● k8s_1014: operação em segredos</li> </ul>

Parâmetro	Tipo	Descrição
		<ul style="list-style-type: none"> <li>● k8s_1015: enumeração de operação permitida</li> <li>● k8s_1016: RoleBinding ou ClusterRoleBinding de alto privilégio</li> <li>● k8s_1017: criação de ServiceAccount</li> <li>● k8s_1018: criação de Cronjob</li> <li>● k8s_1019: shell interativo usado para exec em pods</li> <li>● k8s_1020: acesso não autorizado ao servidor da API</li> <li>● k8s_1021: acesso ao servidor de API com curl</li> <li>● k8s_1022: vulnerabilidade de entrada</li> <li>● k8s_1023: ataque man-in-the-middle (MITM)</li> <li>● k8s_1024: worm, mineração ou cavalo de Troia</li> <li>● k8s_1025: exclusão de evento de K8s</li> <li>● k8s_1026: SelfSubjectRulesReview</li> <li>● imgblock_0001: bloqueio de imagem com base na lista branca</li> <li>● imgblock_0002: bloqueio de imagem com base na lista negra</li> <li>● imgblock_0003: bloqueio de tag de imagem com base na lista branca</li> <li>● imgblock_0004: bloqueio de tags de imagem com base na lista negra</li> <li>● imgblock_0005: criação de container bloqueada com base na lista branca</li> <li>● imgblock_0006: criação de container bloqueada com base na lista negra</li> <li>● imgblock_0007: bloqueio de container mount proc</li> <li>● imgblock_0008: bloqueio de container seccomp unconfined</li> <li>● imgblock_0009: bloqueio de privilégios de container</li> <li>● imgblock_0010: bloqueio de recursos do container</li> </ul>

Parâmetro	Tipo	Descrição
event_type	Integer	<p>Tipo de evento. Seu valor pode ser:</p> <ul style="list-style-type: none"><li>● 1001: malware comum</li><li>● 1002: vírus</li><li>● 1003: worm</li><li>● 1004: cavalo de Troia</li><li>● 1005: rede de bots</li><li>● 1006: backdoor</li><li>● 1010: Rootkit</li><li>● 1011: ransomware</li><li>● 1012: ferramenta de hacker</li><li>● 1015: web shell</li><li>● 1016: mineração</li><li>● 1017: shell reverso</li><li>● 2001: exploração de vulnerabilidade comum</li><li>● 2012: execução remota de código</li><li>● 2047: exploração da vulnerabilidade do Redis</li><li>● 2048: exploração da vulnerabilidade de Hadoop</li><li>● 2049: exploração da vulnerabilidade de MySQL</li><li>● 3002: escalonamento de privilégios de arquivo</li><li>● 3003: escalonamento de privilégio de processo</li><li>● 3004: alteração crítica de arquivo</li><li>● 3005: alteração de arquivo/diretório</li><li>● 3007: comportamento anormal do processo</li><li>● 3015: execução de comandos de alto risco</li><li>● 3018: shell anormal</li><li>● 3027: tarefa crontab suspeita</li><li>● 3029: proteção do sistema desativada</li><li>● 3030: exclusão de backup</li><li>● 3031: operações de registro suspeitas</li><li>● 3036: bloqueio de imagem de container</li><li>● 4002: ataque de força bruta</li><li>● 4004: logon anormal</li><li>● 4006: contas inválidas</li><li>● 4014: conta adicionada</li><li>● 4020: roubo de senha</li><li>● 6002: verificação de porta</li><li>● 6003: verificação do servidor</li><li>● 13001: exclusão de eventos do Kubernetes</li><li>● 13002: comportamento anormal do pod</li></ul>

Parâmetro	Tipo	Descrição
		<ul style="list-style-type: none"> <li>● 13003: enumeração de informações do usuário</li> <li>● 13004: vinculação de função de cluster</li> </ul>
event_name	String	Nome do evento
severity	String	Nível de ameaça. Seu valor pode ser: <ul style="list-style-type: none"> <li>● Security</li> <li>● Low</li> <li>● Medium</li> <li>● High</li> <li>● Critical</li> </ul>
container_name	String	Nome da instância do container. Esta API está disponível apenas para alarmes de container.
image_name	String	Nome da imagem. Esta API está disponível apenas para alarmes de container.
host_name	String	Nome de servidor
host_id	String	ID do host
private_ip	String	Endereço IP privado de servidor
public_ip	String	Endereço IP elástico
os_type	String	Tipo de SO. Seu valor pode ser: <ul style="list-style-type: none"> <li>● Linux</li> <li>● Windows</li> </ul>
host_status	String	Status do servidor. As opções são as seguintes: <ul style="list-style-type: none"> <li>● ACTIVE</li> <li>● SHUTOFF</li> <li>● BUILDING</li> <li>● ERROR</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>
agent_status	String	Status de agente. Seu valor pode ser: <ul style="list-style-type: none"> <li>● installed</li> <li>● not_installed</li> <li>● online</li> <li>● offline</li> <li>● install_failed</li> <li>● installing</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>

Parâmetro	Tipo	Descrição
protect_status	String	Status de proteção. Seu valor pode ser: <ul style="list-style-type: none"><li>● closed</li><li>● opened</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
asset_value	String	Importância de ativo. As opções são as seguintes: <ul style="list-style-type: none"><li>● important</li><li>● common</li><li>● test</li></ul> Mínimo: <b>0</b> Máximo: <b>128</b>
attack_phase	String	Fase de ataque. Seu valor pode ser: <ul style="list-style-type: none"><li>● reconnaissance</li><li>● weaponization</li><li>● delivery</li><li>● exploit</li><li>● installation</li><li>● command_and_control</li><li>● actions</li></ul>
attack_tag	String	Tag de ataque. Seu valor pode ser: <ul style="list-style-type: none"><li>● attack_success</li><li>● attack_attempt</li><li>● attack_blocked</li><li>● abnormal_behavior</li><li>● collapsible_host</li><li>● system_vulnerability</li></ul>
occur_time	Integer	Tempo de ocorrência, com precisão de milissegundos.
handle_time	Integer	Tempo de manipulação, em milissegundos. Esta API está disponível apenas para alarmes manipulados.
handle_status	String	Status de processamento. Seu valor pode ser: <ul style="list-style-type: none"><li>● unhandled</li><li>● handled</li></ul>

Parâmetro	Tipo	Descrição
handle_method	String	Método de manipulação. Esta API está disponível apenas para alarmes manipulados. As opções são as seguintes: <ul style="list-style-type: none"> <li>● mark_as_handled</li> <li>● ignore</li> <li>● add_to_alarm_whitelist</li> <li>● add_to_login_whitelist</li> <li>● isolate_and_kill</li> </ul>
handler	String	Observações. Esta API está disponível apenas para alarmes manipulados.
operate_accept_list	Array of strings	Operação de processamento suportada
operate_detail_list	Array of <a href="#">EventDetailResponseInfo</a> objects	Lista de detalhes da operação (não exibida na página) Comprimento da matriz: <b>0–100</b>
forensic_info	Object	Informações de ataque, em formato JSON.
resource_info	<a href="#">EventResourceResponseInfo</a> object	Informações de recurso
geo_info	Object	Localização geográfica, em formato JSON.
malware_info	Object	Informações de malware, em formato JSON.
network_info	Object	Informações de rede, em formato JSON.
app_info	Object	Informações da aplicação, em formato JSON.
system_info	Object	Informações do sistema, em formato JSON.
extend_info	Object	Informações de evento estendidas, no formato JSON
recommendation	String	Sugestões de manipulação
description	String	Descrição do alarme Mínimo: <b>0</b> Máximo: <b>1024</b>
event_abstract	String	Resumo do evento Mínimo: <b>0</b> Máximo: <b>512</b>

Parâmetro	Tipo	Descrição
process_info_list	Array of <b>EventProcessResponseInfo</b> objects	Lista de informações do processo Comprimento da matriz: <b>0–100</b>
user_info_list	Array of <b>EventUserResponseInfo</b> objects	Lista de informações do usuário Comprimento da matriz: <b>0–100</b>
file_info_list	Array of <b>EventFileResponseInfo</b> objects	Lista de informações do arquivo Comprimento da matriz: <b>0–100</b>
event_details	String	Breve descrição do evento. Mínimo: <b>0</b> Máximo: <b>204800</b>
tag_list	Array of strings	Tags Mínimo: <b>0</b> Máximo: <b>10</b> Comprimento da matriz: <b>0–20</b>
event_count	Integer	Ocorrências de eventos Mínimo: <b>0</b> Máximo: <b>2147483647</b>

**Tabela 3-237** EventDetailResponseInfo

Parâmetro	Tipo	Descrição
agent_id	String	ID do agente
process_pid	Integer	ID do processo
is_parent	Boolean	Se um processo é um processo pai
file_hash	String	Hash de arquivo
file_path	String	Caminho do arquivo
file_attr	String	Atributo de arquivo
private_ip	String	Endereço IP privado de servidor
login_ip	String	Endereço IP de origem de logon
login_username	String	Nome de usuário de logon



Parâmetro	Tipo	Descrição
keyword	String	Palavra-chave de evento de alarme, que é usada apenas para a lista branca de alarmes.
hash	String	Hash de evento de alarme, que é usado apenas para a lista branca de alarme.

**Tabela 3-238** EventResourceResponseInfo

Parâmetro	Tipo	Descrição
domain_id	String	ID da conta de usuário
project_id	String	ID do projeto
enterprise_project_id	String	ID do projeto empresarial
region_name	String	Nome da região
vpc_id	String	ID de VPC
cloud_id	String	ID do ECS
vm_name	String	Nome da VM
vm_uuid	String	Especifica o UUID da VM, ou seja, o ID do host.
container_id	String	ID do container
container_status	String	Status do container
pod_uuid	String	UID do pod
pod_name	String	Nome do pod
namespace	String	namespace
cluster_id	String	ID do cluster
cluster_name	String	Nome do cluster
image_id	String	ID da imagem
image_name	String	Nome da imagem
host_attr	String	Atributo do host
service	String	Serviço
micro_service	String	Microserviço
sys_arch	String	Arquitetura da CPU do sistema
os_bit	String	Versão de bit do SO
os_type	String	Tipo de SO

Parâmetro	Tipo	Descrição
os_name	String	Nome de SO
os_version	String	Versão de SO

**Tabela 3-239** EventProcessResponseInfo

Parâmetro	Tipo	Descrição
process_name	String	Nome do processo
process_path	String	Caminho do arquivo de processo
process_pid	Integer	ID do processo Mínimo: <b>0</b> Máximo: <b>2147483647</b>
process_uid	Integer	ID do usuário do processo Mínimo: <b>0</b> Máximo: <b>2147483647</b>
process_username	String	Nome de usuário do processo
process_cmdline	String	Linha de comando do arquivo de processo
process_filename	String	Nome do arquivo do processo
process_start_time	Long	Hora de início do processo Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b>
process_gid	Integer	ID do grupo de processos Mínimo: <b>0</b> Máximo: <b>2147483647</b>
process_egid	Integer	ID de grupo de processos válido Mínimo: <b>0</b> Máximo: <b>2147483647</b>
process_euid	Integer	ID de usuário do processo válido Mínimo: <b>0</b> Máximo: <b>2147483647</b>
ancestor_process_path	String	Caminho do arquivo de processo avô

Parâmetro	Tipo	Descrição
ancestor_process_pid	Integer	ID do processo avô Mínimo: <b>0</b> Máximo: <b>2147483647</b>
ancestor_process_cmdline	String	Linha de comando do arquivo de processo avô
parent_process_name	String	Nome do processo pai
parent_process_path	String	Caminho do arquivo do processo pai
parent_process_pid	Integer	ID do processo pai Mínimo: <b>0</b> Máximo: <b>2147483647</b>
parent_process_uid	Integer	ID de usuário do processo pai Mínimo: <b>0</b> Máximo: <b>2147483647</b>
parent_process_cmdline	String	Linha de comando do arquivo do processo pai
parent_process_filename	String	Nome do arquivo do processo pai
parent_process_start_time	Long	Hora de início do processo pai Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b>
parent_process_gid	Integer	ID do grupo de processos pai Mínimo: <b>0</b> Máximo: <b>2147483647</b>
parent_process_egid	Integer	ID do grupo de processos pai válido Mínimo: <b>0</b> Máximo: <b>2147483647</b>
parent_process_euid	Integer	ID de usuário do processo pai válido Mínimo: <b>0</b> Máximo: <b>2147483647</b>
child_process_name	String	Nome do subprocesso
child_process_path	String	Caminho do arquivo do subprocesso

Parâmetro	Tipo	Descrição
child_process_pid	Integer	ID do subprocesso Mínimo: <b>0</b> Máximo: <b>2147483647</b>
child_process_uid	Integer	ID do usuário do subprocesso Mínimo: <b>0</b> Máximo: <b>2147483647</b>
child_process_cmdline	String	Linha de comando do arquivo do subprocesso
child_process_filename	String	Nome do arquivo do subprocesso
child_process_start_time	Long	Hora de início do subprocesso Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b>
child_process_gid	Integer	ID do grupo de subprocessos Mínimo: <b>0</b> Máximo: <b>2147483647</b>
child_process_egid	Integer	ID de grupo de subprocessos válido Mínimo: <b>0</b> Máximo: <b>2147483647</b>
child_process_euid	Integer	ID de usuário de subprocesso válido Mínimo: <b>0</b> Máximo: <b>2147483647</b>
virt_cmd	String	Comando de virtualização
virt_process_name	String	Nome do processo de virtualização
escape_mode	String	Modo de escape
escape_cmd	String	Comandos executados após o escape
process_hash	String	Hash do arquivo de inicialização do processo
process_file_hash	String	Hash do arquivo de processo
parent_process_file_hash	String	Hash do arquivo do processo pai
block	Integer	Indica se o bloqueio foi bem-sucedido. 1: sim 0: não Mínimo: <b>0</b> Máximo: <b>1</b>

**Tabela 3-240** EventUserResponseInfo

Parâmetro	Tipo	Descrição
user_id	Integer	UID do usuário Mínimo: <b>0</b> Máximo: <b>2147483647</b>
user_gid	Integer	GID do usuário Mínimo: <b>0</b> Máximo: <b>2147483647</b>
user_name	String	Nome de usuário
user_group_name	String	Nome do grupo de usuários
user_home_dir	String	Diretório inicial do usuário
login_ip	String	Endereço IP de logon do usuário
service_type	String	Tipo de serviço. As opções são as seguintes: <ul style="list-style-type: none"><li>● system</li><li>● mysql</li><li>● redis</li></ul>
service_port	Integer	Porta de serviço de logon Mínimo: <b>0</b> Máximo: <b>2147483647</b>
login_mode	Integer	Modo de logon Mínimo: <b>0</b> Máximo: <b>2147483647</b>
login_last_time	Long	Hora do último logon Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b>
login_fail_count	Integer	Número de tentativas de logon com falha Mínimo: <b>0</b> Máximo: <b>2147483647</b>
pwd_hash	String	Hash de senha
pwd_with_fuzzing	String	Senha mascarada

Parâmetro	Tipo	Descrição
pwd_used_days	Integer	Idade da senha (dias) Mínimo: <b>0</b> Máximo: <b>2147483647</b>
pwd_min_days	Integer	Período mínimo de validade da senha Mínimo: <b>0</b> Máximo: <b>2147483647</b>
pwd_max_days	Integer	Período máximo de validade da senha Mínimo: <b>0</b> Máximo: <b>2147483647</b>
pwd_warn_left_days	Integer	Aviso prévio de expiração da senha (dias) Mínimo: <b>0</b> Máximo: <b>2147483647</b>

**Tabela 3-241** EventFileResponseInfo

Parâmetro	Tipo	Descrição
file_path	String	Caminho do arquivo
file_alias	String	Alias do arquivo
file_size	Integer	Tamanho do arquivo Mínimo: <b>0</b> Máximo: <b>2147483647</b>
file_mtime	Long	Hora em que um arquivo foi modificado pela última vez Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b>
file_atime	Long	Hora em que um arquivo foi acessado pela última vez Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b>
file_ctime	Long	Hora em que o status de um arquivo foi alterado pela última vez Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b>
file_hash	String	O valor de hash calculado usando o algoritmo SHA256.
file_md5	String	Arquivo MD5

Parâmetro	Tipo	Descrição
file_sha256	String	Arquivo SHA256
file_type	String	Tipo de arquivo
file_content	String	Conteúdo do arquivo
file_attr	String	Atributo de arquivo
file_operation	Integer	Tipo de operação de arquivo Mínimo: <b>0</b> Máximo: <b>2147483647</b>
file_action	String	Ação de arquivo
file_change_attr	String	Atributo anterior/novo
file_new_path	String	Novo caminho de arquivo
file_desc	String	Descrição do arquivo
file_key_word	String	Palavra-chave do arquivo
is_dir	Boolean	Se é um diretório
fd_info	String	Informações sobre o identificador de arquivo
fd_count	Integer	Número de identificadores de arquivo Mínimo: <b>0</b> Máximo: <b>2147483647</b>

## Exemplo de solicitações

Consultar os primeiros 50 eventos de servidor não processados cujo projeto empresarial é xxx.

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

## Exemplo de respostas

**Código de status: 200**

Lista de intrusões

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

```
    "ip" : "127.0.0.1",
    "user" : "zhangsan",
    "sub_division" : "Gansu",
    "city_id" : 3110
  },
  "handle_status" : "unhandled",
  "host_name" : "xxx",
  "occur_time" : 1661593036627,
  "operate_accept_list" : [ "ignore" ],
  "operate_detail_list" : [ {
    "agent_id" :
"c9bed5397db449ebdfba15e85fcfc36accee125c68954daf5cab0528bab59bd8",
    "file_hash" :
"e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
    "file_path" : "/usr/test",
    "process_pid" : 3123,
    "file_attr" : 33261,
    "keyword" : "file_path=/usr/test",
    "hash" : "e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
    "login_ip" : "127.0.0.1",
    "private_ip" : "127.0.0.2",
    "login_user_name" : "root",
    "is_parent" : false
  } ],
  "private_ip" : "127.0.0.1",
  "resource_info" : {
    "region_name" : "",
    "project_id" : "",
    "enterprise_project_id" : "0",
    "os_type" : "Linux",
    "os_version" : "2.5",
    "vm_name" : "",
    "vm_uuid" : "71a15ecc",
    "cloud_id" : "",
    "container_id" : "",
    "container_status" : "running / terminated",
    "image_id" : "",
    "pod_uid" : "",
    "pod_name" : "",
    "namespace" : "",
    "cluster_id" : "",
    "cluster_name" : ""
  },
  "severity" : "Medium",
  "extend_info" : "",
  "os_type" : "Linux",
  "agent_status" : "online",
  "asset_value" : "common",
  "protect_status" : "opened",
  "host_status" : "ACTIVE",
  "event_details" : "file_path:/root/test",
  "user_info_list" : [ {
    "login_ip" : "",
    "service_port" : 22,
    "service_type" : "ssh",
    "user_name" : "zhangsan",
    "login_mode" : 0,
    "login_last_time" : 1661593024,
    "login_fail_count" : 0
  } ],
  "process_info_list" : [ {
    "process_path" : "/root/test",
    "process_name" : "test",
    "process_cmdline" : "/bin/bash",
    "process_hash" :
"e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
    "process_filename" : "test",
    "process_file_hash" :
"e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
```



```
"process_username" : "root",
"process_pid" : 372612,
"process_uid" : 10000,
"process_gid" : 10000,
"process_egid" : 10000,
"process_euid" : 10000,
"process_start_time" : 1661593024,
"block" : 0,
"parent_process_path" : "/usr/bin/bash",
"parent_process_name" : "test",
"parent_process_cmdline" : "/bin/bash",
"parent_process_filename" : "test",
"parent_process_file_hash" :
"e8b50f0b91e3dce0885ccc5902846b139d28108a0a7976c9b8d43154c5dbc44d",
"parent_process_pid" : 372612,
"parent_process_uid" : 10000,
"parent_process_gid" : 10000,
"parent_process_egid" : 10000,
"parent_process_euid" : 10000,
"parent_process_start_time" : 1661593024,
"child_process_path" : "/usr/bin/bash",
"child_process_name" : "test",
"child_process_cmdline" : "/bin/bash",
"child_process_filename" : "test",
"child_process_pid" : 372612,
"child_process_uid" : 10000,
"child_process_gid" : 10000,
"child_process_egid" : 10000,
"child_process_euid" : 10000,
"child_process_start_time" : 1661593024,
"virt_process_name" : "test",
"virt_cmd" : "/bin/bash",
"escape_cmd" : "/bin/bash",
"escape_mode" : "0",
"ancestor_process_pid" : 372612,
"ancestor_process_cmdline" : "/bin/bash",
"ancestor_process_path" : "/usr/bin/bash"
} ],
"description" : "",
"event_abstract" : "",
"tag_list" : [ "Hot Event" ]
} ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

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

public class ListSecurityEventsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in
```

plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.

// In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD\_SDK\_AK and CLOUD\_SDK\_SK in the local environment

```
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");

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

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

ListSecurityEventsRequest request = new ListSecurityEventsRequest();
request.withCategory("<category>");
request.withEnterpriseProjectId("<enterprise_project_id>");
request.withLastDays(<last_days>);
request.withHostName("<host_name>");
request.withHostId("<host_id>");
request.withPrivateIp("<private_ip>");
request.withPublicIp("<public_ip>");
request.withContainerName("<container_name>");
request.withOffset(<offset>);
request.withLimit(<limit>);
request.withEventTypes();
request.withHandleStatus("<handle_status>");
request.withSeverity("<severity>");
request.withBeginTime("<begin_time>");
request.withEndTime("<end_time>");
request.withEventClassIds();
request.withSeverityList();
request.withAttackTag("<attack_tag>");
request.withAssetValue("<asset_value>");
request.withTagList();
request.withAttCk("<att_ck>");
request.withEventName("<event_name>");
try {
    ListSecurityEventsResponse response =
client.listSecurityEvents(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

```
# coding: utf-8

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

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
```

plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.

# In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD\_SDK\_AK and CLOUD\_SDK\_SK in the local environment

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

credentials = BasicCredentials(ak, sk) \

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

try:
    request = ListSecurityEventsRequest()
    request.category = "<category>"
    request.enterprise_project_id = "<enterprise_project_id>"
    request.last_days = <last_days>
    request.host_name = "<host_name>"
    request.host_id = "<host_id>"
    request.private_ip = "<private_ip>"
    request.public_ip = "<public_ip>"
    request.container_name = "<container_name>"
    request.offset = <offset>
    request.limit = <limit>
    request.event_types =
    request.handle_status = "<handle_status>"
    request.severity = "<severity>"
    request.begin_time = "<begin_time>"
    request.end_time = "<end_time>"
    request.event_class_ids =
    request.severity_list =
    request.attack_tag = "<attack_tag>"
    request.asset_value = "<asset_value>"
    request.tag_list =
    request.att_ck = "<att_ck>"
    request.event_name = "<event_name>"
    response = client.list_security_events(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

```
package main

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

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

```
sk := os.Getenv("CLOUD_SDK_SK")

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

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

request := &model.ListSecurityEventsRequest{
    request.Category = "<category>"
    enterpriseProjectIdRequest := "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    lastDaysRequest := int32(<last_days>)
    request.LastDays = &lastDaysRequest
    hostNameRequest := "<host_name>"
    request.HostName = &hostNameRequest
    hostIdRequest := "<host_id>"
    request.HostId = &hostIdRequest
    privateIpRequest := "<private_ip>"
    request.PrivateIp = &privateIpRequest
    publicIpRequest := "<public_ip>"
    request.PublicIp = &publicIpRequest
    containerNameRequest := "<container_name>"
    request.ContainerName = &containerNameRequest
    offsetRequest := int32(<offset>)
    request.Offset = &offsetRequest
    limitRequest := int32(<limit>)
    request.Limit = &limitRequest
    handleStatusRequest := "<handle_status>"
    request.HandleStatus = &handleStatusRequest
    severityRequest := "<severity>"
    request.Severity = &severityRequest
    beginTimeRequest := "<begin_time>"
    request.BeginTime = &beginTimeRequest
    endTimeRequest := "<end_time>"
    request.EndTime = &endTimeRequest
    attackTagRequest := "<attack_tag>"
    request.AttackTag = &attackTagRequest
    assetValueRequest := "<asset_value>"
    request.AssetValue = &assetValueRequest
    attCkRequest := "<att_ck>"
    request.AttCk = &attCkRequest
    eventNameRequest := "<event_name>"
    request.EventName = &eventNameRequest
    response, err := client.ListSecurityEvents(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia [Código de amostra no API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de intrusões

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.7.3 Consulta da lista branca de alarmes

#### Função

Essa API é usada para consultar a lista branca de alarmes.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/event/white-list/alarm

**Tabela 3-242** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>20</b> Máximo: <b>64</b>

**Tabela 3-243** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>64</b>

Parâmetro	Obrigatório	Tipo	Descrição
hash	Não	String	Valor de hash da descrição da lista branca de eventos (algoritmo SHA256) Mínimo: <b>64</b> Máximo: <b>64</b>

Parâmetro	Obrigatório	Tipo	Descrição
event_type	Não	Integer	<p>Tipo de evento. Seu valor pode ser:</p> <ul style="list-style-type: none"> <li>● 1001: malware comum</li> <li>● 1002: vírus</li> <li>● 1003: worm</li> <li>● 1004: cavalo de Troia</li> <li>● 1005: rede de bots</li> <li>● 1006: backdoor</li> <li>● 1010: Rootkit</li> <li>● 1011: ransomware</li> <li>● 1012: ferramenta de hacker</li> <li>● 1015: web shell</li> <li>● 1016: mineração</li> <li>● 1017: shell reverso</li> <li>● 2001: exploração de vulnerabilidade comum</li> <li>● 2012: execução remota de código</li> <li>● 2047: exploração da vulnerabilidade do Redis</li> <li>● 2048: exploração da vulnerabilidade de Hadoop</li> <li>● 2049: exploração da vulnerabilidade de MySQL</li> <li>● 3002: escalonamento de privilégios de arquivo</li> <li>● 3003: escalonamento de privilégio de processo</li> <li>● 3004: alteração crítica de arquivo</li> <li>● 3005: alteração de arquivo/ diretório</li> <li>● 3007: comportamento anormal do processo</li> <li>● 3015: execução de comandos de alto risco</li> <li>● 3018: shell anormal</li> <li>● 3027: tarefa crontab suspeita</li> <li>● 3029: proteção do sistema desativada</li> <li>● 3030: exclusão de backup</li> </ul>

Parâmetro	Obrigatório	Tipo	Descrição
			<ul style="list-style-type: none"> <li>● 3031: operações de registro suspeitas</li> <li>● 4002: ataque de força bruta</li> <li>● 4004: logon anormal</li> <li>● 4006: conta do sistema inválida</li> <li>● 4014: conta adicionada</li> <li>● 4020: roubo de senha</li> <li>● 6003: verificação do servidor</li> </ul> <p>Mínimo: <b>1000</b> Máximo: <b>30000</b></p>
offset	Não	Integer	<p>Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número.</p> <p>Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b></p>
limit	Não	Integer	<p>Número de registros exibidos em cada página.</p> <p>Mínimo: <b>10</b> Máximo: <b>1000</b> Padrão: <b>10</b></p>

## Parâmetros de solicitação

Tabela 3-244 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	<p>Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token.</p> <p>Mínimo: <b>1</b> Máximo: <b>32768</b></p>
region	Sim	String	<p>ID da região</p> <p>Mínimo: <b>0</b> Máximo: <b>128</b></p>



## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-245** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total
event_type_list	Array of integers	Tipos de eventos que podem ser filtrados Mínimo: <b>0</b> Máximo: <b>2147483647</b> Comprimento da matriz: <b>0-30000</b>
data_list	Array of <a href="#">AlarmWhiteListResponseInfo</a> objects	Detalhes da lista branca do alarme Comprimento da matriz: <b>0-100</b>

**Tabela 3-246** AlarmWhiteListResponseInfo

Parâmetro	Tipo	Descrição
enterprise_project_name	String	Nome do projeto empresarial
hash	String	Valor de hash da descrição da lista branca de eventos (algoritmo SHA256)
description	String	Descrição

Parâmetro	Tipo	Descrição
event_type	Integer	<p>Tipo de evento. Seu valor pode ser:</p> <ul style="list-style-type: none"> <li>● 1001: malware comum</li> <li>● 1002: vírus</li> <li>● 1003: worm</li> <li>● 1004: cavalo de Troia</li> <li>● 1005: rede de bots</li> <li>● 1006: backdoor</li> <li>● 1010: Rootkit</li> <li>● 1011: ransomware</li> <li>● 1012: ferramenta de hacker</li> <li>● 1015: web shell</li> <li>● 1016: mineração</li> <li>● 1017: shell reverso</li> <li>● 2001: exploração de vulnerabilidade comum</li> <li>● 2012: execução remota de código</li> <li>● 2047: exploração da vulnerabilidade do Redis</li> <li>● 2048: exploração da vulnerabilidade de Hadoop</li> <li>● 2049: exploração da vulnerabilidade de MySQL</li> <li>● 3002: escalonamento de privilégios de arquivo</li> <li>● 3003: escalonamento de privilégio de processo</li> <li>● 3004: alteração crítica de arquivo</li> <li>● 3005: alteração de arquivo/diretório</li> <li>● 3007: comportamento anormal do processo</li> <li>● 3015: execução de comandos de alto risco</li> <li>● 3018: shell anormal</li> <li>● 3027: tarefa crontab suspeita</li> <li>● 3029: proteção do sistema desativada</li> <li>● 3030: exclusão de backup</li> <li>● 3031: operações de registro suspeitas</li> <li>● 3036: bloqueio de imagem de container</li> <li>● 4002: ataque de força bruta</li> <li>● 4004: logon anormal</li> <li>● 4006: contas inválidas</li> <li>● 4014: conta adicionada</li> <li>● 4020: roubo de senha</li> <li>● 6002: verificação de porta</li> <li>● 6003: verificação do servidor</li> <li>● 13001: exclusão de eventos do Kubernetes</li> <li>● 13002: comportamento anormal do pod</li> </ul>

Parâmetro	Tipo	Descrição
		<ul style="list-style-type: none"> <li>● 13003: enumeração de informações do usuário</li> <li>● 13004: vinculação de função de cluster</li> </ul>
white_field	String	Campos da lista branca. As opções são as seguintes: <ul style="list-style-type: none"> <li>● "file/process hash" # hash de processo/arquivo</li> <li>● "file_path"</li> <li>● "process_path"</li> <li>● "login_ip" # endereço IP de logon</li> <li>● "reg_key" # chave de registro</li> <li>● "process_cmdline" # linha de comando do processo</li> <li>● "username"</li> </ul> Mínimo: 1 Máximo: 20
field_value	String	Valor dos campos da lista branca Mínimo: 1 Máximo: 128
judge_type	String	Curinga. As opções são as seguintes: <ul style="list-style-type: none"> <li>● "equal"</li> <li>● "contain"</li> </ul> Mínimo: 1 Máximo: 10
update_time	Long	Hora em que a lista branca de eventos é atualizada, em milissegundos. Mínimo: 0 Máximo: 9223372036854775807

## Exemplo de solicitações

Consultar as 10 primeiras listas brancas de alarmes cujo projeto empresarial é xxx.

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

## Exemplo de respostas

**Código de status: 200**

Lista branca de alarmes

```
{
  "data_list" : [ {
    "enterprise_project_name" : "All projects",
    "event_type" : 1001,
```

```
"hash" : "9ab079e5398cba3a368ccffbd478f54c5ec3edadf6284ec049a73c36419f1178",
"description" : "/opt/cloud/3rdComponent/install/jre-8u201/bin/java",
"update_time" : 1665715677307,
"white_field" : "process/file hash",
"judge_type" : "contain",
"field_value" : "abcd12345612311112212323"
} ],
"event_type_list" : [ 1001 ],
"total_num" : 1
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListAlarmWhiteListSolution {

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

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

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
            .build();
        ListAlarmWhiteListRequest request = new ListAlarmWhiteListRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withHash("<hash>");
        request.withEventType("<event_type>");
        request.withOffset("<offset>");
        request.withLimit("<limit>");
        try {
            ListAlarmWhiteListResponse response =
client.listAlarmWhiteList(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
        }
    }
}
```

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

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListAlarmWhiteListRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.hash = "<hash>"
        request.event_type = <event_type>
        request.offset = <offset>
        request.limit = <limit>
        response = client.list_alarm_white_list(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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

```
sk := os.Getenv("CLOUD_SDK_SK")

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

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

request := &model.ListAlarmWhiteListRequest{
    enterpriseProjectIdRequest:= "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    hashRequest:= "<hash>"
    request.Hash = &hashRequest
    eventTypeRequest:= int32(<event_type>)
    request.EventType = &eventTypeRequest
    offsetRequest:= int32(<offset>)
    request.Offset = &offsetRequest
    limitRequest:= int32(<limit>)
    request.Limit = &limitRequest
    response, err := client.ListAlarmWhiteList(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista branca de alarmes

## Códigos de erro

Consulte [Códigos de erro](#).

# 3.8 Gerenciamento de servidores

## 3.8.1 Consulta de ECSs

### Função

Essa API é usada para consultar ECSs.

## Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

## URI

GET /v5/{project\_id}/host-management/hosts

**Tabela 3-247** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-248** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>
version	Não	String	Edição do HSS. Seu valor pode ser: <ul style="list-style-type: none"><li>● hss.version.null</li><li>● hss.version.basic: edição básica</li><li>● hss.version.advanced: edição profissional</li><li>● hss.version.enterprise: edição empresarial</li><li>● hss.version.premium: edição premium</li><li>● hss.version.wtp: edição WTP</li><li>● hss.version.container.enterprise : edição de container</li></ul> Mínimo: <b>1</b> Máximo: <b>64</b>

Parâmetro	Obrigatório	Tipo	Descrição
agent_status	Não	String	Status de agente. Seu valor pode ser: <ul style="list-style-type: none"> <li>● not_installed</li> <li>● online</li> <li>● offline</li> <li>● install_failed</li> <li>● installing</li> <li>● not_online: todos os status, exceto <b>online</b>, que é usado apenas como uma condição de consulta.</li> </ul> Mínimo: <b>1</b> Máximo: <b>20</b>
detect_result	Não	String	Resultado da detecção. Seu valor pode ser: <ul style="list-style-type: none"> <li>● undetected</li> <li>● clean</li> <li>● risk</li> <li>● scanning</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>
host_name	Não	String	Nome de servidor
host_id	Não	String	ID de servidor
host_status	Não	String	Status de host. Seu valor pode ser: <ul style="list-style-type: none"> <li>● ACTIVE</li> <li>● SHUTOFF</li> <li>● BUILDING</li> <li>● ERROR</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>
os_type	Não	String	Tipo de SO. Seu valor pode ser: <ul style="list-style-type: none"> <li>● Linux</li> <li>● Windows</li> </ul> Mínimo: <b>0</b> Máximo: <b>64</b>
private_ip	Não	String	Endereço IP privado de servidor
public_ip	Não	String	Endereço IP público do servidor



Parâmetro	Obrigatório	Tipo	Descrição
ip_addr	Não	String	Endereço IP público ou privado
protect_status	Não	String	Status de proteção. Seu valor pode ser: <ul style="list-style-type: none"><li>● closed</li><li>● opened</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
group_id	Não	String	ID do grupo de servidores
group_name	Não	String	Nome do grupo de servidores Mínimo: <b>1</b> Máximo: <b>64</b>
has_intrusion	Não	Boolean	Existem alarmes.
policy_group_id	Não	String	ID do grupo de políticas Mínimo: <b>0</b> Máximo: <b>128</b>
policy_group_name	Não	String	Nome do grupo de políticas Mínimo: <b>0</b> Máximo: <b>256</b>
charging_mode	Não	String	Modo de cobrança. Seu valor pode ser: <ul style="list-style-type: none"><li>● packet_cycle: anual/mensal</li><li>● on_demand: pagamento por uso</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
refresh	Não	Boolean	Se deve sincronizar à força servidores de ECSs
above_version	Não	Boolean	Se deve retornar todas as versões posteriores à versão atual
outside_host	Não	Boolean	Se um servidor é um servidor da Huawei Cloud

Parâmetro	Obrigatório	Tipo	Descrição
asset_value	Não	String	<p>Importância de ativo. Seu valor pode ser:</p> <ul style="list-style-type: none"> <li>● important</li> <li>● common</li> <li>● test</li> </ul> <p>Mínimo: <b>0</b> Máximo: <b>128</b></p>
label	Não	String	<p>Tag de ativo</p> <p>Mínimo: <b>1</b> Máximo: <b>64</b></p>
server_group	Não	String	<p>Grupo de servidores de ativos</p> <p>Mínimo: <b>1</b> Máximo: <b>64</b></p>
agent_upgradable	Não	Boolean	Se o agente pode ser atualizado
limit	Não	Integer	<p>Número de registros exibidos em cada página. O valor padrão é <b>10</b>.</p> <p>Mínimo: <b>0</b> Máximo: <b>200</b> Padrão: <b>10</b></p>
offset	Não	Integer	<p>Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é <b>0</b>.</p> <p>Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b></p>

## Parâmetros de solicitação

**Tabela 3-249** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de <b>X-Subject-Token</b> no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Não	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

**Código de status: 200****Tabela 3-250** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total de registros Mínimo: <b>0</b> Máximo: <b>2097152</b>
data_list	Array of <b>Host</b> objects	Consulta sobre o status e a lista do servidor de nuvem Comprimento da matriz: <b>0–10241</b>

**Tabela 3-251** Host

Parâmetro	Tipo	Descrição
host_name	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
host_id	String	ID de servidor Mínimo: <b>0</b> Máximo: <b>128</b>

Parâmetro	Tipo	Descrição
agent_id	String	ID do agente Mínimo: <b>0</b> Máximo: <b>128</b>
private_ip	String	Endereço IP privado Mínimo: <b>0</b> Máximo: <b>128</b>
public_ip	String	Endereço IP elástico Mínimo: <b>0</b> Máximo: <b>128</b>
enterprise_project_id	String	ID do projeto empresarial Mínimo: <b>0</b> Máximo: <b>256</b>
enterprise_project_name	String	Nome do projeto empresarial Mínimo: <b>0</b> Máximo: <b>256</b>
host_status	String	Status do servidor. Seu valor pode ser: <ul style="list-style-type: none"> <li>● ACTIVE</li> <li>● SHUTOFF</li> <li>● BUILDING</li> <li>● ERROR</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>
agent_status	String	Status de agente. Seu valor pode ser: <ul style="list-style-type: none"> <li>● not_installed</li> <li>● online</li> <li>● offline</li> <li>● install_failed</li> <li>● installing</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>

Parâmetro	Tipo	Descrição
install_result_code	String	<p>Resultado da instalação. Seu valor pode ser:</p> <ul style="list-style-type: none"> <li>● install_succeed</li> <li>● network_access_timeout: a conexão atingiu o tempo limite. Erro de rede.</li> <li>● invalid_port</li> <li>● auth_failed: a autenticação falhou devido à senha incorreta.</li> <li>● permission_denied: permissões insuficientes.</li> <li>● no_available_vpc: não há servidores com um agente on-line na VPC atual.</li> <li>● install_exception</li> <li>● invalid_param</li> <li>● install_failed</li> <li>● package_unavailable</li> <li>● os_type_not_support: tipo de SO incorreto</li> <li>● os_arch_not_support: arquitetura incorreta do SO</li> </ul> <p>Mínimo: <b>1</b> Máximo: <b>32</b></p>
version	String	<p>Edição do HSS. Seu valor pode ser:</p> <ul style="list-style-type: none"> <li>● hss.version.null: nenhuma</li> <li>● hss.version.basic: edição básica</li> <li>● hss.version.enterprise: edição empresarial</li> <li>● hss.version.premium: edição premium</li> <li>● hss.version.wtp: edição WTP</li> <li>● hss.version.container.enterprise: edição de container</li> </ul> <p>Mínimo: <b>1</b> Máximo: <b>32</b></p>
protect_status	String	<p>Status de proteção. Seu valor pode ser:</p> <ul style="list-style-type: none"> <li>● closed</li> <li>● opened</li> </ul> <p>Mínimo: <b>1</b> Máximo: <b>32</b></p>
os_image	String	<p>Imagem de disco do sistema</p> <p>Mínimo: <b>0</b> Máximo: <b>128</b></p>

Parâmetro	Tipo	Descrição
os_type	String	Tipo de SO. Seu valor pode ser: <ul style="list-style-type: none"><li>● Linux</li><li>● Windows</li></ul> Mínimo: <b>0</b> Máximo: <b>128</b>
os_bit	String	Versão de bit do SO Mínimo: <b>0</b> Máximo: <b>128</b>
detect_result	String	Resultado da verificação do servidor. Seu valor pode ser: <ul style="list-style-type: none"><li>● undetected</li><li>● clean</li><li>● risk</li><li>● scanning</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
expire_time	Long	Tempo de expiração da versão de teste. (O valor <b>-1</b> indica que a cota é uma versão não de teste. Se o valor não for <b>-1</b> , o valor indica o tempo de expiração da versão de teste.) Mínimo: <b>0</b> Máximo: <b>4824695185000</b>
charging_mode	String	Modo de cobrança. Seu valor pode ser: <ul style="list-style-type: none"><li>● packet_cycle: anual/mensal</li><li>● on_demand: pagamento por uso</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
resource_id	String	ID da instância do recurso do serviço de nuvem (UUID) Mínimo: <b>0</b> Máximo: <b>128</b>
outside_host	Boolean	Se um servidor não é um servidor da Huawei Cloud
group_id	String	ID do grupo de servidores Mínimo: <b>1</b> Máximo: <b>128</b>

Parâmetro	Tipo	Descrição
group_name	String	Nome do grupo de servidores Mínimo: <b>1</b> Máximo: <b>128</b>
policy_group_id	String	ID do grupo de políticas Mínimo: <b>1</b> Máximo: <b>128</b>
policy_group_name	String	Nome do grupo de políticas Mínimo: <b>1</b> Máximo: <b>128</b>
asset	Integer	Risco de ativo Mínimo: <b>0</b> Máximo: <b>2097152</b>
vulnerability	Integer	Número total de riscos de vulnerabilidade, incluindo vulnerabilidades de software Linux, vulnerabilidades de sistema Windows, vulnerabilidades de Web-CMS e vulnerabilidades de aplicações. Mínimo: <b>0</b> Máximo: <b>2097152</b>
baseline	Integer	Número total de riscos de linha de base, incluindo riscos de configuração e senhas fracas. Mínimo: <b>0</b> Máximo: <b>2097152</b>
intrusion	Integer	Riscos totais de intrusão Mínimo: <b>0</b> Máximo: <b>2097152</b>
asset_value	String	Importância de ativo. Seu valor pode ser: <ul style="list-style-type: none"> <li>● important</li> <li>● common</li> <li>● test</li> </ul> Mínimo: <b>0</b> Máximo: <b>128</b>
labels	Array of strings	Lista de tags Mínimo: <b>0</b> Máximo: <b>64</b> Comprimento da matriz: <b>0–100</b>

Parâmetro	Tipo	Descrição
agent_create_time	Long	Tempo de instalação do agente, que é um carimbo de data/hora. A unidade padrão é milissegundos. Mínimo: <b>0</b> Máximo: <b>4824695185000</b>
agent_update_time	Long	Hora em que o status do agente é alterado. Este é um carimbo de data/hora. A unidade padrão é milissegundos. Mínimo: <b>0</b> Máximo: <b>4824695185000</b>
agent_version	String	Versão do agente Mínimo: <b>1</b> Máximo: <b>32</b>
upgrade_status	String	Status de atualização. Seu valor pode ser: <ul style="list-style-type: none"><li>● not_upgrade: não atualizado. Este é o status padrão. O cliente não entregou nenhum comando de atualização ao servidor.</li><li>● upgrading: a atualização está em andamento.</li><li>● upgrade_failed: a atualização falhou.</li><li>● upgrade_succeed</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
upgrade_result_code	String	Causa da falha de atualização. Este parâmetro é exibido somente se upgrade_status for upgrade_failed. Seu valor pode ser: <ul style="list-style-type: none"><li>● package_unavailable: o pacote de atualização falha ao ser analisado porque o arquivo de atualização está incorreto.</li><li>● network_access_timeout: falha ao baixar o pacote de atualização porque a rede está anormal.</li><li>● agent_offline: o agente está off-line.</li><li>● hostguard_abnormal: o processo do agente é anormal.</li><li>● insufficient_disk_space: o espaço de disco é insuficiente.</li><li>● failed_to_replace_file: falha ao substituir o arquivo.</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
upgradable	Boolean	Se o agente do servidor pode ser atualizado



Parâmetro	Tipo	Descrição
open_time	Long	Hora em que a proteção está ativada. Este é um carimbo de data/hora. A unidade padrão é milissegundos.  Mínimo: <b>0</b> Máximo: <b>4824695185000</b>
protect_interrupt	Boolean	Se a proteção foi interrompida

## Exemplo de solicitações

Consultar os 10 servidores Linux em todos os projetos empresariais cujo status do agente esteja on-line.

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

## Exemplo de respostas

**Código de status: 200**

Lista de servidores de nuvem

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

```
"agent_update_time" : 0,  
"open_time" : 0  
} ]  
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;  
import com.huaweicloud.sdk.hss.v5.region.HssRegion;  
import com.huaweicloud.sdk.hss.v5.*;  
import com.huaweicloud.sdk.hss.v5.model.*;  
  
public class ListHostStatusSolution {  
  
    public static void main(String[] args) {  
        // The AK and SK used for authentication are hard-coded or stored in  
plaintext, which has great security risks. It is recommended that the AK and SK  
be stored in ciphertext in configuration files or environment variables and  
decrypted during use to ensure security.  
        // In this example, AK and SK are stored in environment variables for  
authentication. Before running this example, set environment variables  
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
        String ak = System.getenv("CLOUD_SDK_AK");  
        String sk = System.getenv("CLOUD_SDK_SK");  
  
        ICredential auth = new BasicCredentials()  
            .withAk(ak)  
            .withSk(sk);  
  
        HssClient client = HssClient.newBuilder()  
            .withCredential(auth)  
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))  
            .build();  
  
        ListHostStatusRequest request = new ListHostStatusRequest();  
        request.withEnterpriseProjectId("<enterprise_project_id>");  
        request.withVersion("<version>");  
        request.withAgentStatus("<agent_status>");  
        request.withDetectResult("<detect_result>");  
        request.withHostName("<host_name>");  
        request.withHostId("<host_id>");  
        request.withHostStatus("<host_status>");  
        request.withOsType("<os_type>");  
        request.withPrivateIp("<private_ip>");  
        request.withPublicIp("<public_ip>");  
        request.withIpAddr("<ip_addr>");  
        request.withProtectStatus("<protect_status>");  
        request.withGroupId("<group_id>");  
        request.withGroupName("<group_name>");  
        request.withHasIntrusion("<has_intrusion>");  
        request.withPolicyGroupId("<policy_group_id>");  
        request.withPolicyGroupName("<policy_group_name>");  
        request.withChargingMode("<charging_mode>");  
        request.withRefresh("<refresh>");  
        request.withAboveVersion("<above_version>");  
        request.withOutsideHost("<outside_host>");  
        request.withAssetValue("<asset_value>");  
        request.withLabel("<label>");  
    }  
}
```

```
request.withServerGroup("<server_group>");
request.withAgentUpgradable(<agent_upgradable>);
request.withLimit(<limit>);
request.withOffset(<offset>);
try {
    ListHostStatusResponse response = client.listHostStatus(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListHostStatusRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.version = "<version>"
        request.agent_status = "<agent_status>"
        request.detect_result = "<detect_result>"
        request.host_name = "<host_name>"
        request.host_id = "<host_id>"
        request.host_status = "<host_status>"
        request.os_type = "<os_type>"
        request.private_ip = "<private_ip>"
        request.public_ip = "<public_ip>"
        request.ip_addr = "<ip_addr>"
        request.protect_status = "<protect_status>"
        request.group_id = "<group_id>"
        request.group_name = "<group_name>"
        request.has_intrusion = <HasIntrusion>
        request.policy_group_id = "<policy_group_id>"
        request.policy_group_name = "<policy_group_name>"
        request.charging_mode = "<charging_mode>"
        request.refresh = <Refresh>
```

```
request.above_version = <AboveVersion>
request.outside_host = <OutsideHost>
request.asset_value = "<asset_value>"
request.label = "<label>"
request.server_group = "<server_group>"
request.agent_upgradable = <AgentUpgradable>
request.limit = <limit>
request.offset = <offset>
response = client.list_host_status(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ListHostStatusRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        versionRequest:= "<version>"
        request.Version = &versionRequest
        agentStatusRequest:= "<agent_status>"
        request.AgentStatus = &agentStatusRequest
        detectResultRequest:= "<detect_result>"
        request.DetectResult = &detectResultRequest
        hostNameRequest:= "<host_name>"
        request.HostName = &hostNameRequest
        hostIdRequest:= "<host_id>"
        request.HostId = &hostIdRequest
        hostStatusRequest:= "<host_status>"
        request.HostStatus = &hostStatusRequest
        osTypeRequest:= "<os_type>"
        request.OsType = &osTypeRequest
        privateIpRequest:= "<private_ip>"
        request.PrivateIp = &privateIpRequest
```

```

publicIpRequest:= "<public_ip>"
request.PublicIp = &publicIpRequest
ipAddrRequest:= "<ip_addr>"
request.IpAddr = &ipAddrRequest
protectStatusRequest:= "<protect_status>"
request.ProtectStatus = &protectStatusRequest
groupIdRequest:= "<group_id>"
request.GroupId = &groupIdRequest
groupNameRequest:= "<group_name>"
request.GroupName = &groupNameRequest
hasIntrusionRequest:= <has_intrusion>
request.HasIntrusion = &hasIntrusionRequest
policyGroupIdRequest:= "<policy_group_id>"
request.PolicyGroupId = &policyGroupIdRequest
policyGroupNameRequest:= "<policy_group_name>"
request.PolicyGroupName = &policyGroupNameRequest
chargingModeRequest:= "<charging_mode>"
request.ChargingMode = &chargingModeRequest
refreshRequest:= <refresh>
request.Refresh = &refreshRequest
aboveVersionRequest:= <above_version>
request.AboveVersion = &aboveVersionRequest
outsideHostRequest:= <outside_host>
request.OutsideHost = &outsideHostRequest
assetValueRequest:= "<asset_value>"
request.AssetValue = &assetValueRequest
labelRequest:= "<label>"
request.Label = &labelRequest
serverGroupRequest:= "<server_group>"
request.ServerGroup = &serverGroupRequest
agentUpgradableRequest:= <agent_upgradable>
request.AgentUpgradable = &agentUpgradableRequest
limitRequest:= int32(<limit>)
request.Limit = &limitRequest
offsetRequest:= int32(<offset>)
request.Offset = &offsetRequest
response, err := client.ListHostStatus(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}

```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de servidores de nuvem

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.8.2 Alteração do status de proteção

### Função

Esta API é usada para alterar o status de proteção.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

POST /v5/{project\_id}/host-management/protection

Tabela 3-252 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

Tabela 3-253 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>

## Parâmetros de solicitação

**Tabela 3-254** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-255** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
version	Sim	String	Edição do HSS. Seu valor pode ser: <ul style="list-style-type: none"><li>● hss.version.null: proteção desativada</li><li>● hss.version.basic: edição básica</li><li>● hss.version.advanced: edição profissional</li><li>● hss.version.enterprise: edição empresarial</li><li>● hss.version.premium: edição premium</li><li>● hss.version.wtp: edição WTP</li></ul> Mínimo: <b>1</b> Máximo: <b>128</b>
charging_mode	Não	String	Modo de pagamento. Esse parâmetro é obrigatório quando version não está definido como hss.version.null. <ul style="list-style-type: none"><li>● packet_cycle: anual/mensal</li><li>● on_demand: sob demanda</li></ul> Mínimo: <b>1</b> Máximo: <b>64</b>

Parâmetro	Obrigatório	Tipo	Descrição
resource_id	Não	String	ID da cota do HSS. Se esse parâmetro não for especificado, a cota da versão correspondente será selecionada aleatoriamente. Mínimo: <b>1</b> Máximo: <b>128</b>
host_id_list	Sim	Array of strings	Lista de servidores Mínimo: <b>1</b> Máximo: <b>128</b> Comprimento da matriz: <b>0–2097152</b>
tags	Não	Array of <b>TagInfo</b> objects	Lista de tags de recursos Comprimento da matriz: <b>0–2097152</b>

**Tabela 3-256** TagInfo

Parâmetro	Obrigatório	Tipo	Descrição
key	Não	String	Chave. Pode conter até 128 caracteres Unicode. O key não pode ser deixado em branco. Mínimo: <b>1</b> Máximo: <b>128</b>
value	Não	String	Valor. Cada valor de tag pode conter um máximo de 255 caracteres Unicode. Mínimo: <b>1</b> Máximo: <b>255</b>

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Alterar a edição de proteção do servidor cujo ID é 71a15ecc-049f-4cca-bd28-5e90aca1817f para a edição empresarial.

```
{  
  "version" : "hss.version.enterprise",  
  "charging_mode" : "packet_cycle",  
  "resource_id" : "af4d08ad-2b60-4916-a5cf-8d6a23956dda",  
  "host_id_list" : [ "71a15ecc-049f-4cca-bd28-5e90aca1817f" ],  
}
```



```
"tags" : [ {  
  "key" : "Service",  
  "value" : "hss"  
} ]  
}
```

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

Alterar a edição de proteção do servidor cujo ID é 71a15ecc-049f-4cca-bd28-5e90aca1817f para a edição empresarial.

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;  
import com.huaweicloud.sdk.hss.v5.region.HssRegion;  
import com.huaweicloud.sdk.hss.v5.*;  
import com.huaweicloud.sdk.hss.v5.model.*;  
  
import java.util.List;  
import java.util.ArrayList;  
  
public class SwitchHostsProtectStatusSolution {  
  
    public static void main(String[] args) {  
        // The AK and SK used for authentication are hard-coded or stored in  
        plaintext, which has great security risks. It is recommended that the AK and SK  
        be stored in ciphertext in configuration files or environment variables and  
        decrypted during use to ensure security.  
        // In this example, AK and SK are stored in environment variables for  
        authentication. Before running this example, set environment variables  
        CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
        String ak = System.getenv("CLOUD_SDK_AK");  
        String sk = System.getenv("CLOUD_SDK_SK");  
  
        ICredential auth = new BasicCredentials()  
            .withAk(ak)  
            .withSk(sk);  
  
        HssClient client = HssClient.newBuilder()  
            .withCredential(auth)  
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))  
            .build();  
        SwitchHostsProtectStatusRequest request = new  
SwitchHostsProtectStatusRequest();  
        request.withEnterpriseProjectId("<enterprise_project_id>");  
        SwitchHostsProtectStatusRequestInfo body = new  
SwitchHostsProtectStatusRequestInfo();  
        List<TagInfo> listbodyTags = new ArrayList<>();  
        listbodyTags.add(  
            new TagInfo()  
                .withKey("Service")  
                .withValue("hss")  
        );  
        List<String> listbodyHostIdList = new ArrayList<>();
```

```
listbodyHostIdList.add("71a15ecc-049f-4cca-bd28-5e90aca1817f");
body.withTags(listbodyTags);
body.withHostIdList(listbodyHostIdList);
body.withResourceId("af4d08ad-2b60-4916-a5cf-8d6a23956dda");
body.withChargingMode("packet_cycle");
body.withVersion("hss.version.enterprise");
request.withBody(body);
try {
    SwitchHostsProtectStatusResponse response =
client.switchHostsProtectStatus(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

Alterar a edição de proteção do servidor cujo ID é 71a15ecc-049f-4cca-bd28-5e90aca1817f para a edição empresarial.

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = SwitchHostsProtectStatusRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        listTagsbody = [
            TagInfo(
                key="Service",
                value="hss"
            )
        ]
        listHostIdListbody = [
            "71a15ecc-049f-4cca-bd28-5e90aca1817f"
        ]
        request.body = SwitchHostsProtectStatusRequestInfo(
            tags=listTagsbody,
```

```
        host_id_list=listHostIdListbody,
        resource_id="af4d08ad-2b60-4916-a5cf-8d6a23956dda",
        charging_mode="packet_cycle",
        version="hss.version.enterprise"
    )
    response = client.switch_hosts_protect_status(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

Alterar a edição de proteção do servidor cujo ID é 71a15ecc-049f-4cca-bd28-5e90aca1817f para a edição empresarial.

```
package main

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

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

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

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

    request := &model.SwitchHostsProtectStatusRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        keyTags:= "Service"
        valueTags:= "hss"
        var listTagsbody = []model.TagInfo{
            {
                Key: &keyTags,
                Value: &valueTags,
            },
        }
        var listHostIdListbody = []string{
            "71a15ecc-049f-4cca-bd28-5e90aca1817f",
        }
        resourceIdSwitchHostsProtectStatusRequestInfo:= "af4d08ad-2b60-4916-
a5cf-8d6a23956dda"
        chargingModeSwitchHostsProtectStatusRequestInfo:= "packet_cycle"
        request.Body = &model.SwitchHostsProtectStatusRequestInfo{
            Tags: &listTagsbody,
```

```
HostIdList: listHostIdListbody,  
ResourceId: &resourceIdSwitchHostsProtectStatusRequestInfo,  
ChargingMode: &chargingModeSwitchHostsProtectStatusRequestInfo,  
Version: "hss.version.enterprise",  
}  
response, err := client.SwitchHostsProtectStatus(request)  
if err == nil {  
    fmt.Printf("%+v\n", response)  
} else {  
    fmt.Println(err)  
}  
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Resposta bem-sucedida

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.8.3 Consulta de grupos de servidores

### Função

Essa API é usada para consultar grupos de servidores.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/host-management/groups

Tabela 3-257 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-258** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é <b>0</b> . Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
limit	Não	Integer	Número de registros exibidos em cada página. Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>
group_name	Não	String	Nome do grupo de servidores Mínimo: <b>1</b> Máximo: <b>64</b>

## Parâmetros de solicitação

**Tabela 3-259** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>

Parâmetro	Obrigatório	Tipo	Descrição
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-260** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total
data_list	Array of <b>HostGroupItem</b> objects	Lista de grupos de servidores Comprimento da matriz: <b>0–100</b>

**Tabela 3-261** HostGroupItem

Parâmetro	Tipo	Descrição
group_id	String	ID do grupo de servidores
group_name	String	Nome do grupo de servidores
host_num	Integer	Número de servidores vinculados
risk_host_num	Integer	Número de servidores inseguros
unprotect_host_num	Integer	Número de servidores desprotegidos
host_id_list	Array of strings	Lista de IDs do servidor
is_outside	Boolean	Indica se o grupo de servidores é um grupo de servidores de data center local.

## Exemplo de solicitações

Consultar o grupo de servidores cujo nome é test.

```
GET https://{endpoint}/v5/{project_id}/host-management/groups?offset=0&limit=200&enterprise_project_id=all_granted_eps&&group_name=test
```

## Exemplo de respostas

**Código de status: 200**

## Lista de grupos de servidores

```
{
  "data_list" : [ {
    "group_id" : "36e59701-e2e7-4d56-b229-0db3bcf4e6e8",
    "group_name" : "test",
    "host_id_list" : [ "71a15ecc-049f-4cca-bd28-5e90aca1817f" ],
    "host_num" : 1,
    "risk_host_num" : 1,
    "unprotect_host_num" : 0
  } ],
  "total_num" : 1
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListHostGroupsSolution {

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

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

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
            .build();
        ListHostGroupsRequest request = new ListHostGroupsRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withOffset("<offset>");
        request.withLimit("<limit>");
        request.withGroupName("<group_name>");
        try {
            ListHostGroupsResponse response = client.listHostGroups(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
        }
    }
}
```

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

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListHostGroupsRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.offset = <offset>
        request.limit = <limit>
        request.group_name = "<group_name>"
        response = client.list_host_groups(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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



```
sk := os.Getenv("CLOUD_SDK_SK")

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

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

request := &model.ListHostGroupsRequest{
    enterpriseProjectIdRequest:= "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    offsetRequest:= int32(<offset>)
    request.Offset = &offsetRequest
    limitRequest:= int32(<limit>)
    request.Limit = &limitRequest
    groupNameRequest:= "<group_name>"
    request.GroupName = &groupNameRequest
    response, err := client.ListHostGroups(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia [Código de amostra no API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de grupos de servidores

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.8.4 Criação de um grupo de servidores

### Função

Esta API é usada para criar um grupo de servidores.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

## URI

POST /v5/{project\_id}/host-management/groups

**Tabela 3-262** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-263** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>

## Parâmetros de solicitação

**Tabela 3-264** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

Parâmetro	Obrigatório	Tipo	Descrição
Content-Type	Não	String	Valor padrão: application/json; charset=utf-8 Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-265** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
group_name	Sim	String	Nome do grupo de servidores Mínimo: <b>1</b> Máximo: <b>128</b>
host_id_list	Sim	Array of strings	Lista de IDs do servidor Mínimo: <b>1</b> Máximo: <b>128</b> Comprimento da matriz: <b>1–10000</b>

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Criar um grupo de servidores chamado test. O ID do servidor no grupo de servidores é 15dac7fe-d81b-43bc-a4a7-4710fe673972.

```
POST https://{endpoint}/v5/{project_id}/host-management/groups
{
  "group_name" : "test",
  "host_id_list" : [ "15dac7fe-d81b-43bc-a4a7-4710fe673972" ]
}
```

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

Criar um grupo de servidores chamado test. O ID do servidor no grupo de servidores é 15dac7fe-d81b-43bc-a4a7-4710fe673972.

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

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

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

public class AddHostsGroupSolution {

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

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

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
            .build();
        AddHostsGroupRequest request = new AddHostsGroupRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        AddHostsGroupRequestInfo body = new AddHostsGroupRequestInfo();
        List<String> listbodyHostIdList = new ArrayList<>();
        listbodyHostIdList.add("15dac7fe-d81b-43bc-a4a7-4710fe673972");
        body.withHostIdList(listbodyHostIdList);
        body.withGroupName("test");
        request.withBody(body);
        try {
            AddHostsGroupResponse response = client.addHostsGroup(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Criar um grupo de servidores chamado test. O ID do servidor no grupo de servidores é 15dac7fe-d81b-43bc-a4a7-4710fe673972.

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = AddHostsGroupRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        listHostIdListbody = [
            "15dac7fe-d81b-43bc-a4a7-4710fe673972"
        ]
        request.body = AddHostsGroupRequestInfo(
            host_id_list=listHostIdListbody,
            group_name="test"
        )
        response = client.add_hosts_group(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Criar um grupo de servidores chamado test. O ID do servidor no grupo de servidores é 15dac7fe-d81b-43bc-a4a7-4710fe673972.

```
package main

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

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

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

    client := hss.NewHssClient(
```

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

request := &model.AddHostsGroupRequest{
    enterpriseProjectIdRequest:= "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    var listHostIdListbody = []string{
        "15dac7fe-d81b-43bc-a4a7-4710fe673972",
    }
    request.Body = &model.AddHostsGroupRequestInfo{
        HostIdList: listHostIdListbody,
        GroupName: "test",
    }
}
response, err := client.AddHostsGroup(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Bem-sucedido
400	Parâmetro inválido.
401	Falha na autenticação.
403	Permissão insuficiente.
404	Recurso não encontrado.
500	Erro de sistema.

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.8.5 Edição de um grupo de servidores

### Função

Esta API é usada para editar um grupo de servidores.

## Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

## URI

PUT /v5/{project\_id}/host-management/groups

Tabela 3-266 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

Tabela 3-267 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>

## Parâmetros de solicitação

Tabela 3-268 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

Parâmetro	Obrigatório	Tipo	Descrição
Content-Type	Não	String	Valor padrão: application/json; charset=utf-8 Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-269** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
group_name	Não	String	Nome do grupo de servidores
group_id	Sim	String	ID do grupo de servidores
host_id_list	Não	Array of strings	Lista de IDs do servidor

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Editar o grupo de servidores chamado test. O ID do grupo de servidores é eca40dbe-27f7-4229-8f9d-a58213129fdc. Os IDs dos servidores no grupo de servidores são 15dac7fe-d81b-43bc-a4a7-4710fe673972 e 21303c5b-36ad-4510-a1b0-cb4ac4c2875c.

```
PUT https://{endpoint}/v5/{project_id}/host-management/groups
{
  "group_id" : "eca40dbe-27f7-4229-8f9d-a58213129fdc",
  "group_name" : "test",
  "host_id_list" : [ "15dac7fe-d81b-43bc-a4a7-4710fe673972", "21303c5b-36ad-4510-a1b0-cb4ac4c2875c" ]
}
```

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

Editar o grupo de servidores chamado test. O ID do grupo de servidores é eca40dbe-27f7-4229-8f9d-a58213129fdc. Os IDs dos servidores no grupo de servidores são 15dac7fe-d81b-43bc-a4a7-4710fe673972 e 21303c5b-36ad-4510-a1b0-cb4ac4c2875c.

```
package com.huaweicloud.sdk.test;
import com.huaweicloud.sdk.core.auth.ICredential;
```



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

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

public class ChangeHostsGroupSolution {

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

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

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

        ChangeHostsGroupRequest request = new ChangeHostsGroupRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        ChangeHostsGroupRequestInfo body = new ChangeHostsGroupRequestInfo();
        List<String> listbodyHostIdList = new ArrayList<>();
        listbodyHostIdList.add("15dac7fe-d81b-43bc-a4a7-4710fe673972");
        listbodyHostIdList.add("21303c5b-36ad-4510-alb0-cb4ac4c2875c");
        body.withHostIdList(listbodyHostIdList);
        body.withGroupId("eca40dbe-27f7-4229-8f9d-a58213129fdc");
        body.withGroupName("test");
        request.withBody(body);
        try {
            ChangeHostsGroupResponse response = client.changeHostsGroup(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Editar o grupo de servidores chamado test. O ID do grupo de servidores é eca40dbe-27f7-4229-8f9d-a58213129fdc. Os IDs dos servidores no grupo de servidores são 15dac7fe-d81b-43bc-a4a7-4710fe673972 e 21303c5b-36ad-4510-alb0-cb4ac4c2875c.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
```

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ChangeHostsGroupRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        listHostIdListbody = [
            "15dac7fe-d81b-43bc-a4a7-4710fe673972",
            "21303c5b-36ad-4510-a1b0-cb4ac4c2875c"
        ]
        request.body = ChangeHostsGroupRequestInfo(
            host_id_list=listHostIdListbody,
            group_id="eca40dbe-27f7-4229-8f9d-a58213129fdc",
            group_name="test"
        )
        response = client.change_hosts_group(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Editar o grupo de servidores chamado test. O ID do grupo de servidores é eca40dbe-27f7-4229-8f9d-a58213129fdc. Os IDs dos servidores no grupo de servidores são 15dac7fe-d81b-43bc-a4a7-4710fe673972 e 21303c5b-36ad-4510-a1b0-cb4ac4c2875c.

```
package main

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

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

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

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

request := &model.ChangeHostsGroupRequest{}
enterpriseProjectIdRequest := "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
var listHostIdListbody = []string{
    "15dac7fe-d81b-43bc-a4a7-4710fe673972",
    "21303c5b-36ad-4510-a1b0-cb4ac4c2875c",
}
groupNameChangeHostsGroupRequestInfo := "test"
request.Body = &model.ChangeHostsGroupRequestInfo{
    HostIdList: &listHostIdListbody,
    GroupId: "eca40dbe-27f7-4229-8f9d-a58213129fdc",
    GroupName: &groupNameChangeHostsGroupRequestInfo,
}
response, err := client.ChangeHostsGroup(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Bem-sucedido
400	Parâmetro inválido.
401	Falha na autenticação.
403	Permissão insuficiente.
404	Recurso não encontrado.
500	Erro de sistema.

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.8.6 Exclusão de um grupo de servidores

### Função

Esta API é usada para excluir um grupo de servidores.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

DELETE /v5/{project\_id}/host-management/groups

Tabela 3-270 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

Tabela 3-271 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>
group_id	Sim	String	ID do grupo de servidores

## Parâmetros de solicitação

Tabela 3-272 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Excluir o grupo de servidores cujo ID é 34fcf861-402b-45c6-9b6a-13087791aae3.

```
DELETE https://{endpoint}/v5/{project_id}/host-management/groups
{
  "group_id" : "34fcf861-402b-45c6-9b6a-13087791aae3"
}
```

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

Excluir o grupo de servidores cujo ID é 34fcf861-402b-45c6-9b6a-13087791aae3.

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

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

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

public class DeleteHostsGroupSolution {

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

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

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

        DeleteHostsGroupRequest request = new DeleteHostsGroupRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withGroupId("<group_id>");
        try {
            DeleteHostsGroupResponse response = client.deleteHostsGroup(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Excluir o grupo de servidores cujo ID é 34fcf861-402b-45c6-9b6a-13087791aae3.

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

    client = HssClient.new_builder() \
```

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

try:
    request = DeleteHostsGroupRequest()
    request.enterprise_project_id = "<enterprise_project_id>"
    request.group_id = "<group_id>"
    response = client.delete_hosts_group(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

Excluir o grupo de servidores cujo ID é 34fcf861-402b-45c6-9b6a-13087791aae3.

```
package main

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

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

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

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

    request := &model.DeleteHostsGroupRequest{}
    enterpriseProjectIdRequest := "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    request.GroupId = "<group_id>"
    response, err := client.DeleteHostsGroup(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Bem-sucedido
400	Parâmetro inválido.
401	Falha na autenticação.
403	Permissão insuficiente.
404	Recurso não encontrado.
500	Erro de sistema.

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.9 Imagem do container

### 3.9.1 Consulta da lista de imagens no repositório de imagens do SWR

#### Função

Essa API é usada para consultar a lista de imagens no repositório de imagens do SWR. Para sincronizar as imagens mais recentes do SWR, chame a API para sincronizar imagens do SWR primeiro.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/image/swr-repository



**Tabela 3-273** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-274** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como all_granted_eps. Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>
namespace	Não	String	Nome da organização Mínimo: <b>1</b> Máximo: <b>256</b>
image_name	Não	String	ID do nome da imagem Mínimo: <b>1</b> Máximo: <b>128</b>
image_version	Não	String	Tag da imagem Mínimo: <b>1</b> Máximo: <b>64</b>
latest_version	Não	Boolean	Exibir apenas as versões de imagem mais recentes Padrão: <b>false</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é 0. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>

Parâmetro	Obrigatório	Tipo	Descrição
limit	Não	Integer	Número de registros exibidos em cada página. Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>
image_type	Sim	String	Tipo de imagem. As opções são as seguintes: <ul style="list-style-type: none"><li>● private_image: repositório privado de imagens</li><li>● shared_image: repositório de imagens compartilhado</li><li>● local_image</li><li>● instance_image: imagem empresarial</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
scan_status	Não	String	Status da verificação. As opções são as seguintes: <ul style="list-style-type: none"><li>● unscan</li><li>● success</li><li>● scanning</li><li>● failed</li><li>● waiting_for_scan</li></ul> Mínimo: <b>0</b> Máximo: <b>32</b>
instance_name	Não	String	Nome da instância de imagem empresarial Mínimo: <b>0</b> Máximo: <b>128</b>
image_size	Não	Long	Tamanho da imagem Mínimo: <b>0</b> Máximo: <b>2147483547</b> Padrão: <b>0</b>
start_latest_update_time	Não	Long	Hora de início da criação (ms). Mínimo: <b>0</b> Máximo: <b>4070880000000</b> Padrão: <b>0</b>

Parâmetro	Obrigatório	Tipo	Descrição
end_latest_update_time	Não	Long	Hora de término da criação (ms). Mínimo: <b>0</b> Máximo: <b>4070880000000</b> Padrão: <b>0</b>
start_latest_scan_time	Não	Long	A hora de início da última conclusão da verificação, em ms. Mínimo: <b>0</b> Máximo: <b>4070880000000</b> Padrão: <b>0</b>
end_latest_scan_time	Não	Long	A hora de término da última conclusão da verificação, em ms. Mínimo: <b>0</b> Máximo: <b>4070880000000</b> Padrão: <b>0</b>
has_malicious_file	Não	Boolean	Se existem arquivos maliciosos
has_unsafe_setting	Não	Boolean	Se a verificação de linha de base existe
has_vul	Não	Boolean	Se existem vulnerabilidades de software
instance_id	Não	String	ID da instância do repositório empresarial. Esta API não é necessária para a edição compartilhada do SWR. Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de solicitação

**Tabela 3-275** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

**Código de status: 200****Tabela 3-276** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total Mínimo: <b>0</b> Máximo: <b>2147483547</b>
data_list	Array of <a href="#">PrivateImageRepositoryInfo</a> objects	Consulta da lista de imagens no repositório de imagens do SWR Comprimento da matriz: <b>0–200</b>

**Tabela 3-277** PrivateImageRepositoryInfo

Parâmetro	Tipo	Descrição
id	Long	ID Mínimo: <b>0</b> Máximo: <b>2147483547</b>
namespace	String	Namespace Mínimo: <b>0</b> Máximo: <b>64</b>

Parâmetro	Tipo	Descrição
image_name	String	Nome da imagem Mínimo: <b>0</b> Máximo: <b>128</b>
image_id	String	ID da imagem Mínimo: <b>0</b> Máximo: <b>64</b>
image_digest	String	Resumo da imagem Mínimo: <b>0</b> Máximo: <b>128</b>
image_version	String	Tag da imagem Mínimo: <b>0</b> Máximo: <b>64</b>
image_type	String	Tipo de imagem. As opções são as seguintes: <ul style="list-style-type: none"><li>● private_image</li><li>● shared_image</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>
latest_version	Boolean	Verificar se a versão é a mais recente.
scan_status	String	Status da verificação. As opções são as seguintes: <ul style="list-style-type: none"><li>● unscan</li><li>● success</li><li>● scanning</li><li>● failed</li><li>● download_failed</li><li>● image_oversized</li><li>● waiting_for_scan</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>

Parâmetro	Tipo	Descrição
scan_failed_desc	String	<p>Causa da falha de verificação. As opções são as seguintes:</p> <ul style="list-style-type: none"> <li>● "unknown_error"</li> <li>● "authentication_failed"</li> <li>● "download_failed": falha ao fazer o download da imagem.</li> <li>● "image_over_sized": o tamanho da imagem excede o máximo.</li> <li>● "image_oversized"</li> <li>● "failed_to_scan_vulnerability"</li> <li>● "failed_to_scan_file"</li> <li>● "failed_to_scan_software"</li> <li>● "failed_to_check_sensitive_information"</li> <li>● "failed_to_check_baseline"</li> <li>● "failed_to_check_software_compliance"</li> <li>● "failed_to_query_basic_image_information"</li> <li>● "response_timed_out"</li> <li>● "database_error"</li> <li>● "failed_to_send_the_scan_request"</li> </ul> <p>Mínimo: <b>0</b> Máximo: <b>64</b></p>
image_size	Long	<p>Tamanho da imagem</p> <p>Mínimo: <b>0</b> Máximo: <b>2147483547</b></p>
latest_update_time	Long	<p>Hora da última atualização da versão da imagem, em ms.</p> <p>Mínimo: <b>0</b> Máximo: <b>407088000000</b></p>
latest_scan_time	Long	<p>Última verificação, em ms.</p> <p>Mínimo: <b>0</b> Máximo: <b>407088000000</b></p>
vul_num	Integer	<p>Vulnerabilidades</p> <p>Mínimo: <b>0</b> Máximo: <b>2147483647</b></p>
unsafe_setting_num	Integer	<p>Número de verificações de linha de base com falha</p> <p>Mínimo: <b>0</b> Máximo: <b>2147483647</b></p>

Parâmetro	Tipo	Descrição
malicious_file_num	Integer	Número de arquivos maliciosos Mínimo: <b>0</b> Máximo: <b>2147483647</b>
domain_name	String	Proprietário (parâmetro de imagem compartilhada) Mínimo: <b>0</b> Máximo: <b>128</b>
shared_status	String	O status de uma imagem compartilhada. O valor pode ser: <ul style="list-style-type: none"><li>● expired</li><li>● effective</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
scannable	Boolean	Digitalizável ou não
instance_name	String	Nome da instância da imagem da edição empresarial Mínimo: <b>0</b> Máximo: <b>128</b>
instance_id	String	ID de instância da imagem da edição empresarial Mínimo: <b>0</b> Máximo: <b>64</b>
instance_url	String	URL de instância da imagem da edição empresarial Mínimo: <b>0</b> Máximo: <b>256</b>
association_images	Array of <a href="#">AssociateImages</a> objects	Informações de imagem vinculadas a várias arquiteturas Comprimento da matriz: <b>0–200</b>

**Tabela 3-278** AssociateImages

Parâmetro	Tipo	Descrição
image_name	String	Nome da imagem Mínimo: <b>0</b> Máximo: <b>128</b>
image_version	String	Tag da imagem Mínimo: <b>0</b> Máximo: <b>64</b>

Parâmetro	Tipo	Descrição
image_type	String	Tipo de imagem Mínimo: <b>0</b> Máximo: <b>64</b>
namespace	String	Namespace Mínimo: <b>0</b> Máximo: <b>64</b>
image_digest	String	Resumo da imagem Mínimo: <b>0</b> Máximo: <b>128</b>
scan_status	String	Status da verificação. As opções são as seguintes: <ul style="list-style-type: none"><li>● unscan</li><li>● success</li><li>● scanning</li><li>● failed</li><li>● download_failed</li><li>● image_oversized</li><li>● waiting_for_scan</li></ul> Mínimo: <b>0</b> Máximo: <b>32</b>

## Exemplo de solicitações

Consultar a lista de imagens no repositório de imagens do SWR cujo tipo de imagem é imagem privada.

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

## Exemplo de respostas

### Código de status: 200

Essa API é usada para consultar a lista de imagens no repositório de imagens do SWR, incluindo a lista de imagens privadas e a lista de imagens compartilhadas (controladas pelo parâmetro de entrada image\_type).

```
{
  "total_num" : 3,
  "data_list" : [ {
    "id" : "111 (example for private images)",
    "image_digest" : "sha256:cebcdacde18091448a5040dc55bb1a9f6540b093db8XXXXXX",
    "image_id" : "cebcdacde18091448a5040dc55bb1a9f6540b093db8XXXXXX",
    "image_name" : "centos7",
    "image_size" : "1000 (Bytes)",
    "image_type" : "private_image",
```



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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListSwrImageRepositorySolution {

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

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

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

        ListSwrImageRepositoryRequest request = new
ListSwrImageRepositoryRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withNamespace("<namespace>");
        request.withImageName("<image_name>");
        request.withImageVersion("<image_version>");
        request.withLatestVersion(<latest_version>);
        request.withOffset(<offset>);
        request.withLimit(<limit>);
        request.withImageType("<image_type>");
        request.withScanStatus("<scan_status>");
        request.withInstanceName("<instance_name>");
        request.withImageSize(<image_size>L);
        request.withStartLatestUpdateTime(<start_latest_update_time>L);
        request.withEndLatestUpdateTime(<end_latest_update_time>L);
        request.withStartLatestScanTime(<start_latest_scan_time>L);
        request.withEndLatestScanTime(<end_latest_scan_time>L);
        request.withHasMaliciousFile(<has_malicious_file>);
        request.withHasUnsafeSetting(<has_unsafe_setting>);
        request.withHasVul(<has_vul>);
        request.withInstanceId("<instance_id>");
        try {
            ListSwrImageRepositoryResponse response =
client.listSwrImageRepository(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.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 huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListSwrImageRepositoryRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.namespace = "<namespace>"
        request.image_name = "<image_name>"
        request.image_version = "<image_version>"
        request.latest_version = <LatestVersion>
        request.offset = <offset>
        request.limit = <limit>
        request.image_type = "<image_type>"
        request.scan_status = "<scan_status>"
        request.instance_name = "<instance_name>"
        request.image_size = <image_size>
        request.start_latest_update_time = <start_latest_update_time>
        request.end_latest_update_time = <end_latest_update_time>
        request.start_latest_scan_time = <start_latest_scan_time>
        request.end_latest_scan_time = <end_latest_scan_time>
        request.has_malicious_file = <HasMaliciousFile>
        request.has_unsafe_setting = <HasUnsafeSetting>
        request.has_vul = <HasVul>
        request.instance_id = "<instance_id>"
        response = client.list_swr_image_repository(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

func main() {
```

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

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

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

request := &model.ListSwrImageRepositoryRequest{
    enterpriseProjectIdRequest:= "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    namespaceRequest:= "<namespace>"
    request.Namespace = &namespaceRequest
    imageNameRequest:= "<image_name>"
    request.ImageName = &imageNameRequest
    imageVersionRequest:= "<image_version>"
    request.ImageVersion = &imageVersionRequest
    latestVersionRequest:= <latest_version>
    request.LatestVersion = &latestVersionRequest
    offsetRequest:= int32(<offset>)
    request.Offset = &offsetRequest
    limitRequest:= int32(<limit>)
    request.Limit = &limitRequest
    request.ImageType = "<image_type>"
    scanStatusRequest:= "<scan_status>"
    request.ScanStatus = &scanStatusRequest
    instanceNameRequest:= "<instance_name>"
    request.InstanceName = &instanceNameRequest
    imageSizeRequest:= int64(<image_size>)
    request.ImageSize = &imageSizeRequest
    startLatestUpdateTimeRequest:= int64(<start_latest_update_time>)
    request.StartLatestUpdateTime = &startLatestUpdateTimeRequest
    endLatestUpdateTimeRequest:= int64(<end_latest_update_time>)
    request.EndLatestUpdateTime = &endLatestUpdateTimeRequest
    startLatestScanTimeRequest:= int64(<start_latest_scan_time>)
    request.StartLatestScanTime = &startLatestScanTimeRequest
    endLatestScanTimeRequest:= int64(<end_latest_scan_time>)
    request.EndLatestScanTime = &endLatestScanTimeRequest
    hasMaliciousFileRequest:= <has_malicious_file>
    request.HasMaliciousFile = &hasMaliciousFileRequest
    hasUnsafeSettingRequest:= <has_unsafe_setting>
    request.HasUnsafeSetting = &hasUnsafeSettingRequest
    hasVulRequest:= <has_vul>
    request.HasVul = &hasVulRequest
    instanceIdRequest:= "<instance_id>"
    request.InstanceId = &instanceIdRequest
    response, err := client.ListSwrImageRepository(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Essa API é usada para consultar a lista de imagens no repositório de imagens do SWR, incluindo a lista de imagens privadas e a lista de imagens compartilhadas (controladas pelo parâmetro de entrada <code>image_type</code> ).

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.9.2 Verificação de imagens no repositório de imagens em lotes

### Função

Essa API é usada para verificar imagens no repositório de imagens em lotes.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

POST /v5/{project\_id}/image/batch-scan

Tabela 3-279 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-280** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como all_granted_eps. Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>

## Parâmetros de solicitação

**Tabela 3-281** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-282** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
repo_type	Não	String	Tipo de repositório. Atualmente, os repositórios de imagens de SWR estão conectados. As opções são as seguintes: <ul style="list-style-type: none"><li>● SWR: repositório de imagens do SWR</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>

Parâmetro	Obrigatório	Tipo	Descrição
image_info_list	Não	Array of <b>BatchScanSwr ImageInfo</b> objects	Especifica a lista de imagens a serem verificadas. Este parâmetro é obrigatório quando operate_all é false. Comprimento da matriz: <b>0–10241</b>
operate_all	Não	Boolean	Se esse parâmetro for definido como true, todos os critérios de filtro poderão ser usados para consulta completa. Se image_info_list estiver vazio, este parâmetro será obrigatório.
namespace	Não	String	Nome da organização Mínimo: <b>1</b> Máximo: <b>256</b>
image_name	Não	String	Nome da imagem Mínimo: <b>1</b> Máximo: <b>256</b>
image_version	Não	String	Tag da imagem Mínimo: <b>1</b> Máximo: <b>256</b>
image_type	Sim	String	Tipo de imagem. As opções são as seguintes: <ul style="list-style-type: none"><li>● private_image: repositório privado de imagens</li><li>● shared_image: repositório de imagens compartilhado</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
scan_status	Não	String	Status da verificação. As opções são as seguintes: <ul style="list-style-type: none"><li>● unscan</li><li>● success</li><li>● scanning</li><li>● failed</li><li>● download_failed</li><li>● image_oversized</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
latest_version	Não	Boolean	Exibir apenas as versões de imagem mais recentes

Parâmetro	Obrigatório	Tipo	Descrição
image_size	Não	Long	Tamanho da imagem Mínimo: <b>0</b> Máximo: <b>2147483547</b> Padrão: <b>0</b>
start_latest_update_time	Não	Long	Data de início da criação, em ms. Mínimo: <b>0</b> Máximo: <b>2147483547</b> Padrão: <b>0</b>
end_latest_update_time	Não	Long	Data de término da criação, em ms. Mínimo: <b>0</b> Máximo: <b>2147483547</b> Padrão: <b>0</b>
start_latest_scan_time	Não	Long	A hora de início da última conclusão da verificação, em ms. Mínimo: <b>0</b> Máximo: <b>2147483547</b> Padrão: <b>0</b>
end_latest_scan_time	Não	Long	A hora de término da última conclusão da verificação, em ms. Mínimo: <b>0</b> Máximo: <b>2147483547</b> Padrão: <b>0</b>

Tabela 3-283 BatchScanSwrImageInfo

Parâmetro	Obrigatório	Tipo	Descrição
namespace	Não	String	Namespace Mínimo: <b>1</b> Máximo: <b>64</b>
image_name	Não	String	Nome da imagem Mínimo: <b>1</b> Máximo: <b>128</b>
image_version	Não	String	Tag da imagem Mínimo: <b>1</b> Máximo: <b>128</b>



Parâmetro	Obrigatório	Tipo	Descrição
instance_id	Não	String	ID da instância empresarial Mínimo: <b>1</b> Máximo: <b>128</b>
instance_url	Não	String	Baixar o URL da imagem empresarial Mínimo: <b>0</b> Máximo: <b>256</b>

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

- Verificar imagens privadas em lotes. O corpo da solicitação transfere a lista de imagens e o `operate_all` não contém nenhum parâmetro, indicando que a lista de imagens precisa ser verificada em lotes.

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

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

- Realizar uma verificação completa para imagens privadas. O corpo da solicitação não transfere a lista de imagens e `operate_all` é definido como `true`, indicando que a lista de imagens precisa ser totalmente verificada.

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

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

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

- Verificar imagens privadas em lotes. O corpo da solicitação transfere a lista de imagens e o `operate_all` não contém nenhum parâmetro, indicando que a lista de imagens precisa ser verificada em lotes.

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

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

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

public class BatchScanSwrImageSolution {

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

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

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

        BatchScanSwrImageRequest request = new BatchScanSwrImageRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        BatchScanPrivateImageRequestInfo body = new
        BatchScanPrivateImageRequestInfo();
        List<BatchScanSwrImageInfo> listbodyImageInfoList = new ArrayList<>();
        listbodyImageInfoList.add(
            new BatchScanSwrImageInfo()
                .withNamespace("test")
                .withImageName("openjdk")
                .withImageVersion("v8.8")
        );
        listbodyImageInfoList.add(
            new BatchScanSwrImageInfo()
                .withNamespace("test1")
                .withImageName("openjdk1")
                .withImageVersion("v1.0")
        );
        body.withImageType("private_image");
        body.withImageInfoList(listbodyImageInfoList);
        request.withBody(body);
        try {
            BatchScanSwrImageResponse response =
            client.batchScanSwrImage(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());
    }
}
}
```

- Realizar uma verificação completa para imagens privadas. O corpo da solicitação não transfere a lista de imagens e `operate_all` é definido como `true`, indicando que a lista de imagens precisa ser totalmente verificada.

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

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

public class BatchScanSwrImageSolution {

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

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

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

        BatchScanSwrImageRequest request = new BatchScanSwrImageRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        BatchScanPrivateImageRequestInfo body = new
BatchScanPrivateImageRequestInfo();
        body.withImageType("private_image");
        body.withOperateAll(true);
        request.withBody(body);
        try {
            BatchScanSwrImageResponse response =
client.batchScanSwrImage(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

- Verificar imagens privadas em lotes. O corpo da solicitação transfere a lista de imagens e o `operate_all` não contém nenhum parâmetro, indicando que a lista de imagens precisa ser verificada em lotes.

```
# coding: utf-8  
  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudsdkhss.v5.region.hss_region import HssRegion  
from huaweicloudsdkcore.exceptions import exceptions  
from huaweicloudsdkhss.v5 import *  
  
if __name__ == "__main__":  
    # The AK and SK used for authentication are hard-coded or stored in  
    # plaintext, which has great security risks. It is recommended that the AK and  
    # SK be stored in ciphertext in configuration files or environment variables  
    # and decrypted during use to ensure security.  
    # In this example, AK and SK are stored in environment variables for  
    # authentication. Before running this example, set environment variables  
    # CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak = __import__('os').getenv("CLOUD_SDK_AK")  
    sk = __import__('os').getenv("CLOUD_SDK_SK")  
  
    credentials = BasicCredentials(ak, sk) \  
  
    client = HssClient.new_builder() \  
        .with_credentials(credentials) \  
        .with_region(HssRegion.value_of("<YOUR REGION>")) \  
        .build()  
  
    try:  
        request = BatchScanSvrImageRequest()  
        request.enterprise_project_id = "<enterprise_project_id>"  
        listImageInfoListbody = [  
            BatchScanSvrImageInfo(  
                namespace="test",  
                image_name="openjdk",  
                image_version="v8.8"  
            ),  
            BatchScanSvrImageInfo(  
                namespace="test1",  
                image_name="openjdk1",  
                image_version="v1.0"  
            )  
        ]  
        request.body = BatchScanPrivateImageRequestInfo(  
            image_type="private_image",  
            image_info_list=listImageInfoListbody  
        )  
        response = client.batch_scan_svr_image(request)  
        print(response)  
    except exceptions.ClientRequestException as e:  
        print(e.status_code)  
        print(e.request_id)  
        print(e.error_code)  
        print(e.error_msg)
```

- Realizar uma verificação completa para imagens privadas. O corpo da solicitação não transfere a lista de imagens e `operate_all` é definido como `true`, indicando que a lista de imagens precisa ser totalmente verificada.

```
# coding: utf-8  
  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
```

```
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = BatchScanSwrImageRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.body = BatchScanPrivateImageRequestInfo(
            image_type="private_image",
            operate_all=True
        )
        response = client.batch_scan_swr_image(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

- Verificar imagens privadas em lotes. O corpo da solicitação transfere a lista de imagens e o `operate_all` não contém nenhum parâmetro, indicando que a lista de imagens precisa ser verificada em lotes.

```
package main

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

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

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

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

request := &model.BatchScanSwrImageRequest{}
enterpriseProjectIdRequest:= "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
namespaceImageInfoList:= "test"
imageNameImageInfoList:= "openjdk"
imageVersionImageInfoList:= "v8.8"
namespaceImageInfoList1:= "test1"
imageNameImageInfoList1:= "openjdk1"
imageVersionImageInfoList1:= "v1.0"
var listImageInfoListbody = []model.BatchScanSwrImageInfo{
    {
        Namespace: &namespaceImageInfoList,
        ImageName: &imageNameImageInfoList,
        ImageVersion: &imageVersionImageInfoList,
    },
    {
        Namespace: &namespaceImageInfoList1,
        ImageName: &imageNameImageInfoList1,
        ImageVersion: &imageVersionImageInfoList1,
    },
}
request.Body = &model.BatchScanPrivateImageRequestInfo{
    ImageType: "private_image",
    ImageInfoList: &listImageInfoListbody,
}
response, err := client.BatchScanSwrImage(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

- Realizar uma verificação completa para imagens privadas. O corpo da solicitação não transfere a lista de imagens e `operate_all` é definido como `true`, indicando que a lista de imagens precisa ser totalmente verificada.

```
package main

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

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

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

```
client := hss.NewHssClient(  
    hss.HssClientBuilder().  
        WithRegion(region.ValueOf("<YOUR REGION>")).  
        WithCredential(auth).  
        Build())  
  
request := &model.BatchScanSwrImageRequest{  
    enterpriseProjectIdRequest:= "<enterprise_project_id>"  
    request.EnterpriseProjectId = &enterpriseProjectIdRequest  
    operateAllBatchScanPrivateImageRequestInfo:= true  
    request.Body = &model.BatchScanPrivateImageRequestInfo{  
        ImageType: "private_image",  
        OperateAll: &operateAllBatchScanPrivateImageRequestInfo,  
    }  
}  
response, err := client.BatchScanSwrImage(request)  
if err == nil {  
    fmt.Printf("%+v\n", response)  
} else {  
    fmt.Println(err)  
}  
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Resposta bem-sucedida

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.9.3 Consulta de informações de vulnerabilidade de imagem

### Função

Essa API é usada para consultar informações de vulnerabilidade de imagem.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/image/{image\_id}/vulnerabilities

Tabela 3-284 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: <b>1</b> Máximo: <b>256</b>
image_id	Sim	String	ID da imagem Mínimo: <b>0</b> Máximo: <b>128</b>

Tabela 3-285 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como all_granted_eps. Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>
image_type	Sim	String	Tipo de imagem. As opções são as seguintes: <ul style="list-style-type: none"><li>● private_image: repositório privado de imagens</li><li>● shared_image: repositório de imagens compartilhado</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é <b>0</b> . Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
limit	Não	Integer	Número de registros exibidos em cada página. Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>



Parâmetro	Obrigatório	Tipo	Descrição
instance_id	Não	String	ID da instância do repositório empresarial. Esta API não é necessária para a edição compartilhada do SWR. Mínimo: <b>0</b> Máximo: <b>128</b>
namespace	Sim	String	Nome da organização Mínimo: <b>0</b> Máximo: <b>64</b>
image_name	Sim	String	Nome da imagem Mínimo: <b>0</b> Máximo: <b>128</b>
tag_name	Sim	String	Tag da imagem Mínimo: <b>0</b> Máximo: <b>64</b>
repair_necessity	Não	String	Nível de risco. As opções são as seguintes: <ul style="list-style-type: none"><li>● immediate_repair: alto risco</li><li>● delay_repair: risco médio</li><li>● not_needed_repair: baixo risco</li></ul> Mínimo: <b>0</b> Máximo: <b>32</b>
vul_id	Não	String	ID da vulnerabilidade (pesquisa difusa suportada) Mínimo: <b>0</b> Máximo: <b>64</b>
app_name	Não	String	Software Mínimo: <b>0</b> Máximo: <b>64</b>
type	Não	String	Tipo de vulnerabilidade. As opções são as seguintes: - linux_vul: vulnerabilidade do Linux -app_vul: vulnerabilidade da aplicação Mínimo: <b>0</b> Máximo: <b>32</b>

## Parâmetros de solicitação

**Tabela 3-286** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

**Código de status: 200****Tabela 3-287** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total de vulnerabilidades de imagem Mínimo: <b>0</b> Máximo: <b>2147483547</b>
data_list	Array of <b>ImageVulInfo</b> objects	Lista de vulnerabilidades de imagem Comprimento da matriz: <b>0–10241</b>

**Tabela 3-288** ImageVulInfo

Parâmetro	Tipo	Descrição
vul_id	String	ID de vulnerabilidade Mínimo: <b>0</b> Máximo: <b>128</b>

Parâmetro	Tipo	Descrição
repair_necessity	String	Nível de emergência. Seus valores e seus significados são os seguintes: <ul style="list-style-type: none"><li>● immediate_repair: alto risco</li><li>● delay_repair: risco médio</li><li>● not_needed_repair: baixo risco</li></ul> Mínimo: <b>0</b> Máximo: <b>128</b>
description	String	Descrição da vulnerabilidade Mínimo: <b>0</b> Máximo: <b>128</b>
position	String	Imagem em que existe uma vulnerabilidade Mínimo: <b>0</b> Máximo: <b>128</b>
app_name	String	Nome do software da vulnerabilidade Mínimo: <b>0</b> Máximo: <b>128</b>
app_path	String	Caminho do software de aplicação (este campo está disponível apenas para vulnerabilidades de aplicação). Mínimo: <b>1</b> Máximo: <b>512</b>
version	String	Versão do software Mínimo: <b>0</b> Máximo: <b>128</b>
solution	String	Solução Mínimo: <b>0</b> Máximo: <b>256</b>
url	String	Endereço do patch Mínimo: <b>0</b> Máximo: <b>128</b>

## Exemplo de solicitações

Consultar as informações de vulnerabilidade da imagem privada cujo namespace é scc\_hss\_container, o nome da imagem é apttest e a versão da imagem é V1.

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

## Exemplo de respostas

### Código de status: 200

Lista de vulnerabilidades de imagem

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListImageVulnerabilitiesSolution {

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

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

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
            .build();
        ListImageVulnerabilitiesRequest request = new
        ListImageVulnerabilitiesRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withImageType("<image_type>");
        request.withOffset(<offset>);
        request.withLimit(<limit>);
        request.withInstanceId("<instance_id>");
        request.withNamespace("<namespace>");
    }
}
```

```
request.withImageName("<image_name>");
request.withTagName("<tag_name>");
request.withRepairNecessity("<repair_necessity>");
request.withVulId("<vul_id>");
request.withAppName("<app_name>");
request.withType("<type>");
try {
    ListImageVulnerabilitiesResponse response =
client.listImageVulnerabilities(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.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 huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListImageVulnerabilitiesRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.image_type = "<image_type>"
        request.offset = <offset>
        request.limit = <limit>
        request.instance_id = "<instance_id>"
        request.namespace = "<namespace>"
        request.image_name = "<image_name>"
        request.tag_name = "<tag_name>"
        request.repair_necessity = "<repair_necessity>"
        request.vul_id = "<vul_id>"
        request.app_name = "<app_name>"
        request.type = "<type>"
        response = client.list_image_vulnerabilities(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
```

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

## Go

```
package main

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

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

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

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

    request := &model.ListImageVulnerabilitiesRequest{}
    enterpriseProjectIdRequest := "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    request.ImageType = "<image_type>"
    offsetRequest := int32(<offset>)
    request.Offset = &offsetRequest
    limitRequest := int32(<limit>)
    request.Limit = &limitRequest
    instanceIdRequest := "<instance_id>"
    request.InstanceId = &instanceIdRequest
    request.Namespace = "<namespace>"
    request.ImageName = "<image_name>"
    request.TagName = "<tag_name>"
    repairNecessityRequest := "<repair_necessity>"
    request.RepairNecessity = &repairNecessityRequest
    vulIdRequest := "<vul_id>"
    request.VulId = &vulIdRequest
    appNameRequest := "<app_name>"
    request.AppName = &appNameRequest
    typeRequest := "<type>"
    request.Type = &typeRequest
    response, err := client.ListImageVulnerabilities(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de vulnerabilidades de imagem

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.9.4 Informações de CVE correspondentes à vulnerabilidade

### Função

Essa API é usada para consultar as informações de CVE correspondentes à vulnerabilidade.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/image/vulnerability/{vul\_id}/cve

Tabela 3-289 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: <b>1</b> Máximo: <b>256</b>
vul_id	Sim	String	ID de vulnerabilidade Mínimo: <b>0</b> Máximo: <b>64</b>

Tabela 3-290 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como all_granted_eps. Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é 0. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
limit	Não	Integer	Número de registros exibidos em cada página. Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>

## Parâmetros de solicitação

Tabela 3-291 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>



## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-292** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total Mínimo: <b>0</b> Máximo: <b>2147483547</b>
data_list	Array of <b>ImageVulCveInfo</b> objects	Lista Comprimento da matriz: <b>1–10000</b>

**Tabela 3-293** ImageVulCveInfo

Parâmetro	Tipo	Descrição
cve_id	String	ID de CVE Mínimo: <b>0</b> Máximo: <b>32</b>
cvss_score	Float	Pontuação de CVSS Mínimo: <b>0</b> Máximo: <b>100</b>
publish_time	Long	Data de lançamento, em ms. Mínimo: <b>0</b> Máximo: <b>2147483547</b>
description	String	Descrição de CVE Mínimo: <b>0</b> Máximo: <b>65534</b>

## Exemplo de solicitações

Consultar as informações de CVE da vulnerabilidade cujo ID é vul\_id.

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

## Exemplo de respostas

**Código de status: 200**

Sucesso ao solicitar a lista de informações de CVE correspondente à vulnerabilidade.

```
{
  "total_num" : 1,
```

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListVulnerabilityCveRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.offset = <offset>
        request.limit = <limit>
        response = client.list_vulnerability_cve(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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

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

    client := hss.NewHssClient(
```

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

request := &model.ListVulnerabilityCveRequest{
    enterpriseProjectIdRequest:= "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    offsetRequest:= int32(<offset>)
    request.Offset = &offsetRequest
    limitRequest:= int32(<limit>)
    request.Limit = &limitRequest
}
response, err := client.ListVulnerabilityCve(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Sucesso ao solicitar a lista de informações de CVE correspondente à vulnerabilidade.

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.9.5 Sincronização da lista de imagens do SWR

### Função

Essa API é usada para sincronizar a lista de imagens do SWR.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

POST /v5/{project\_id}/image/synchronize

**Tabela 3-294** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-295** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como all_granted_eps. Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>

## Parâmetros de solicitação

**Tabela 3-296** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-297** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
image_type	Sim	String	Tipo de imagem. As opções são as seguintes: <ul style="list-style-type: none"><li>● private_image: repositório privado de imagens</li><li>● shared_image: repositório de imagens compartilhado</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-298** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
error_code	Integer	Código de erro Mínimo: <b>0</b> Máximo: <b>10</b>
error_description	String	Descrição do erro Mínimo: <b>1</b> Máximo: <b>128</b>

## Exemplo de solicitações

Sincronizar imagens privadas ou compartilhadas do SWR.

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

## Exemplo de respostas

**Código de status: 200**

Solicitação bem-sucedida.

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

Sincronizar imagens privadas ou compartilhadas do SWR.

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

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

public class RunImageSynchronizeSolution {

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

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

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

        RunImageSynchronizeRequest request = new RunImageSynchronizeRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        RunImageSynchronizeRequestInfo body = new
RunImageSynchronizeRequestInfo();
        body.withImageType("private_image");
        request.withBody(body);
        try {
            RunImageSynchronizeResponse response =
client.runImageSynchronize(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

### Python

Sincronizar imagens privadas ou compartilhadas do SWR.

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = RunImageSynchronizeRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.body = RunImageSynchronizeRequestInfo(
            image_type="private_image"
        )
        response = client.run_image_synchronize(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

### Sincronizar imagens privadas ou compartilhadas do SWR.

```
package main

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

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

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



```
client := hss.NewHssClient(  
    hss.HssClientBuilder().  
        WithRegion(region.ValueOf("<YOUR REGION>")).  
        WithCredential(auth).  
        Build())  
  
request := &model.RunImageSynchronizeRequest{  
    enterpriseProjectIdRequest:= "<enterprise_project_id>"  
    request.EnterpriseProjectId = &enterpriseProjectIdRequest  
    request.Body = &model.RunImageSynchronizeRequestInfo{  
        ImageType: "private_image",  
    }  
}  
response, err := client.RunImageSynchronize(request)  
if err == nil {  
    fmt.Printf("%+v\n", response)  
} else {  
    fmt.Println(err)  
}  
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Solicitação bem-sucedida.

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.9.6 Consulta da lista de resultados de detecção de configuração de segurança de imagem

### Função

Essa API é usada para consultar a lista de resultados de detecção de configuração de segurança de imagem.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/image/baseline/risk-configs

**Tabela 3-299** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-300** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como all_granted_eps. Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>
image_type	Sim	String	Tipo de imagem. As opções são as seguintes: <ul style="list-style-type: none"> <li>● private_image: repositório privado de imagens</li> <li>● shared_image: repositório de imagens compartilhado</li> <li>● local_image: imagem local</li> <li>● instance_image: imagem empresarial</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é 0. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
limit	Não	Integer	Número de registros exibidos em cada página. Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>

Parâmetro	Obrigatório	Tipo	Descrição
namespace	Não	String	Nome da organização Mínimo: <b>0</b> Máximo: <b>64</b>
image_name	Não	String	Nome da imagem Mínimo: <b>0</b> Máximo: <b>128</b>
image_version	Não	String	Nome da tag de imagem Mínimo: <b>0</b> Máximo: <b>64</b>
check_name	Não	String	Nome da linha de base Mínimo: <b>0</b> Máximo: <b>256</b>
severity	Não	String	Nível de risco. Seu valor pode ser: <ul style="list-style-type: none"><li>● Security</li><li>● Low</li><li>● Medium</li><li>● High</li></ul> Mínimo: <b>0</b> Máximo: <b>32</b>
standard	Não	String	Tipo padrão. Seu valor pode ser: <ul style="list-style-type: none"><li>● cn_standard: padrão de conformidade DJCP MLPS</li><li>● hw_standard: padrão da Huawei</li><li>● qt_standard: padrão de Qingteng</li></ul> Mínimo: <b>0</b> Máximo: <b>256</b>
instance_id	Não	String	ID da instância do repositório empresarial. Esta API não é necessária para a edição compartilhada do SWR. Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de solicitação

Tabela 3-301 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

Código de status: **200**

Tabela 3-302 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total Mínimo: <b>0</b> Máximo: <b>2147483647</b>
data_list	Array of <b>ImageRiskConfInfoResponseInfo</b> objects	Configurar a lista de detecção Comprimento da matriz: <b>0–2147483647</b>

**Tabela 3-303** ImageRiskConfigsInfoResponseInfo

Parâmetro	Tipo	Descrição
severity	String	Nível de risco. Seu valor pode ser: <ul style="list-style-type: none"><li>● Security</li><li>● Low</li><li>● Medium</li><li>● High</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
check_name	String	Nome da linha de base Mínimo: <b>0</b> Máximo: <b>256</b>
check_type	String	Tipo de linha de base Mínimo: <b>0</b> Máximo: <b>256</b>
standard	String	Tipo padrão. Seu valor pode ser: <ul style="list-style-type: none"><li>● cn_standard: padrão de conformidade DJCP MLPS</li><li>● hw_standard: padrão da Huawei</li><li>● qt_standard: padrão de Qingteng</li></ul> Mínimo: <b>1</b> Máximo: <b>16</b>
check_rule_num	Integer	Número de itens de verificação Mínimo: <b>0</b> Máximo: <b>2097152</b>
failed_rule_num	Integer	Número de itens de risco Mínimo: <b>0</b> Máximo: <b>2097152</b>
check_type_desc	String	Descrição da linha de base Mínimo: <b>0</b> Máximo: <b>65534</b>

## Exemplo de solicitações

Consultar a lista de resultados de configuração de segurança da imagem privada cujo namespace é scc\_hss\_container, o nome da imagem é euleros e a versão da imagem é 2.2.

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

## Exemplo de respostas

### Código de status: 200

Essa API é usada para consultar a lista de resultados de configuração de imagem.

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListImageRiskConfigsSolution {

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

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

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

        ListImageRiskConfigsRequest request = new ListImageRiskConfigsRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withImageType("<image_type>");
        request.withOffset(<offset>);
        request.withLimit(<limit>);
        request.withNamespace("<namespace>");
        request.withImageName("<image_name>");
        request.withImageVersion("<image_version>");
        request.withCheckName("<check_name>");
    }
}
```

```
request.withSeverity("<severity>");
request.withStandard("<standard>");
request.withInstanceId("<instance_id>");
try {
    ListImageRiskConfigsResponse response =
client.listImageRiskConfigs(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListImageRiskConfigsRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.image_type = "<image_type>"
        request.offset = <offset>
        request.limit = <limit>
        request.namespace = "<namespace>"
        request.image_name = "<image_name>"
        request.image_version = "<image_version>"
        request.check_name = "<check_name>"
        request.severity = "<severity>"
        request.standard = "<standard>"
        request.instance_id = "<instance_id>"
        response = client.list_image_risk_configs(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ListImageRiskConfigsRequest{}
    enterpriseProjectIdRequest := "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    request.ImageType = "<image_type>"
    offsetRequest := int32(<offset>)
    request.Offset = &offsetRequest
    limitRequest := int32(<limit>)
    request.Limit = &limitRequest
    namespaceRequest := "<namespace>"
    request.Namespace = &namespaceRequest
    imageNameRequest := "<image_name>"
    request.ImageName = &imageNameRequest
    imageVersionRequest := "<image_version>"
    request.ImageVersion = &imageVersionRequest
    checkNameRequest := "<check_name>"
    request.CheckName = &checkNameRequest
    severityRequest := "<severity>"
    request.Severity = &severityRequest
    standardRequest := "<standard>"
    request.Standard = &standardRequest
    instanceIdRequest := "<instance_id>"
    request.InstanceId = &instanceIdRequest
    response, err := client.ListImageRiskConfigs(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```



## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Essa API é usada para consultar a lista de resultados de configuração de imagem.

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.9.7 Consulta da lista de itens de verificação de um item de configuração de segurança especificado de uma imagem

#### Função

Essa API é usada para consultar a lista de itens de verificação de um item de configuração de segurança especificado de uma imagem.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/image/baseline/risk-configs/{check\_name}/rules

**Tabela 3-304** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>
check_name	Sim	String	Nome da linha de base Mínimo: <b>0</b> Máximo: <b>128</b>

Tabela 3-305 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>
image_type	Sim	String	Tipo de imagem. As opções são as seguintes: <ul style="list-style-type: none"><li>● private_image: repositório privado de imagens</li><li>● shared_image: repositório de imagens compartilhado</li><li>● local_image: imagem local</li><li>● instance_image: imagem empresarial</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é <b>0</b> . Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
limit	Não	Integer	Número de registros exibidos em cada página. Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>
namespace	Não	String	Especifica o nome da organização. Se nenhuma informação de imagem estiver disponível, todas as imagens serão consultadas. Mínimo: <b>0</b> Máximo: <b>64</b>
image_name	Não	String	Nome da imagem Mínimo: <b>0</b> Máximo: <b>128</b>

Parâmetro	Obrigatório	Tipo	Descrição
image_version	Não	String	Nome da tag de imagem Mínimo: <b>0</b> Máximo: <b>64</b>
standard	Sim	String	Tipo padrão. Seu valor pode ser: <ul style="list-style-type: none"> <li>● cn_standard: padrão de conformidade DJCP MLPS</li> <li>● hw_standard: padrão da Huawei</li> <li>● qt_standard: padrão de Qingteng</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>
result_type	Não	String	Tipo de resultado. Seu valor pode ser: <ul style="list-style-type: none"> <li>● pass: o item passou na verificação.</li> <li>● failed: o item falhou na verificação.</li> </ul> Padrão: <b>unhandled</b> Mínimo: <b>0</b> Máximo: <b>64</b>
check_rule_name	Não	String	Nome do item de verificação. A correspondência difusa é suportada. Mínimo: <b>0</b> Máximo: <b>2048</b>
severity	Não	String	Nível de risco. Seu valor pode ser: <ul style="list-style-type: none"> <li>● Security</li> <li>● Low</li> <li>● Medium</li> <li>● High</li> <li>● Critical</li> </ul> Mínimo: <b>0</b> Máximo: <b>255</b>
instance_id	Não	String	ID da instância do repositório empresarial. Esta API não é necessária para a edição compartilhada do SWR. Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de solicitação

Tabela 3-306 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

Código de status: **200**

Tabela 3-307 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Riscos totais Mínimo: <b>0</b> Máximo: <b>2147483647</b>
data_list	Array of <b>ImageRiskConfigsCheckRulesResponseInfo</b> objects	Lista de dados Comprimento da matriz: <b>0–2147483647</b>

**Tabela 3-308** ImageRiskConfigsCheckRulesResponseInfo

Parâmetro	Tipo	Descrição
severity	String	Nível de risco. Seu valor pode ser: <ul style="list-style-type: none"><li>● Security</li><li>● Low</li><li>● Medium</li><li>● High</li></ul> Mínimo: <b>0</b> Máximo: <b>255</b>
check_name	String	Nome da linha de base Mínimo: <b>0</b> Máximo: <b>256</b>
check_type	String	Tipo de linha de base Mínimo: <b>0</b> Máximo: <b>256</b>
standard	String	Tipo padrão. Seu valor pode ser: <ul style="list-style-type: none"><li>● cn_standard: padrão de conformidade DJCP MLPS</li><li>● hw_standard: padrão da Huawei</li><li>● qt_standard: padrão de Qingteng</li></ul> Mínimo: <b>0</b> Máximo: <b>16</b>
check_rule_name	String	Itens de verificação Mínimo: <b>0</b> Máximo: <b>2048</b>
check_rule_id	String	ID do item de verificação Mínimo: <b>0</b> Máximo: <b>64</b>
scan_result	String	Resultado da detecção. As opções são as seguintes: <ul style="list-style-type: none"><li>● pass</li><li>● failed</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>

## Exemplo de solicitações

Consultar os itens de verificação de um item de configuração de segurança especificado cuja organização é aaa, o nome da imagem é centos7, a versão da imagem é common e o tipo padrão é o padrão da Huawei.

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

## Exemplo de respostas

### Código de status: 200

Lista de verificação do item de configuração de segurança especificado

```
{
  "total_num" : 1,
  "data_list" : [ {
    "check_rule_id" : "1.1",
    "check_rule_name" : "Rule: Password locking policy.",
    "check_name" : "CentOS 7",
    "check_type" : "CentOS 7",
    "standard" : "hw_standard",
    "scan_result" : "failed",
    "severity" : "High"
  } ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListImageRiskConfigRulesSolution {

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

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

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
            .build();
        ListImageRiskConfigRulesRequest request = new
ListImageRiskConfigRulesRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
```

```
request.withImageType("<image_type>");
request.withOffset(<offset>);
request.withLimit(<limit>);
request.withNamespace("<namespace>");
request.withImageName("<image_name>");
request.withImageVersion("<image_version>");
request.withStandard("<standard>");
request.withResultType("<result_type>");
request.withCheckRuleName("<check_rule_name>");
request.withSeverity("<severity>");
request.withInstanceId("<instance_id>");
try {
    ListImageRiskConfigRulesResponse response =
client.listImageRiskConfigRules(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListImageRiskConfigRulesRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.image_type = "<image_type>"
        request.offset = <offset>
        request.limit = <limit>
        request.namespace = "<namespace>"
        request.image_name = "<image_name>"
        request.image_version = "<image_version>"
        request.standard = "<standard>"
        request.result_type = "<result_type>"
        request.check_rule_name = "<check_rule_name>"
        request.severity = "<severity>"
```

```
request.instance_id = "<instance_id>"
response = client.list_image_risk_config_rules(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ListImageRiskConfigRulesRequest{}
    enterpriseProjectIdRequest := "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    request.ImageType = "<image_type>"
    offsetRequest := int32(<offset>)
    request.Offset = &offsetRequest
    limitRequest := int32(<limit>)
    request.Limit = &limitRequest
    namespaceRequest := "<namespace>"
    request.Namespace = &namespaceRequest
    imageNameRequest := "<image_name>"
    request.ImageName = &imageNameRequest
    imageVersionRequest := "<image_version>"
    request.ImageVersion = &imageVersionRequest
    request.Standard = "<standard>"
    resultTypeRequest := "<result_type>"
    request.ResultType = &resultTypeRequest
    checkRuleNameRequest := "<check_rule_name>"
    request.CheckRuleName = &checkRuleNameRequest
    severityRequest := "<severity>"
    request.Severity = &severityRequest
    instanceIdRequest := "<instance_id>"
    request.InstanceId = &instanceIdRequest
    response, err := client.ListImageRiskConfigRules(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    }
}
```



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

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de verificação do item de configuração de segurança especificado

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.9.8 Consulta do relatório de verificação de configuração de espelho

### Função

Essa API é usada para consultar o relatório de verificação de configuração de espelho.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/image/baseline/check-rule/detail

**Tabela 3-309** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: <b>1</b> Máximo: <b>256</b>

Tabela 3-310 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como all_granted_eps. Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>
image_type	Sim	String	Tipo de imagem. As opções são as seguintes: <ul style="list-style-type: none"><li>● private_image: repositório privado de imagens</li><li>● shared_image: repositório de imagens compartilhado</li><li>● local_image: imagem local</li><li>● instance_image: imagem empresarial</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>
namespace	Não	String	Especifica o nome da organização. Se nenhuma informação de imagem estiver disponível, todas as imagens serão consultadas. Mínimo: <b>0</b> Máximo: <b>64</b>
image_name	Não	String	Nome da imagem Mínimo: <b>0</b> Máximo: <b>128</b>
image_version	Não	String	Nome da tag de imagem Mínimo: <b>0</b> Máximo: <b>64</b>
check_name	Sim	String	Nome da linha de base Mínimo: <b>0</b> Máximo: <b>255</b>
check_type	Sim	String	Tipo de linha de base Mínimo: <b>0</b> Máximo: <b>255</b>

Parâmetro	Obrigatório	Tipo	Descrição
check_rule_id	Sim	String	ID do item de verificação Mínimo: <b>0</b> Máximo: <b>255</b>
standard	Sim	String	Tipo padrão. Seu valor pode ser: <ul style="list-style-type: none"><li>● cn_standard: padrão de conformidade DJCP MLPS</li><li>● hw_standard: padrão da Huawei</li><li>● qt_standard: padrão de Qingteng</li></ul> Mínimo: <b>0</b> Máximo: <b>32</b>
instance_id	Não	String	ID da instância do repositório empresarial. Esta API não é necessária para a edição compartilhada do SWR. Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de solicitação

**Tabela 3-311** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-312** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
description	String	Descrição do item de verificação Mínimo: <b>0</b> Máximo: <b>2048</b>
reference	String	Referência Mínimo: <b>0</b> Máximo: <b>255</b>
audit	String	Descrição da auditoria Mínimo: <b>0</b> Máximo: <b>65534</b>
remediation	String	Sugestão Mínimo: <b>0</b> Máximo: <b>65534</b>
check_info_list	Array of <a href="#">ImageCheckRuleCheckCaseResponseInfo</a> objects	Caso de teste Comprimento da matriz: <b>0–2147483647</b>

**Tabela 3-313** ImageCheckRuleCheckCaseResponseInfo

Parâmetro	Tipo	Descrição
check_description	String	Descrição do caso de teste Mínimo: <b>0</b> Máximo: <b>65534</b>
current_value	String	Resultado atual Mínimo: <b>0</b> Máximo: <b>65534</b>
suggest_value	String	Resultado esperado Mínimo: <b>0</b> Máximo: <b>65534</b>

## Exemplo de solicitações

Consultar o relatório de verificação do item de configuração cuja organização é aaa, o nome da imagem é centos7, a versão da imagem é comum, o nome da linha de base é SSH, o ID do item de verificação é 1.12 e o tipo padrão é padrão da Huawei.

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

## Exemplo de respostas

### Código de status: 200

O relatório de verificação de itens de verificação de configuração é retornado.

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ShowImageCheckRuleDetailSolution {

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

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

```
        .withSk(sk);

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

        ShowImageCheckRuleDetailRequest request = new
ShowImageCheckRuleDetailRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withImageType("<image_type>");
        request.withNamespace("<namespace>");
        request.withImageName("<image_name>");
        request.withImageVersion("<image_version>");
        request.withCheckName("<check_name>");
        request.withCheckType("<check_type>");
        request.withCheckRuleId("<check_rule_id>");
        request.withStandard("<standard>");
        request.withInstanceId("<instance_id>");
        try {
            ShowImageCheckRuleDetailResponse response =
client.showImageCheckRuleDetail(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ShowImageCheckRuleDetailRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.image_type = "<image_type>"
        request.namespace = "<namespace>"
        request.image_name = "<image_name>"
```

```
request.image_version = "<image_version>"
request.check_name = "<check_name>"
request.check_type = "<check_type>"
request.check_rule_id = "<check_rule_id>"
request.standard = "<standard>"
request.instance_id = "<instance_id>"
response = client.show_image_check_rule_detail(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ShowImageCheckRuleDetailRequest{}
    enterpriseProjectIdRequest := "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    request.ImageType = "<image_type>"
    namespaceRequest := "<namespace>"
    request.Namespace = &namespaceRequest
    imageNameRequest := "<image_name>"
    request.ImageName = &imageNameRequest
    imageVersionRequest := "<image_version>"
    request.ImageVersion = &imageVersionRequest
    request.CheckName = "<check_name>"
    request.CheckType = "<check_type>"
    request.CheckRuleId = "<check_rule_id>"
    request.Standard = "<standard>"
    instanceIdRequest := "<instance_id>"
    request.InstanceId = &instanceIdRequest
    response, err := client.ShowImageCheckRuleDetail(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

```
}  
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	O relatório de verificação de itens de verificação de configuração é retornado.

## Códigos de erro

Consulte [Códigos de erro](#).

# 3.10 Gerenciamento de políticas

## 3.10.1 Consulta da lista de grupos de políticas

### Função

Essa API é usada para consultar a lista de grupos de políticas.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/policy/groups

Tabela 3-314 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>



Tabela 3-315 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>
group_name	Não	String	Nome do grupo de políticas Mínimo: <b>1</b> Máximo: <b>256</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é <b>0</b> . Mínimo: <b>0</b> Máximo: <b>100000</b> Padrão: <b>0</b>
limit	Não	Integer	Número de registros exibidos em cada página. Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>
container_mode	Não	Boolean	Se deve consultar a política de edição do container.

## Parâmetros de solicitação

Tabela 3-316 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>

Parâmetro	Obrigatório	Tipo	Descrição
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de resposta

Código de status: **200**

Tabela 3-317 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total
data_list	Array of <b>PolicyGroupResponseInfo</b> objects	Lista de grupos de políticas Comprimento da matriz: <b>0–100</b>

Tabela 3-318 PolicyGroupResponseInfo

Parâmetro	Tipo	Descrição
group_name	String	Nome do grupo de políticas
group_id	String	ID do grupo de políticas
description	String	Descrição do grupo de políticas Mínimo: <b>1</b> Máximo: <b>64</b>
deletable	Boolean	Se um grupo de políticas pode ser excluído
host_num	Integer	Número de servidores vinculados
default_group	Boolean	Se um grupo de políticas é o grupo de políticas padrão
support_os	String	SO suportado. As opções são as seguintes: <ul style="list-style-type: none"><li>● Linux</li><li>● Windows: o SO Windows é suportado.</li></ul>

Parâmetro	Tipo	Descrição
support_version	String	<p>Versões suportadas. As opções são as seguintes:</p> <ul style="list-style-type: none"> <li>● hss.version.basic: grupo de políticas da edição básica</li> <li>● hss.version.advanced: grupo de políticas da edição profissional</li> <li>● hss.version.enterprise: grupo de políticas da edição empresarial</li> <li>● hss.version.premium: grupo de políticas da edição premium</li> <li>● hss.version.wtp: grupo de políticas da edição WTP</li> <li>● hss.version.container.enterprise: grupo de políticas da edição de container</li> </ul>

## Exemplo de solicitações

Consultar a lista de grupos de políticas de todos os projetos empresariais.

```
GET https://{endpoint}/v5/{project_id}/policy/groups?
offset=0&limit=100&enterprise_project_id=all_granted_eps
```

## Exemplo de respostas

**Código de status: 200**

Lista de grupos de políticas

```
{
  "data_list" : [ {
    "default_group" : true,
    "deletable" : false,
    "description" : "container policy group for linux",
    "group_id" : "c831f177-226d-4b91-be0f-bcf98d04ef5d",
    "group_name" : "tenant_linux_container_default_policy_group ",
    "host_num" : 0,
    "support_version" : "hss.version.container.enterprise",
    "support_os" : "Linux"
  }, {
    "default_group" : true,
    "deletable" : false,
    "description" : "enterprise policy group for windows",
    "group_id" : "1ff54b90-1b3e-42a9-alda-9883a83385ce",
    "group_name" : "tenant_windows_enterprise_default_policy_group ",
    "host_num" : 0,
    "support_version" : "hss.version.enterprise",
    "support_os" : "Windows"
  }, {
    "default_group" : true,
    "deletable" : false,
    "description" : "enterprise policy group for linux",
    "group_id" : "1069bcc0-c806-4ccd-a35d-f1f7456805e9",
    "group_name" : "tenant_linux_enterprise_default_policy_group ",
    "host_num" : 1,
    "support_version" : "hss.version.enterprise",
    "support_os" : "Linux"
  }, {
```

```
    "default_group" : true,
    "deletable" : false,
    "description" : "premium policy group for windows",
    "group_id" : "11216d24-9e91-4a05-9212-c4c1d646ee79",
    "group_name" : "tenant_windows_premium_default_policy_group ",
    "host_num" : 0,
    "support_version" : "hss.version.premium",
    "support_os" : "Linux"
  }, {
    "default_group" : true,
    "deletable" : false,
    "description" : "premium policy group for linux",
    "group_id" : "e6e1228a-7bb4-424f-a42b-755162234da7",
    "group_name" : "tenant_linux_premium_default_policy_group ",
    "host_num" : 0,
    "support_version" : "hss.version.premium",
    "support_os" : "Windows"
  } ],
  "total_num" : 5
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListPolicyGroupSolution {

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

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

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
            .build();
        ListPolicyGroupRequest request = new ListPolicyGroupRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withGroupName("<group_name>");
        request.withOffset(<offset>);
        request.withLimit(<limit>);
        request.withContainerMode(<container_mode>);
        try {
            ListPolicyGroupResponse response = client.listPolicyGroup(request);
```

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

## Python

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = ListPolicyGroupRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.group_name = "<group_name>"
        request.offset = <offset>
        request.limit = <limit>
        request.container_mode = <ContainerMode>
        response = client.list_policy_group(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

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

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

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

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

    request := &model.ListPolicyGroupRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        groupNameRequest:= "<group_name>"
        request.GroupName = &groupNameRequest
        offsetRequest:= int32(<offset>)
        request.Offset = &offsetRequest
        limitRequest:= int32(<limit>)
        request.Limit = &limitRequest
        containerModeRequest:= <container_mode>
        request.ContainerMode = &containerModeRequest
    }
    response, err := client.ListPolicyGroup(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de grupos de políticas

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.10.2 Aplicação de um grupo de políticas

### Função

Esta API é usada para aplicar um grupo de políticas.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

POST /v5/{project\_id}/policy/deploy

**Tabela 3-319** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-320** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>1</b> Máximo: <b>256</b>

## Parâmetros de solicitação

**Tabela 3-321** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>128</b>
Content-Type	Não	String	Valor padrão: application/json; charset=utf-8 Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-322** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
target_policy_group_id	Sim	String	ID do grupo de políticas a ser implementado Mínimo: <b>36</b> Máximo: <b>64</b>
operate_all	Não	Boolean	Se a política deve ser implementada em todos os hosts. Se o valor for true, não será necessário configurar host_id_list. Se o valor for false, configure host_id_list.
host_id_list	Não	Array of strings	Lista de IDs de servidores onde o grupo de políticas precisa ser implementado Mínimo: <b>1</b> Máximo: <b>128</b> Comprimento da matriz: <b>0-10000</b>



## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Implementar uma política de proteção de servidor. O ID do servidor de destino é 15462c0e-32c6-4217-a869-bbd131a00ecf, e o ID da política de destino é f671f7-2677-4705-a320-de1a62bff306.

```
POST https://{endpoint}/v5/{project_id}/policy/deploy
{
  "target_policy_group_id" : "1df671f7-2677-4705-a320-de1a62bff306",
  "host_id_list" : [ "15462c0e-32c6-4217-a869-bbd131a00ecf" ],
  "operate_all" : false
}
```

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

Implementar uma política de proteção de servidor. O ID do servidor de destino é 15462c0e-32c6-4217-a869-bbd131a00ecf, e o ID da política de destino é f671f7-2677-4705-a320-de1a62bff306.

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

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

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

public class AssociatePolicyGroupSolution {

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

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

```
HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();
AssociatePolicyGroupRequest request = new AssociatePolicyGroupRequest();
request.withEnterpriseProjectId("<enterprise_project_id>");
AssociatePolicyGroupRequestInfo body = new
AssociatePolicyGroupRequestInfo();
List<String> listbodyHostIdList = new ArrayList<>();
listbodyHostIdList.add("15462c0e-32c6-4217-a869-bbd131a00ecf");
body.withHostIdList(listbodyHostIdList);
body.withOperateAll(false);
body.withTargetPolicyGroupId("1df671f7-2677-4705-a320-de1a62bff306");
request.withBody(body);
try {
    AssociatePolicyGroupResponse response =
client.associatePolicyGroup(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

Implementar uma política de proteção de servidor. O ID do servidor de destino é 15462c0e-32c6-4217-a869-bbd131a00ecf, e o ID da política de destino é f671f7-2677-4705-a320-de1a62bff306.

```
# coding: utf-8

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

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

    credentials = BasicCredentials(ak, sk) \

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

    try:
        request = AssociatePolicyGroupRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        listHostIdListbody = [
            "15462c0e-32c6-4217-a869-bbd131a00ecf"
```

```
]
request.body = AssociatePolicyGroupRequestInfo(
    host_id_list=listHostIdListbody,
    operate_all=False,
    target_policy_group_id="1df671f7-2677-4705-a320-de1a62bff306"
)
response = client.associate_policy_group(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

Implementar uma política de proteção de servidor. O ID do servidor de destino é 15462c0e-32c6-4217-a869-bbd131a00ecf, e o ID da política de destino é f671f7-2677-4705-a320-de1a62bff306.

```
package main

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

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

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

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

    request := &model.AssociatePolicyGroupRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        var listHostIdListbody = []string{
            "15462c0e-32c6-4217-a869-bbd131a00ecf",
        }
        operateAllAssociatePolicyGroupRequestInfo:= false
        request.Body = &model.AssociatePolicyGroupRequestInfo{
            HostIdList: &listHostIdListbody,
            OperateAll: &operateAllAssociatePolicyGroupRequestInfo,
            TargetPolicyGroupId: "1df671f7-2677-4705-a320-de1a62bff306",
        }
        response, err := client.AssociatePolicyGroup(request)
        if err == nil {
            fmt.Printf("%+v\n", response)
        } else {
```

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

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Bem-sucedido
400	Parâmetro inválido.
401	Falha na autenticação.
403	Permissão insuficiente.
404	Recurso não encontrado.
500	Erro de sistema.

## Códigos de erro

Consulte [Códigos de erro](#).

# 3.11 Gerenciamento de vulnerabilidades

## 3.11.1 Consulta da lista de vulnerabilidades

### Função

Essa API é usada para consultar a lista de vulnerabilidades detectadas.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/vulnerability/vulnerabilities

**Tabela 3-323** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-324** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. O valor <b>0</b> indica o projeto empresarial padrão. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>0</b> Máximo: <b>256</b>
type	Não	String	Tipo de vulnerabilidade. As opções são as seguintes: - linux_vul: vulnerabilidade do Linux -windows_vul: vulnerabilidade do Windows -web_cms: vulnerabilidade de Web-CMS -app_vul: vulnerabilidade de aplicação Mínimo: <b>0</b> Máximo: <b>32</b>
vul_id	Não	String	ID de vulnerabilidade Mínimo: <b>0</b> Máximo: <b>256</b>
vul_name	Não	String	Nome de vulnerabilidade Mínimo: <b>0</b> Máximo: <b>256</b>
limit	Não	Integer	Número de registros exibidos em cada página Mínimo: <b>0</b> Máximo: <b>200</b> Padrão: <b>10</b>

Parâmetro	Obrigatório	Tipo	Descrição
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é <b>0</b> . Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
repair_priority	Não	String	Prioridade de correção: Critical, High, Medium, Low Mínimo: <b>1</b> Máximo: <b>10</b>
handle_status	Não	String	Status de manipulação. As opções são as seguintes: -unhandled - handled Padrão: <b>unhandled</b> Mínimo: <b>1</b> Máximo: <b>32</b>
cve_id	Não	String	ID de vulnerabilidade Mínimo: <b>0</b> Máximo: <b>32</b>
label_list	Não	String	Tag de vulnerabilidade Mínimo: <b>0</b> Máximo: <b>128</b>
status	Não	String	Status da vulnerabilidade Mínimo: <b>0</b> Máximo: <b>32</b>
asset_value	Não	String	Importância do ativo: important, common, test Mínimo: <b>0</b> Máximo: <b>32</b>
group_name	Não	String	Nome do grupo de servidores Mínimo: <b>0</b> Máximo: <b>256</b>

## Parâmetros de solicitação

**Tabela 3-325** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de <b>X-Subject-Token</b> no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>

## Parâmetros de resposta

**Código de status: 200****Tabela 3-326** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Long	Número total de vulnerabilidades de software Mínimo: <b>0</b> Máximo: <b>2147483647</b>
data_list	Array of <b>VulInfo</b> objects	Lista de vulnerabilidades de software Comprimento da matriz: <b>0–2147483647</b>

**Tabela 3-327** VulInfo

Parâmetro	Tipo	Descrição
vul_name	String	Nome de vulnerabilidade Mínimo: <b>0</b> Máximo: <b>256</b>
vul_id	String	ID de vulnerabilidade Mínimo: <b>0</b> Máximo: <b>64</b>
label_list	Array of strings	Tag de vulnerabilidade Mínimo: <b>0</b> Máximo: <b>65534</b> Comprimento da matriz: <b>0–2147483647</b>

Parâmetro	Tipo	Descrição
repair_necessity	String	<p>Necessidade de reparo</p> <ul style="list-style-type: none"><li>● Critical: a pontuação de CVSS da vulnerabilidade é maior ou igual a 9, correspondendo ao nível de alto risco no console.</li><li>● High: a pontuação de CVSS da vulnerabilidade é maior ou igual a 7 e menor que 9, correspondendo ao nível de risco médio no console.</li><li>● Medium: a pontuação de CVSS da vulnerabilidade é maior ou igual a 4 e menor que 7, correspondendo ao nível de risco médio no console.</li><li>● Low: a pontuação de CVSS da vulnerabilidade é menor que 4, correspondendo ao nível de risco baixo no console.</li></ul> <p>Mínimo: <b>0</b> Máximo: <b>64</b></p>
severity_level	String	<p>Gravidade</p> <ul style="list-style-type: none"><li>● Critical: a pontuação de CVSS da vulnerabilidade é maior ou igual a 9, correspondendo ao nível de alto risco no console.</li><li>● High: a pontuação de CVSS da vulnerabilidade é maior ou igual a 7 e menor que 9, correspondendo ao nível de risco médio no console.</li><li>● Medium: a pontuação de CVSS da vulnerabilidade é maior ou igual a 4 e menor que 7, correspondendo ao nível de risco médio no console.</li><li>● Low: a pontuação de CVSS da vulnerabilidade é menor que 4, correspondendo ao nível de risco baixo no console.</li></ul> <p>Mínimo: <b>0</b> Máximo: <b>64</b></p>
host_num	Integer	<p>Número de servidores afetados</p> <p>Mínimo: <b>0</b> Máximo: <b>2147483647</b></p>
unhandle_host_num	Integer	<p>Número de servidores não processados, excluindo servidores ignorados e corrigidos</p> <p>Mínimo: <b>0</b> Máximo: <b>2147483647</b></p>
scan_time	Long	<p>Última verificação, em ms.</p> <p>Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b></p>



Parâmetro	Tipo	Descrição
solution_detail	String	Guia de correção de vulnerabilidades Mínimo: <b>0</b> Máximo: <b>65534</b>
url	String	URL de vulnerabilidade Mínimo: <b>0</b> Máximo: <b>2083</b>
description	String	Descrição da vulnerabilidade Mínimo: <b>0</b> Máximo: <b>65534</b>
type	String	Tipo de vulnerabilidade. As opções são as seguintes: -linux_vul: vulnerabilidade do Linux -windows_vul: vulnerabilidade do Windows -web_cms: vulnerabilidade de Web-CMS -app_vul: vulnerabilidade de aplicação Mínimo: <b>0</b> Máximo: <b>128</b>
host_id_list	Array of strings	Listas de servidores que podem lidar com a vulnerabilidade Mínimo: <b>0</b> Máximo: <b>128</b> Comprimento da matriz: <b>0-2147483647</b>
cve_list	Array of <a href="#">cve_list</a> objects	Lista de CVE Comprimento da matriz: <b>1-10000</b>
patch_url	String	Endereço do patch Mínimo: <b>0</b> Máximo: <b>512</b>
repair_priority	String	Prioridade de correção: Critical, High, Medium, Low Mínimo: <b>1</b> Máximo: <b>32</b>
hosts_num	<a href="#">VulnerabilityHostNumberInfo</a> object	Servidor afetado
repair_success_num	Integer	Número de reparos bem-sucedidos Mínimo: <b>0</b> Máximo: <b>1000000</b>

Parâmetro	Tipo	Descrição
fixed_num	Long	Número de reparos Mínimo: <b>0</b> Máximo: <b>1000000</b>
ignored_num	Long	Número de itens ignorados Mínimo: <b>0</b> Máximo: <b>1000000</b>
verify_num	Integer	Número de verificações Mínimo: <b>0</b> Máximo: <b>1000000</b>
repair_priority_list	Array of <a href="#">RepairPriorityListInfo</a> objects	Prioridade de correção. O número de servidores correspondentes a cada prioridade de correção. Comprimento da matriz: <b>0-4</b>

**Tabela 3-328** cve\_list

Parâmetro	Tipo	Descrição
cve_id	String	ID de CVE Mínimo: <b>1</b> Máximo: <b>32</b>
cvss	Float	Pontuação de CVSS Mínimo: <b>0</b> Máximo: <b>10</b>

**Tabela 3-329** VulnerabilityHostNumberInfo

Parâmetro	Tipo	Descrição
important	Integer	Número de servidores importantes Mínimo: <b>0</b> Máximo: <b>10000</b>
common	Integer	Número de servidores comuns Mínimo: <b>0</b> Máximo: <b>10000</b>
test	Integer	Número de servidores de teste Mínimo: <b>0</b> Máximo: <b>10000</b>

**Tabela 3-330** RepairPriorityListInfo

Parâmetro	Tipo	Descrição
repair_priority	String	Prioridade: Critical, High, Medium, Low Mínimo: <b>1</b> Máximo: <b>10</b>
host_num	Integer	Número de servidores correspondentes à prioridade de correção Mínimo: <b>0</b> Máximo: <b>2147483647</b>

## Exemplo de solicitações

Consultar os 10 primeiros registros na lista de vulnerabilidades cujo project\_id é 2b31ed520xxxxxxebdb6e57xxxxxxx.

```
GET https://{endpoint}/v5/2b31ed520xxxxxxebdb6e57xxxxxxx/vulnerability/vulnerabilities?offset=0&limit=10
```

## Exemplo de respostas

**Código de status: 200**

Lista de vulnerabilidades

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

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

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

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

public class ListVulnerabilitiesSolution {

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

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

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

        ListVulnerabilitiesRequest request = new ListVulnerabilitiesRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withType("<type>");
        request.withVulId("<vul_id>");
        request.withVulName("<vul_name>");
        request.withLimit("<limit>");
        request.withOffset("<offset>");
        request.withRepairPriority("<repair_priority>");
        request.withHandleStatus("<handle_status>");
        request.withCveId("<cve_id>");
        request.withLabelList("<label_list>");
        request.withStatus("<status>");
        request.withAssetValue("<asset_value>");
        request.withGroupName("<group_name>");
        try {
            ListVulnerabilitiesResponse response =
client.listVulnerabilities(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

```
}  
}
```

## Python

```
# coding: utf-8  
  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudsdkhss.v5.region.hss_region import HssRegion  
from huaweicloudsdkcore.exceptions import exceptions  
from huaweicloudsdkhss.v5 import *  
  
if __name__ == "__main__":  
    # The AK and SK used for authentication are hard-coded or stored in  
    plaintext, which has great security risks. It is recommended that the AK and SK  
    be stored in ciphertext in configuration files or environment variables and  
    decrypted during use to ensure security.  
    # In this example, AK and SK are stored in environment variables for  
    authentication. Before running this example, set environment variables  
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak = __import__('os').getenv("CLOUD_SDK_AK")  
    sk = __import__('os').getenv("CLOUD_SDK_SK")  
  
    credentials = BasicCredentials(ak, sk) \  
  
    client = HssClient.new_builder() \  
        .with_credentials(credentials) \  
        .with_region(HssRegion.value_of("<YOUR REGION>")) \  
        .build()  
  
    try:  
        request = ListVulnerabilitiesRequest()  
        request.enterprise_project_id = "<enterprise_project_id>"  
        request.type = "<type>"  
        request.vul_id = "<vul_id>"  
        request.vul_name = "<vul_name>"  
        request.limit = <limit>  
        request.offset = <offset>  
        request.repair_priority = "<repair_priority>"  
        request.handle_status = "<handle_status>"  
        request.cve_id = "<cve_id>"  
        request.label_list = "<label_list>"  
        request.status = "<status>"  
        request.asset_value = "<asset_value>"  
        request.group_name = "<group_name>"  
        response = client.list_vulnerabilities(request)  
        print(response)  
    except exceptions.ClientRequestException as e:  
        print(e.status_code)  
        print(e.request_id)  
        print(e.error_code)  
        print(e.error_msg)
```

## Go

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in  
    plaintext, which has great security risks. It is recommended that the AK and SK  
    be stored in ciphertext in configuration files or environment variables and
```

```

decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")

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

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

request := &model.ListVulnerabilitiesRequest{}
enterpriseProjectIdRequest:= "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
typeRequest:= "<type>"
request.Type = &typeRequest
vulIdRequest:= "<vul_id>"
request.VulId = &vulIdRequest
vulNameRequest:= "<vul_name>"
request.VulName = &vulNameRequest
limitRequest:= int32(<limit>)
request.Limit = &limitRequest
offsetRequest:= int32(<offset>)
request.Offset = &offsetRequest
repairPriorityRequest:= "<repair_priority>"
request.RepairPriority = &repairPriorityRequest
handleStatusRequest:= "<handle_status>"
request.HandleStatus = &handleStatusRequest
cveIdRequest:= "<cve_id>"
request.CveId = &cveIdRequest
labelListRequest:= "<label_list>"
request.LabelList = &labelListRequest
statusRequest:= "<status>"
request.Status = &statusRequest
assetValueRequest:= "<asset_value>"
request.AssetValue = &assetValueRequest
groupNameRequest:= "<group_name>"
request.GroupName = &groupNameRequest
response, err := client.ListVulnerabilities(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}

```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de vulnerabilidades

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.11.2 Consulta dos servidores afetados por uma vulnerabilidade

### Função

Esta API é usada para consultar os servidores afetados por uma vulnerabilidade.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/vulnerability/hosts

Tabela 3-331 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

Tabela 3-332 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>128</b>
vul_id	Sim	String	ID de vulnerabilidade Mínimo: <b>0</b> Máximo: <b>64</b>

Parâmetro	Obrigatório	Tipo	Descrição
type	Sim	String	<p>Tipo de vulnerabilidade</p> <ul style="list-style-type: none"> <li>● linux_vul: vulnerabilidade do Linux</li> <li>● windows_vul: vulnerabilidade do Windows -web_cms: vulnerabilidade de Web-CMS</li> <li>● app_vul: vulnerabilidade da aplicação</li> <li>● urgent_vul: vulnerabilidade de emergência</li> </ul> <p>Mínimo: <b>0</b> Máximo: <b>64</b></p>
host_name	Não	String	<p>Nome do servidor afetado</p> <p>Mínimo: <b>0</b> Máximo: <b>256</b></p>
host_ip	Não	String	<p>Endereço IP do servidor afetado</p> <p>Mínimo: <b>0</b> Máximo: <b>128</b></p>
status	Não	String	<p>Status da vulnerabilidade.</p> <ul style="list-style-type: none"> <li>● vul_status_unfix: não corrigido</li> <li>● vul_status_ignored: ignorado <ul style="list-style-type: none"> <li>– vul_status_verified: verificação em andamento</li> <li>– vul_status_fixing: a correção está em andamento.</li> <li>– vul_status_fixed: a correção foi bem sucedida.</li> <li>– vul_status_reboot: o problema foi corrigido e aguarda a reinicialização.</li> <li>– vul_status_failed: o problema não foi corrigido.</li> <li>– vul_status_fix_after_reboot: reinicie o servidor e tente novamente.</li> </ul> </li> </ul> <p>Mínimo: <b>0</b> Máximo: <b>128</b></p>



Parâmetro	Obrigatório	Tipo	Descrição
limit	Não	Integer	Número de registros em cada página Mínimo: <b>10</b> Máximo: <b>200</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é 0. Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
asset_value	Não	String	Importância do ativo: important, common, test Mínimo: <b>0</b> Máximo: <b>32</b>
group_name	Não	String	Nome do grupo de servidores Mínimo: <b>0</b> Máximo: <b>256</b>
handle_status	Não	String	Status de manipulação. As opções são as seguintes: -unhandled - handled Mínimo: <b>1</b> Máximo: <b>32</b>
severity_level	Não	String	Nível de risco. O valor pode ser Critical, High, Medium ou Low. Mínimo: <b>0</b> Máximo: <b>32</b>
is_affect_business	Não	Boolean	Indica se os serviços são afetados. O valor pode ser y ou n.
repair_priority	Não	String	Prioridade de correção. As opções são as seguintes: <ul style="list-style-type: none"><li>● Critical</li><li>● High</li><li>● Medium</li><li>● Low</li></ul> Mínimo: <b>1</b> Máximo: <b>10</b>

## Parâmetros de solicitação

**Tabela 3-333** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-334** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número de servidores afetados Mínimo: <b>0</b> Máximo: <b>10000</b>
data_list	Array of <b>VulHostInfo</b> objects	Lista de ECSs afetados Comprimento da matriz: <b>1–10000</b>

**Tabela 3-335** VulHostInfo

Parâmetro	Tipo	Descrição
host_id	String	ID do servidor afetado pela vulnerabilidade Mínimo: <b>1</b> Máximo: <b>128</b>

Parâmetro	Tipo	Descrição
severity_level	String	<p>Nível de risco.</p> <ul style="list-style-type: none"> <li>● Critical: a pontuação de CVSS da vulnerabilidade é maior ou igual a 9, correspondendo ao nível de alto risco no console.</li> <li>● High: a pontuação de CVSS da vulnerabilidade é maior ou igual a 7 e menor que 9, correspondendo ao nível de risco médio no console.</li> <li>● Medium: a pontuação de CVSS da vulnerabilidade é maior ou igual a 4 e menor que 7, correspondendo ao nível de risco médio no console.</li> <li>● Low: a pontuação de CVSS da vulnerabilidade é menor que 4, correspondendo ao nível de risco baixo no console.</li> </ul> <p>Mínimo: <b>1</b> Máximo: <b>128</b></p>
host_name	String	<p>Nome do servidor afetado</p> <p>Mínimo: <b>1</b> Máximo: <b>256</b></p>
host_ip	String	<p>Endereço IP do servidor afetado</p> <p>Mínimo: <b>1</b> Máximo: <b>256</b></p>
agent_id	String	<p>ID do agente correspondente ao servidor</p> <p>Mínimo: <b>1</b> Máximo: <b>128</b></p>
version	String	<p>A versão da cota vinculada ao servidor</p> <p>Mínimo: <b>1</b> Máximo: <b>128</b></p>
cve_num	Integer	<p>CVES de vulnerabilidade</p> <p>Mínimo: <b>0</b> Máximo: <b>10000</b></p>
cve_id_list	Array of strings	<p>A lista de IDs de CVE correspondente à vulnerabilidade</p> <p>Mínimo: <b>1</b> Máximo: <b>64</b> Comprimento da matriz: <b>1-10000</b></p>

Parâmetro	Tipo	Descrição
status	String	Status da vulnerabilidade. <ul style="list-style-type: none"><li>● vul_status_unfix: não corrigido</li><li>● vul_status_ignored: ignorado</li><li>● vul_status_verified: verificação em andamento</li><li>● vul_status_fixing: a correção está em andamento.</li><li>● vul_status_fixed: a correção foi bem sucedida.</li><li>● vul_status_reboot: o problema foi corrigido e aguarda a reinicialização.</li><li>● vul_status_failed: o problema não foi corrigido.</li><li>● vul_status_fix_after_reboot: reinicie o servidor e tente novamente.</li></ul> Mínimo: <b>1</b> Máximo: <b>128</b>
repair_cmd	String	Linha de comando a ser executada para corrigir a vulnerabilidade (este campo está disponível apenas para vulnerabilidades do Linux). Mínimo: <b>1</b> Máximo: <b>256</b>
app_path	String	Caminho do software de aplicação (este campo está disponível apenas para vulnerabilidades de aplicação). Mínimo: <b>1</b> Máximo: <b>512</b>
region_name	String	Região Mínimo: <b>0</b> Máximo: <b>128</b>
public_ip	String	Endereço IP público do servidor Mínimo: <b>0</b> Máximo: <b>128</b>
private_ip	String	Endereço IP privado de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
group_id	String	ID do grupo de servidores Mínimo: <b>0</b> Máximo: <b>128</b>
group_name	String	Nome do grupo de servidores Mínimo: <b>0</b> Máximo: <b>256</b>

Parâmetro	Tipo	Descrição
os_type	String	Sistema operacional (SO) Mínimo: <b>0</b> Máximo: <b>32</b>
asset_value	String	Importância de ativo. As opções são as seguintes: <ul style="list-style-type: none"> <li>● important</li> <li>● common</li> <li>● test</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>
is_affect_business	Boolean	Se os serviços são afetados
first_scan_time	Long	Hora da primeira verificação Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b>
scan_time	Long	Tempo de verificação, em ms. Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b>
support_restore	Boolean	Indica se os dados podem ser revertidos para o backup criado quando a vulnerabilidade foi corrigida.
disabled_operation_types	Array of <b>disabled_operation_types</b> objects	Lista de tipos de operação de vulnerabilidades que não podem ser executadas no servidor atual. Comprimento da matriz: <b>1–10000</b>
repair_priority	String	Prioridade de correção. As opções são as seguintes: <ul style="list-style-type: none"> <li>● Critical</li> <li>● High</li> <li>● Medium</li> <li>● Low</li> </ul> Mínimo: <b>1</b> Máximo: <b>10</b>

**Tabela 3-336** disabled\_operate\_types

Parâmetro	Tipo	Descrição
operate_type	String	Tipo de operação. <ul style="list-style-type: none"> <li>● ignore</li> <li>● not_ignore: cancelar a ignoração</li> <li>● immediate_repair: corrigir</li> <li>● manual_repair</li> <li>● verify</li> <li>● add_to_whitelist</li> </ul> Mínimo: 1 Máximo: 64
reason	String	Indica o motivo pelo qual a operação não pode ser executada. Mínimo: 0 Máximo: 512

## Exemplo de solicitações

Consultar os 10 primeiros registros na lista de servidores com vulnerabilidade EulerOS-SA-2021-1894.

```
GET https://{endpoint}/v5/2b31ed520xxxxxxebeb6e57xxxxxxx/vulnerability/hosts?
vul_id=EulerOS-SA-2021-1894&offset=0&limit=10
```

## Exemplo de respostas

**Código de status: 200**

Lista de informações do host Vul

```
{
  "total_num" : 1,
  "data_list" : [ {
    "host_id" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "severity_level" : "Low",
    "host_name" : "ecs",
    "host_ip" : "xxx.xxx.xxx.xxx",
    "agent_id" :
"xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
    "version" : "hss.version.enterprise",
    "cve_num" : 1,
    "cve_id_list" : [ "CVE-2022-1664" ],
    "status" : "vul_status_ignored",
    "repair_cmd" : "zypper update update-alternatives",
    "app_path" : "/root/apache-tomcat-8.5.15/bin/bootstrap.jar",
    "support_restore" : true,
    "disabled_operate_types" : [ {
      "operate_type" : "immediate_repair",
      "reason" : "The kernel vulnerability of CCE container node cannot be
automatically fixed."
    } ],
    "repair_priority" : "Critical"
  } ]
}
```

```
} ]  
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;  
import com.huaweicloud.sdk.hss.v5.region.HssRegion;  
import com.huaweicloud.sdk.hss.v5.*;  
import com.huaweicloud.sdk.hss.v5.model.*;  
  
public class ListVulHostsSolution {  
  
    public static void main(String[] args) {  
        // The AK and SK used for authentication are hard-coded or stored in  
        plaintext, which has great security risks. It is recommended that the AK and SK  
        be stored in ciphertext in configuration files or environment variables and  
        decrypted during use to ensure security.  
        // In this example, AK and SK are stored in environment variables for  
        authentication. Before running this example, set environment variables  
        CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
        String ak = System.getenv("CLOUD_SDK_AK");  
        String sk = System.getenv("CLOUD_SDK_SK");  
  
        ICredential auth = new BasicCredentials()  
            .withAk(ak)  
            .withSk(sk);  
  
        HssClient client = HssClient.newBuilder()  
            .withCredential(auth)  
            .withRegion(HssRegion.valueOf("<YOUR_REGION>"))  
            .build();  
  
        ListVulHostsRequest request = new ListVulHostsRequest();  
        request.withEnterpriseProjectId("<enterprise_project_id>");  
        request.withVulId("<vul_id>");  
        request.withType("<type>");  
        request.withHostName("<host_name>");  
        request.withHostIp("<host_ip>");  
        request.withStatus("<status>");  
        request.withLimit(<limit>);  
        request.withOffset(<offset>);  
        request.withAssetValue("<asset_value>");  
        request.withGroupName("<group_name>");  
        request.withHandleStatus("<handle_status>");  
        request.withSeverityLevel("<severity_level>");  
        request.withIsAffectBusiness(<is_affect_business>);  
        request.withRepairPriority("<repair_priority>");  
        try {  
            ListVulHostsResponse response = client.listVulHosts(request);  
            System.out.println(response.toString());  
        } catch (ConnectionException e) {  
            e.printStackTrace();  
        } catch (RequestTimeoutException e) {  
            e.printStackTrace();  
        } catch (ServiceResponseException e) {  
            e.printStackTrace();  
            System.out.println(e.getHttpStatusCode());  
            System.out.println(e.getRequestId());  
        }  
    }  
}
```

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

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
    # plaintext, which has great security risks. It is recommended that the AK and SK
    # be stored in ciphertext in configuration files or environment variables and
    # decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for
    # authentication. Before running this example, set environment variables
    # CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListVulHostsRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.vul_id = "<vul_id>"
        request.type = "<type>"
        request.host_name = "<host_name>"
        request.host_ip = "<host_ip>"
        request.status = "<status>"
        request.limit = <limit>
        request.offset = <offset>
        request.asset_value = "<asset_value>"
        request.group_name = "<group_name>"
        request.handle_status = "<handle_status>"
        request.severity_level = "<severity_level>"
        request.is_affect_business = <IsAffectBusiness>
        request.repair_priority = "<repair_priority>"
        response = client.list_vul_hosts(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)
```



```
func main() {
    // The AK and SK used for authentication are hard-coded or stored in
    // plaintext, which has great security risks. It is recommended that the AK and SK
    // be stored in ciphertext in configuration files or environment variables and
    // decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for
    // authentication. Before running this example, set environment variables
    // CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListVulHostsRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        request.VulId = "<vul_id>"
        request.Type = "<type>"
        hostNameRequest:= "<host_name>"
        request.HostName = &hostNameRequest
        hostIpRequest:= "<host_ip>"
        request.HostIp = &hostIpRequest
        statusRequest:= "<status>"
        request.Status = &statusRequest
        limitRequest:= int32(<limit>)
        request.Limit = &limitRequest
        offsetRequest:= int32(<offset>)
        request.Offset = &offsetRequest
        assetValueRequest:= "<asset_value>"
        request.AssetValue = &assetValueRequest
        groupNameRequest:= "<group_name>"
        request.GroupName = &groupNameRequest
        handleStatusRequest:= "<handle_status>"
        request.HandleStatus = &handleStatusRequest
        severityLevelRequest:= "<severity_level>"
        request.SeverityLevel = &severityLevelRequest
        isAffectBusinessRequest:= <is_affect_business>
        request.IsAffectBusiness = &isAffectBusinessRequest
        repairPriorityRequest:= "<repair_priority>"
        request.RepairPriority = &repairPriorityRequest
        response, err := client.ListVulHosts(request)
        if err == nil {
            fmt.Printf("%+v\n", response)
        } else {
            fmt.Println(err)
        }
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia [Código de amostra no API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de informações do host Vul

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.11.3 Alteração do status de uma vulnerabilidade

#### Função

Esta API é usada para alterar o status de uma vulnerabilidade.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

PUT /v5/{project\_id}/vulnerability/status

**Tabela 3-337** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-338** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de solicitação

**Tabela 3-339** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>32</b> Máximo: <b>4096</b>
Content-Type	Não	String	Valor padrão: application/json; charset=utf-8 Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-340** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
operate_type	Sim	String	Tipo de operação. <ul style="list-style-type: none"><li>● ignore</li><li>● not_ignore: cancelar a ignoração</li><li>● immediate_repair: corrigir</li><li>● verify</li></ul> Mínimo: <b>1</b> Máximo: <b>64</b>
remark	Não	String	Observações Mínimo: <b>0</b> Máximo: <b>512</b>
select_type	Não	String	Selecionar vulnerabilidades. <ul style="list-style-type: none"><li>● all_vul: selecionar todas as vulnerabilidades.</li><li>● all_host: selecionar todas as vulnerabilidades do servidor.</li></ul> Mínimo: <b>1</b> Máximo: <b>64</b>

Parâmetro	Obrigatório	Tipo	Descrição
type	Não	String	Tipo de vulnerabilidade. O valor padrão é <b>linux_vul</b> . As opções são as seguintes: <ul style="list-style-type: none"> <li>● linux_vul: vulnerabilidade do Linux</li> <li>● windows_vul: vulnerabilidade do Windows</li> <li>● web_cms: vulnerabilidade de Web-CMS</li> <li>● app_vul: vulnerabilidade da aplicação</li> </ul> Mínimo: <b>0</b> Máximo: <b>64</b>
data_list	Não	Array of <b>VulOperateInfo</b> objects	Lista de vulnerabilidades Comprimento da matriz: <b>1–500</b>
host_data_list	Não	Array of <b>HostVulOperateInfo</b> objects	Lista de vulnerabilidades na dimensão do servidor Comprimento da matriz: <b>1–500</b>
backup_info_id	Não	String	Especifica o ID das informações de backup processadas pela vulnerabilidade. Se esse parâmetro não for especificado, o backup não será executado. Mínimo: <b>1</b> Máximo: <b>128</b>
custom_backup_hosts	Não	Array of <b>custom_backup_hosts</b> objects	Personalize o cofre e o nome de backup usados pelo host de backup. Para hosts que não estão na lista, o sistema seleciona automaticamente o cofre com o maior espaço restante e gera um nome de backup. Comprimento da matriz: <b>1–50</b>

Tabela 3-341 VulOperateInfo

Parâmetro	Obrigatório	Tipo	Descrição
vul_id	Sim	String	ID de vulnerabilidade Mínimo: <b>1</b> Máximo: <b>64</b>

Parâmetro	Obrigatório	Tipo	Descrição
host_id_list	Sim	Array of strings	Lista de servidores Mínimo: <b>1</b> Máximo: <b>64</b> Comprimento da matriz: <b>1–500</b>

Tabela 3-342 HostVulOperateInfo

Parâmetro	Obrigatório	Tipo	Descrição
host_id	Sim	String	ID de servidor Mínimo: <b>1</b> Máximo: <b>64</b>
vul_id_list	Sim	Array of strings	Lista de vulnerabilidades Mínimo: <b>1</b> Máximo: <b>64</b> Comprimento da matriz: <b>1–500</b>

Tabela 3-343 custom\_backup\_hosts

Parâmetro	Obrigatório	Tipo	Descrição
host_id	Não	String	ID do host Mínimo: <b>1</b> Máximo: <b>128</b>
vault_id	Não	String	ID do cofre Mínimo: <b>1</b> Máximo: <b>128</b>
backup_name	Não	String	Nome do backup Mínimo: <b>1</b> Máximo: <b>64</b>

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Alterar o status de vulnerabilidade do servidor cujo ID é 71a15ecc-049f-4cca-bd28-5e90aca1817f. Alterar o status de EulerOS-SA-2021-1894 para ignorado.

```
{
  "operate_type" : "ignore",
  "data_list" : [ {
    "vul_id" : "EulerOS-SA-2021-1894",
    "host_id_list" : [ "71a15ecc-049f-4cca-bd28-5e90aca1817f" ]
  } ]
}
```

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

Alterar o status de vulnerabilidade do servidor cujo ID é 71a15ecc-049f-4cca-bd28-5e90aca1817f. Alterar o status de EulerOS-SA-2021-1894 para ignorado.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class ChangeVulStatusSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in
        plaintext, which has great security risks. It is recommended that the AK and SK
        be stored in ciphertext in configuration files or environment variables and
        decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for
        authentication. Before running this example, set environment variables
        CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
            .build();

        ChangeVulStatusRequest request = new ChangeVulStatusRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        ChangeVulStatusRequestInfo body = new ChangeVulStatusRequestInfo();
        List<String> listDataListHostIdList = new ArrayList<>();
        listDataListHostIdList.add("71a15ecc-049f-4cca-bd28-5e90aca1817f");
        List<VulOperateInfo> listbodyDataList = new ArrayList<>();
        listbodyDataList.add(
            new VulOperateInfo()
                .withVulId("EulerOS-SA-2021-1894")
                .withHostIdList(listDataListHostIdList)
        );
    }
}
```

```
);
body.withDataList(listbodyDataList);
body.withOperateType("ignore");
request.withBody(body);
try {
    ChangeVulStatusResponse response = client.changeVulStatus(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

Alterar o status de vulnerabilidade do servidor cujo ID é 71a15ecc-049f-4cca-bd28-5e90aca1817f. Alterar o status de EulerOS-SA-2021-1894 para ignorado.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
    # plaintext, which has great security risks. It is recommended that the AK and SK
    # be stored in ciphertext in configuration files or environment variables and
    # decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for
    # authentication. Before running this example, set environment variables
    # CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ChangeVulStatusRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        listHostIdListDataList = [
            "71a15ecc-049f-4cca-bd28-5e90aca1817f"
        ]
        listDataListbody = [
            VulOperateInfo(
                vul_id="EulerOS-SA-2021-1894",
                host_id_list=listHostIdListDataList
            )
        ]
        request.body = ChangeVulStatusRequestInfo(
            data_list=listDataListbody,
            operate_type="ignore"
        )
        response = client.change_vul_status(request)
        print(response)
```

```
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

Alterar o status de vulnerabilidade do servidor cujo ID é 71a15ecc-049f-4cca-bd28-5e90aca1817f. Alterar o status de EulerOS-SA-2021-1894 para ignorado.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
    be stored in ciphertext in configuration files or environment variables and
    decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for
    authentication. Before running this example, set environment variables
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ChangeVulStatusRequest{}
    enterpriseProjectIdRequest := "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    var listHostIdListDataList = []string{
        "71a15ecc-049f-4cca-bd28-5e90aca1817f",
    }
    var listDataListbody = []model.VulOperateInfo{
        {
            VulId: "EulerOS-SA-2021-1894",
            HostIdList: listHostIdListDataList,
        },
    }
    request.Body = &model.ChangeVulStatusRequestInfo{
        DataList: &listDataListbody,
        OperateType: "ignore",
    }
    response, err := client.ChangeVulStatus(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```



## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Resposta bem-sucedida

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.11.4 Consulta de informações de vulnerabilidade sobre um servidor

#### Função

Esta API é usada para consultar as informações de vulnerabilidade sobre um servidor.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/vulnerability/host/{host\_id}

Tabela 3-344 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário. Mínimo: <b>1</b> Máximo: <b>256</b>
host_id	Sim	String	ID do servidor. Mínimo: <b>1</b> Máximo: <b>128</b>

Tabela 3-345 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>0</b> Máximo: <b>256</b>
type	Não	String	Tipo de vulnerabilidade. O valor padrão é <b>linux_vul</b> . As opções são as seguintes: <ul style="list-style-type: none"><li>● <b>linux_vul</b>: vulnerabilidade do Linux</li><li>● <b>windows_vul</b>: vulnerabilidade do Windows -<b>web_cms</b>: vulnerabilidade de Web-CMS</li><li>● <b>app_vul</b>: vulnerabilidade da aplicação</li><li>● <b>urgent_vul</b>: vulnerabilidade de emergência</li></ul> Mínimo: <b>0</b> Máximo: <b>64</b>
vul_name	Não	String	Nome de vulnerabilidade Mínimo: <b>0</b> Máximo: <b>256</b>
limit	Não	Integer	Número de registros exibidos em cada página. Mínimo: <b>0</b> Máximo: <b>200</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é <b>0</b> . Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>

Parâmetro	Obrigatório	Tipo	Descrição
handle_status	Não	String	Status de manipulação. As opções são as seguintes: -unhandled - handled Mínimo: <b>1</b> Máximo: <b>32</b>
status	Não	String	Status da vulnerabilidade. As opções são as seguintes: <ul style="list-style-type: none"> <li>● vul_status_unfix: não corrigido</li> <li>● vul_status_ignored: ignorado</li> <li>● vul_status_verified: verificação em andamento</li> <li>● vul_status_fixing: a correção está em andamento.</li> <li>● vul_status_fixed: a correção foi bem sucedida.</li> <li>● vul_status_reboot: o problema foi corrigido e aguarda a reinicialização.</li> <li>● vul_status_failed: o problema não foi corrigido.</li> <li>● vul_status_fix_after_reboot: reinicie o servidor e tente novamente.</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>
repair_priority	Não	String	Prioridade de correção. As opções são as seguintes: <ul style="list-style-type: none"> <li>● Critical</li> <li>● High</li> <li>● Medium</li> <li>● Low</li> </ul> Mínimo: <b>1</b> Máximo: <b>10</b>

## Parâmetros de solicitação

**Tabela 3-346** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>

## Parâmetros de resposta

**Código de status: 200****Tabela 3-347** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Long	Total Mínimo: <b>0</b> Máximo: <b>2147483647</b>
data_list	Array of <a href="#">HostVulInfo</a> objects	Lista de vulnerabilidades em um servidor Comprimento da matriz: <b>0–2147483647</b>

**Tabela 3-348** HostVulInfo

Parâmetro	Tipo	Descrição
vul_name	String	Nome de vulnerabilidade Mínimo: <b>0</b> Máximo: <b>256</b>
vul_id	String	ID de vulnerabilidade Mínimo: <b>0</b> Máximo: <b>64</b>
label_list	Array of strings	Lista de tags de vulnerabilidade Mínimo: <b>0</b> Máximo: <b>65534</b> Comprimento da matriz: <b>0–2147483647</b>

Parâmetro	Tipo	Descrição
repair_necessity	String	<p>Urgência de reparo. As opções são as seguintes:</p> <ul style="list-style-type: none"> <li>● immediate_repair: o problema deve ser corrigido o mais rápido possível.</li> <li>● delay_repair: o problema pode ser corrigido mais tarde.</li> <li>● not_needed_repair: o problema não precisa ser corrigido.</li> </ul> <p>Mínimo: <b>0</b> Máximo: <b>64</b></p>
scan_time	Long	<p>Hora da última verificação</p> <p>Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b></p>
type	String	<p>Tipo de vulnerabilidade. As opções são as seguintes:</p> <ul style="list-style-type: none"> <li>-linux_vul: vulnerabilidade do Linux</li> <li>-windows_vul: vulnerabilidade do Windows</li> <li>-web_cms: vulnerabilidade de Web-CMS</li> <li>-app_vul: vulnerabilidade de aplicação</li> </ul> <p>Mínimo: <b>0</b> Máximo: <b>128</b></p>
app_list	Array of <a href="#">app_list</a> objects	<p>Lista de softwares afetados pela vulnerabilidade no servidor</p> <p>Comprimento da matriz: <b>0–2147483647</b></p>
severity_level	String	<p>Nível de risco.</p> <ul style="list-style-type: none"> <li>● Critical: a pontuação de CVSS da vulnerabilidade é maior ou igual a 9, correspondendo ao nível de alto risco no console.</li> <li>● High: a pontuação de CVSS da vulnerabilidade é maior ou igual a 7 e menor que 9, correspondendo ao nível de risco médio no console.</li> <li>● Medium: a pontuação de CVSS da vulnerabilidade é maior ou igual a 4 e menor que 7, correspondendo ao nível de risco médio no console.</li> <li>● Low: a pontuação de CVSS da vulnerabilidade é menor que 4, correspondendo ao nível de risco baixo no console.</li> </ul> <p>Mínimo: <b>1</b> Máximo: <b>128</b></p>
solution_detail	String	<p>Solução</p> <p>Mínimo: <b>0</b> Máximo: <b>65534</b></p>

Parâmetro	Tipo	Descrição
url	String	URL Mínimo: <b>0</b> Máximo: <b>2083</b>
description	String	Descrição da vulnerabilidade Mínimo: <b>0</b> Máximo: <b>65534</b>
repair_cmd	String	Comando de reparo Mínimo: <b>1</b> Máximo: <b>256</b>
status	String	Status da vulnerabilidade <ul style="list-style-type: none"> <li>● vul_status_unfix: não corrigido</li> <li>● vul_status_ignored: ignorado</li> <li>● vul_status_verified: verificação em andamento</li> <li>● vul_status_fixing: a correção está em andamento.</li> <li>● vul_status_fixed: a correção foi bem sucedida.</li> <li>● vul_status_reboot: o problema foi corrigido e aguarda a reinicialização.</li> <li>● vul_status_failed: o problema não foi corrigido.</li> <li>● vul_status_fix_after_reboot: reinicie o servidor e tente novamente.</li> </ul> Mínimo: <b>1</b> Máximo: <b>128</b>
repair_success_num	Integer	Total de vezes que a vulnerabilidade é corrigida pelo HSS em toda a rede Mínimo: <b>0</b> Máximo: <b>1000000</b>
cve_list	Array of <a href="#">cve_list</a> objects	Lista de CVE Comprimento da matriz: <b>1–10000</b>
is_affect_business	Boolean	Se os serviços são afetados
first_scan_time	Long	Hora da primeira verificação Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b>
app_name	String	Software Mínimo: <b>0</b> Máximo: <b>256</b>

Parâmetro	Tipo	Descrição
app_version	String	Versão Mínimo: <b>0</b> Máximo: <b>256</b>
app_path	String	Caminho do software Mínimo: <b>0</b> Máximo: <b>512</b>
version	String	Cota do ECS Mínimo: <b>0</b> Máximo: <b>128</b>
support_restore	Boolean	Indica se os dados podem ser revertidos para o backup criado quando a vulnerabilidade foi corrigida.
disabled_operate_types	Array of <b>disabled_operate_types</b> objects	Lista de tipos de operação de vulnerabilidades que não podem ser executadas. Comprimento da matriz: <b>1–10000</b>
repair_priority	String	Prioridade de correção. As opções são as seguintes: <ul style="list-style-type: none"> <li>● Critical</li> <li>● High</li> <li>● Medium</li> <li>● Low</li> </ul> Mínimo: <b>1</b> Máximo: <b>10</b>

Tabela 3-349 app\_list

Parâmetro	Tipo	Descrição
app_name	String	Software Mínimo: <b>0</b> Máximo: <b>256</b>
app_version	String	Versão do software Mínimo: <b>0</b> Máximo: <b>256</b>
upgrade_version	String	Versão para a qual o software com vulnerabilidade precisa ser atualizado Mínimo: <b>0</b> Máximo: <b>256</b>

Parâmetro	Tipo	Descrição
app_path	String	Caminho do software de aplicação (este campo está disponível apenas para vulnerabilidades de aplicação). Mínimo: <b>1</b> Máximo: <b>512</b>

**Tabela 3-350** cve\_list

Parâmetro	Tipo	Descrição
cve_id	String	ID de CVE Mínimo: <b>1</b> Máximo: <b>32</b>
cvss	Float	Pontuação de CVSS Mínimo: <b>0</b> Máximo: <b>10</b>

**Tabela 3-351** disabled\_operate\_types

Parâmetro	Tipo	Descrição
operate_type	String	Tipo de operação. <ul style="list-style-type: none"> <li>● ignore</li> <li>● not_ignore: cancelar a ignoração</li> <li>● immediate_repair: corrigir</li> <li>● manual_repair</li> <li>● verify</li> <li>● add_to_whitelist</li> </ul> Mínimo: <b>1</b> Máximo: <b>64</b>
reason	String	Indica o motivo pelo qual a operação não pode ser executada. Mínimo: <b>0</b> Máximo: <b>512</b>

## Exemplo de solicitações

Consultar as 10 primeiras vulnerabilidades no servidor cujo ID é xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx.



```
GET https://{endpoint}/v5/2b31ed520xxxxxxebedb6e57xxxxxxx/vulnerability/host/  
xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx?offset=0&limit=10
```

## Exemplo de respostas

### Código de status: 200

#### Lista de vulnerabilidades em um servidor

```
{  
  "data_list" : [ {  
    "app_list" : [ {  
      "app_name" : "Apache Log4j API (Apache Log4j API)",  
      "app_version" : "2.8.2",  
      "upgrade_version" : "2.8.3",  
      "app_path" : "/CloudResetPwdUpdateAgent/lib/log4j-api-2.8.2.jar"  
    }, {  
      "app_name" : "Apache Log4j Core (Apache Log4j Core)",  
      "app_version" : "2.8.2",  
      "upgrade_version" : "2.8.3",  
      "app_path" : "/CloudResetPwdUpdateAgent/lib/log4j-api-2.8.2.jar"  
    } ],  
    "app_name" : "Apache Log4j API (Apache Log4j API)",  
    "app_path" : "/CloudResetPwdUpdateAgent/lib/log4j-api-2.8.2.jar",  
    "app_version" : "2.8.2",  
    "cve_list" : [ {  
      "cve_id" : "CVE-2021-45046",  
      "cvss" : 9  
    } ],  
    "description" : "It was found that the fix for address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in some non-default configurations. This could allow attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, ${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern, leading to information leakage and remote code execution in some environments. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for the message search mode and disabling the JNDI function by default.",  
    "first_scan_time" : 1688956612533,  
    "is_affect_business" : true,  
    "label_list" : [ ],  
    "repair_necessity" : "Critical",  
    "scan_time" : 1690469489713,  
    "severity_level" : "Critical",  
    "repair_cmd" : "yum update tcpdump",  
    "solution_detail" : "The official fixing suggestions for this vulnerability have been released. You can visit the following website and fix the vulnerability accordingly:\nhttps://logging.apache.org/log4j/2.x/security.html\nFor details about the patch for this vulnerability, visit the following website:\nhttps://www.oracle.com/security-alerts/cpujan2022.html\nFor details about unofficial fixing suggestions for this vulnerability, visit the following website:\nhttp://www.openwall.com/lists/oss-security/2021/12/14/4\nhttps://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00646.html\nhttps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd\nhttp://www.openwall.com/lists/oss-security/2021/12/15/3\nhttps://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf\nhttps://www.kb.cert.org/vuls/id/930724\nhttps://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf\nhttps://www.debian.org/security/2021/dsa-5022\nhttps://www.oracle.com/security-alerts/alert-cve-2021-44228.html\nhttps://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0032\nhttp://www.openwall.com/lists/oss-security/2021/12/18/1\nhttps://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf\nhttps://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf\nhttps://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/EOKPQGV24RRBBI4TBZUDQMM4MEH7MXCY/\nhttps://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/SIG7FZULMNK2XF6FZRU4VWYDQXNMUGAJ/\n\nThe vulnerability exploitation/POC of this vulnerability has been exposed. You can verify the vulnerability by referring to the following links:\nhttps://github.com/Xlpe0/Log4J-Scan-Win\nhttps://github.com/cckuailong/Log4j_CVE-2021-45046\nhttps://github.com/BobTheShoplifter/
```

```
CVE-2021-45046-Info\nhttps://github.com/tejas-nagchandi/CVE-2021-45046\nhttps://github.com/pravin-pp/log4j2-CVE-2021-45046\nhttps://github.com/mergebase/log4j-samples\nhttps://github.com/lukepasek/log4jndilookupremove\nhttps://github.com/ludy-dev/cve-2021-45046\nhttps://github.com/lijiejie/log4j2_vul_local_scanner\nhttps://github.com/CaptanMoss/Log4Shell-Sandbox-Signature\nhttps://github.com/taise-hub/log4j-poc",
  "status" : "vul_status_unfix",
  "type" : "app_vul",
  "url" : "[\"https://www.oracle.com/security-alerts/cpujan2022.html\"]",
  "version" : "hss.version.wtp",
  "vul_id" : "HCVD-APP-CVE-2021-45046",
  "vul_name" : "CVE-2021-45046",
  "repair_success_num" : 3,
  "support_restore" : true,
  "disabled_operate_types" : [ {
    "operate_type" : "immediate_repair",
    "reason" : "The kernel vulnerability of CCE container node cannot be automatically fixed."
  } ]
} ],
"total_num" : 31
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListHostVulsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
            .build();

        ListHostVulsRequest request = new ListHostVulsRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withType("<type>");
        request.withVulName("<vul_name>");
        request.withLimit(<limit>);
        request.withOffset(<offset>);
    }
}
```

```
request.withHandleStatus("<handle_status>");
request.withStatus("<status>");
request.withRepairPriority("<repair_priority>");
try {
    ListHostVulsResponse response = client.listHostVuls(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.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 huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
    # plaintext, which has great security risks. It is recommended that the AK and SK
    # be stored in ciphertext in configuration files or environment variables and
    # decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for
    # authentication. Before running this example, set environment variables
    # CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListHostVulsRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.type = "<type>"
        request.vul_name = "<vul_name>"
        request.limit = <limit>
        request.offset = <offset>
        request.handle_status = "<handle_status>"
        request.status = "<status>"
        request.repair_priority = "<repair_priority>"
        response = client.list_host_vuls(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main
```

```
import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
    be stored in ciphertext in configuration files or environment variables and
    decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for
    authentication. Before running this example, set environment variables
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListHostVulsRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        typeRequest:= "<type>"
        request.Type = &typeRequest
        vulNameRequest:= "<vul_name>"
        request.VulName = &vulNameRequest
        limitRequest:= int32(<limit>)
        request.Limit = &limitRequest
        offsetRequest:= int32(<offset>)
        request.Offset = &offsetRequest
        handleStatusRequest:= "<handle_status>"
        request.HandleStatus = &handleStatusRequest
        statusRequest:= "<status>"
        request.Status = &statusRequest
        repairPriorityRequest:= "<repair_priority>"
        request.RepairPriority = &repairPriorityRequest
        response, err := client.ListHostVuls(request)
        if err == nil {
            fmt.Printf("%+v\n", response)
        } else {
            fmt.Println(err)
        }
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Lista de vulnerabilidades em um servidor

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.11.5 Criação de uma tarefa de verificação de vulnerabilidade

#### Função

Esta API é usada para criar uma tarefa de verificação de vulnerabilidades.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

POST /v5/{project\_id}/vulnerability/scan-task

**Tabela 3-352** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto. Mínimo: <b>20</b> Máximo: <b>64</b>

**Tabela 3-353** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial do locatário Mínimo: <b>0</b> Máximo: <b>64</b>

## Parâmetros de solicitação

**Tabela 3-354** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando uma API do IAM. O valor de X-Subject-Token no cabeçalho de resposta é o token do usuário.  Mínimo: <b>32</b> Máximo: <b>2097152</b>

**Tabela 3-355** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
manual_scan_type	Não	Array of strings	Tipo de operação. As opções são as seguintes: -linux_vul: vulnerabilidade do Linux - windows_vul: vulnerabilidade do Windows -web_cms: vulnerabilidade de Web-CMS - app_vul: vulnerabilidade de aplicação -urgent_vul: vulnerabilidade de emergência Comprimento da matriz: <b>1–200</b>
batch_flag	Não	Boolean	Especifica se a operação é realizada em lotes. Se o valor for true, todos os servidores suportados serão verificados.
range_type	Não	String	Intervalo de servidores a serem verificados. As opções são as seguintes: -all_host: verificar todos os servidores. Não é necessário definir agent_id_list para esse tipo. -specific_host: verificar o servidor específico.  Mínimo: <b>0</b> Máximo: <b>32</b>
agent_id_list	Não	Array of strings	Lista de servidores  Mínimo: <b>0</b> Máximo: <b>32</b> Comprimento da matriz: <b>1–200</b>

Parâmetro	Obrigatório	Tipo	Descrição
urgent_vul_id_list	Não	Array of strings	Verificar toda a lista de IDs de vulnerabilidades de emergência. Se esse parâmetro for deixado em branco, todas as vulnerabilidades de emergência serão verificadas. Seu valor pode ser: URGENT-CVE-2023-46604 Apache ActiveMQ Remote Code Execution Vulnerability URGENT-HSSVD-2020-1109 Elasticsearch Unauthorized Access Vulnerability URGENT-CVE-2022-26134 Atlassian Confluence OGNL Remote Code Execution Vulnerability (Cve-2022-26134) URGENT-CVE-2023-22515 Atlassian Confluence Data Center and Server Privilege Escalation Vulnerability (CVE-2023-22515) URGENT-CVE-2023-22518 Atlassian Confluence Data Center & Server Inappropriate Authorization Mechanism Vulnerability (CVE-2023-22518) URGENT-CVE-2023-28432 MinIO Information Disclosure Vulnerability (CVE-2023-28432) URGENT-CVE-2023-37582 Apache RocketMQ Remote Code Execution Vulnerability (CVE-2023-37582) URGENT-CVE-2023-33246 Apache RocketMQ Remote Code Execution Vulnerability (CVE-2023-33246) URGENT-CNVD-2023-02709 ZENTAO Project Management System Remote Command Execution Vulnerability (CNVD-2023-02709) URGENT-CVE-2022-36804 Atlassian Bitbucket Server and Data Center Command Injection Vulnerability (CVE-2022-36804) URGENT-CVE-2022-22965 Spring Framework JDK >= 9 Remote Code Execution Vulnerability URGENT-CVE-2022-25845 fastjson <1.2.83 Remote Code

Parâmetro	Obrigatório	Tipo	Descrição
			<p>Execution Vulnerability URGENT-CVE-2019-14439 Jackson-databind Remote Command Execution Vulnerability (CVE-2019-14439) URGENT-CVE-2020-13933 Apache Shiro Authentication Bypass Vulnerability (CVE-2020-13933) URGENT-CVE-2020-26217 XStream &lt; 1.4.14 Remote Code Execution Vulnerability (CVE-2020-26217) URGENT-CVE-2021-4034 Linux Polkit Privilege Escalation Vulnerability (CVE-2021-4034) URGENT-CVE-2021-44228 Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228 and CVE-2021-45046) URGENT-CVE-2022-0847 Dirty Pipe - Linux Kernel Local Privilege Escalation Vulnerability (CVE-2022-0847)</p> <p>Mínimo: <b>0</b> Máximo: <b>32</b> Comprimento da matriz: <b>1–200</b></p>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-356** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
task_id	String	<p>ID da tarefa de detecção</p> <p>Mínimo: <b>0</b> Máximo: <b>32</b></p>

## Exemplo de solicitações

Criar uma tarefa de detecção de vulnerabilidades de emergência cujo agent\_id seja 0253edfd-30e7-439d-8f3f-17c54c997064 e a lista de IDs de vulnerabilidade seja urgent\_vul\_id\_list.

```
POST https://{endpoint}/v5/{project_id}/vulnerability/scan-task?
enterprise_project_id=XXX
```



```
{
  "manual_scan_type" : "urgent_vul",
  "batch_flag" : false,
  "range_type" : "specific_host",
  "agent_id_list" : [ "0253edfd-30e7-439d-8f3f-17c54c997064" ],
  "urgent_vul_id_list" : [ "URGENT-CVE-2023-46604", "URGENT-HSSVD-2020-1109",
"URGENT-CVE-2022-26134", "URGENT-CVE-2023-22515", "URGENT-CVE-2023-22518",
"URGENT-CVE-2023-28432", "URGENT-CVE-2023-37582", "URGENT-CVE-2023-33246",
"URGENT-CNVD-2023-02709", "URGENT-CVE-2022-36804", "URGENT-CVE-2022-22965",
"URGENT-CVE-2022-25845", "URGENT-CVE-2019-14439", "URGENT-CVE-2020-13933",
"URGENT-CVE-2020-26217", "URGENT-CVE-2021-4034", "URGENT-CVE-2021-44228", "URGENT-
CVE-2022-0847" ]
}
```

## Exemplo de respostas

### Código de status: 200

Sucesso na detecção manual de vulnerabilidades

```
{
  "task_id" : "d8a12cf7-6a43-4cd6-92b4-aabf1e917"
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

Criar uma tarefa de detecção de vulnerabilidades de emergência cujo `agent_id` seja `0253edfd-30e7-439d-8f3f-17c54c997064` e a lista de IDs de vulnerabilidade seja `urgent_vul_id_list`.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class CreateVulnerabilityScanTaskSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in
        // plaintext, which has great security risks. It is recommended that the AK and SK
        // be stored in ciphertext in configuration files or environment variables and
        // decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for
        // authentication. Before running this example, set environment variables
        // CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
            .withAk(ak)
            .withSk(sk);
```

```
HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR REGION>"))
    .build();
CreateVulnerabilityScanTaskRequest request = new
CreateVulnerabilityScanTaskRequest();
request.withEnterpriseProjectId("<enterprise_project_id>");
ManualVulScanRequestInfo body = new ManualVulScanRequestInfo();
List<String> listbodyUrgentVulIdList = new ArrayList<>();
listbodyUrgentVulIdList.add("URGENT-CVE-2023-46604");
listbodyUrgentVulIdList.add("URGENT-HSSVD-2020-1109");
listbodyUrgentVulIdList.add("URGENT-CVE-2022-26134");
listbodyUrgentVulIdList.add("URGENT-CVE-2023-22515");
listbodyUrgentVulIdList.add("URGENT-CVE-2023-22518");
listbodyUrgentVulIdList.add("URGENT-CVE-2023-28432");
listbodyUrgentVulIdList.add("URGENT-CVE-2023-37582");
listbodyUrgentVulIdList.add("URGENT-CVE-2023-33246");
listbodyUrgentVulIdList.add("URGENT-CNVD-2023-02709");
listbodyUrgentVulIdList.add("URGENT-CVE-2022-36804");
listbodyUrgentVulIdList.add("URGENT-CVE-2022-22965");
listbodyUrgentVulIdList.add("URGENT-CVE-2022-25845");
listbodyUrgentVulIdList.add("URGENT-CVE-2019-14439");
listbodyUrgentVulIdList.add("URGENT-CVE-2020-13933");
listbodyUrgentVulIdList.add("URGENT-CVE-2020-26217");
listbodyUrgentVulIdList.add("URGENT-CVE-2021-4034");
listbodyUrgentVulIdList.add("URGENT-CVE-2021-44228");
listbodyUrgentVulIdList.add("URGENT-CVE-2022-0847");
List<String> listbodyAgentIdList = new ArrayList<>();
listbodyAgentIdList.add("0253edfd-30e7-439d-8f3f-17c54c997064");
body.withUrgentVulIdList(listbodyUrgentVulIdList);
body.withAgentIdList(listbodyAgentIdList);
body.withRangeType("specific_host");
body.withBatchFlag(false);
request.withBody(body);
try {
    CreateVulnerabilityScanTaskResponse response =
client.createVulnerabilityScanTask(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

Criar uma tarefa de detecção de vulnerabilidades de emergência cujo `agent_id` seja `0253edfd-30e7-439d-8f3f-17c54c997064` e a lista de IDs de vulnerabilidade seja `urgent_vul_id_list`.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
```

be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.

# In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD\_SDK\_AK and CLOUD\_SDK\_SK in the local environment

```
ak = __import__('os').getenv("CLOUD_SDK_AK")
sk = __import__('os').getenv("CLOUD_SDK_SK")

credentials = BasicCredentials(ak, sk) \

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = CreateVulnerabilityScanTaskRequest()
    request.enterprise_project_id = "<enterprise_project_id>"
    listUrgentVulIdListbody = [
        "URGENT-CVE-2023-46604",
        "URGENT-HSSVD-2020-1109",
        "URGENT-CVE-2022-26134",
        "URGENT-CVE-2023-22515",
        "URGENT-CVE-2023-22518",
        "URGENT-CVE-2023-28432",
        "URGENT-CVE-2023-37582",
        "URGENT-CVE-2023-33246",
        "URGENT-CNVD-2023-02709",
        "URGENT-CVE-2022-36804",
        "URGENT-CVE-2022-22965",
        "URGENT-CVE-2022-25845",
        "URGENT-CVE-2019-14439",
        "URGENT-CVE-2020-13933",
        "URGENT-CVE-2020-26217",
        "URGENT-CVE-2021-4034",
        "URGENT-CVE-2021-44228",
        "URGENT-CVE-2022-0847"
    ]
    listAgentIdListbody = [
        "0253edfd-30e7-439d-8f3f-17c54c997064"
    ]
    request.body = ManualVulScanRequestInfo(
        urgent_vul_id_list=listUrgentVulIdListbody,
        agent_id_list=listAgentIdListbody,
        range_type="specific_host",
        batch_flag=False
    )
    response = client.create_vulnerability_scan_task(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

Criar uma tarefa de detecção de vulnerabilidades de emergência cujo `agent_id` seja `0253edfd-30e7-439d-8f3f-17c54c997064` e a lista de IDs de vulnerabilidade seja `urgent_vul_id_list`.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
```

```
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
    be stored in ciphertext in configuration files or environment variables and
    decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for
    authentication. Before running this example, set environment variables
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateVulnerabilityScanTaskRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        var listUrgentVulIdListbody = []string{
            "URGENT-CVE-2023-46604",
            "URGENT-HSSVD-2020-1109",
            "URGENT-CVE-2022-26134",
            "URGENT-CVE-2023-22515",
            "URGENT-CVE-2023-22518",
            "URGENT-CVE-2023-28432",
            "URGENT-CVE-2023-37582",
            "URGENT-CVE-2023-33246",
            "URGENT-CNVD-2023-02709",
            "URGENT-CVE-2022-36804",
            "URGENT-CVE-2022-22965",
            "URGENT-CVE-2022-25845",
            "URGENT-CVE-2019-14439",
            "URGENT-CVE-2020-13933",
            "URGENT-CVE-2020-26217",
            "URGENT-CVE-2021-4034",
            "URGENT-CVE-2021-44228",
            "URGENT-CVE-2022-0847",
        }
        var listAgentIdListbody = []string{
            "0253edfd-30e7-439d-8f3f-17c54c997064",
        }
        rangeTypeManualVulScanRequestInfo:= "specific_host"
        batchFlagManualVulScanRequestInfo:= false
        request.Body = &model.ManualVulScanRequestInfo{
            UrgentVulIdList: &listUrgentVulIdListbody,
            AgentIdList: &listAgentIdListbody,
            RangeType: &rangeTypeManualVulScanRequestInfo,
            BatchFlag: &batchFlagManualVulScanRequestInfo,
        }
        response, err := client.CreateVulnerabilityScanTask(request)
        if err == nil {
            fmt.Printf("%+v\n", response)
        } else {
            fmt.Println(err)
        }
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Sucesso na detecção manual de vulnerabilidades

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.11.6 Consulta de uma política de verificação de vulnerabilidades

### Função

Essa API é usada para consultar uma política de verificação de vulnerabilidades.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/vulnerability/scan-policy

Tabela 3-357 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-358** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>0</b> Máximo: <b>256</b>

## Parâmetros de solicitação

**Tabela 3-359** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando uma API do IAM. O valor de X-Subject-Token no cabeçalho de resposta é o token do usuário. Mínimo: <b>1</b> Máximo: <b>32768</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-360** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
scan_period	String	Período de verificação <ul style="list-style-type: none"> <li>● one_day</li> <li>● three_day</li> <li>● one_week</li> </ul> Mínimo: <b>1</b> Máximo: <b>32</b>
scan_vul_types	Array of strings	Lista de tipos de vulnerabilidades verificados Mínimo: <b>0</b> Máximo: <b>32</b> Comprimento da matriz: <b>0-2147483647</b>

Parâmetro	Tipo	Descrição
scan_range_type	String	Intervalo de hosts a serem verificados. As opções são as seguintes: -all_host -specific_host Mínimo: <b>0</b> Máximo: <b>32</b>
host_ids	Array of strings	Especifica a lista de IDs de host. Quando scan_range_type é definido como specific_host, este parâmetro indica a lista de hosts a serem verificados. Mínimo: <b>1</b> Máximo: <b>128</b> Comprimento da matriz: <b>0-20000</b>
total_host_num	Long	Número total de hosts que podem ser verificados em busca de vulnerabilidades Mínimo: <b>0</b> Máximo: <b>20000</b>
status	String	Status da política de verificação. As opções são as seguintes: -open: ativado -close: desativado Mínimo: <b>0</b> Máximo: <b>32</b>

## Exemplo de solicitações

Consultar a política de verificação de vulnerabilidades cujo project\_id é 2b31ed520xxxxxxebdb6e57xxxxxxx.

```
GET https://{endpoint}/v5/2b31ed520xxxxxxebdb6e57xxxxxxx/vulnerability/scan-policy
```

## Exemplo de respostas

**Código de status: 200**

Política de verificação de vulnerabilidades

```
{
  "scan_period" : "one_day",
  "scan_vul_types" : [ "linux_vul" ],
  "scan_range_type" : "specific_host",
  "host_ids" : [ "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" ],
  "total_host_num" : 5,
  "status" : "open"
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ShowVulScanPolicySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in
        plaintext, which has great security risks. It is recommended that the AK and SK
        be stored in ciphertext in configuration files or environment variables and
        decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for
        authentication. Before running this example, set environment variables
        CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
            .build();
        ShowVulScanPolicyRequest request = new ShowVulScanPolicyRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        try {
            ShowVulScanPolicyResponse response =
client.showVulScanPolicy(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
    be stored in ciphertext in configuration files or environment variables and
    decrypted during use to ensure security.
```



```
# In this example, AK and SK are stored in environment variables for
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak = __import__('os').getenv("CLOUD_SDK_AK")
sk = __import__('os').getenv("CLOUD_SDK_SK")

credentials = BasicCredentials(ak, sk) \

client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ShowVulScanPolicyRequest()
    request.enterprise_project_id = "<enterprise_project_id>"
    response = client.show_vul_scan_policy(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in
plaintext, which has great security risks. It is recommended that the AK and SK
be stored in ciphertext in configuration files or environment variables and
decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowVulScanPolicyRequest{
        enterpriseProjectIdRequest := "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        response, err := client.ShowVulScanPolicy(request)
        if err == nil {
            fmt.Printf("%+v\n", response)
        } else {
            fmt.Println(err)
        }
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Política de verificação de vulnerabilidades

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.11.7 Modificação de uma política de verificação de vulnerabilidades

#### Função

Essa API é usada para modificar uma política de verificação de vulnerabilidades.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

PUT /v5/{project\_id}/vulnerability/scan-policy

**Tabela 3-361** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-362** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Observação: a política de verificação de vulnerabilidades afeta o comportamento de verificação de todos os servidores sob o locatário. Portanto, esse parâmetro deve ser definido como <code>all_granted_eps</code> se o projeto multiempresarial estiver ativado.  Padrão: <b>0</b> Mínimo: <b>0</b> Máximo: <b>256</b>

## Parâmetros de solicitação

**Tabela 3-363** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando uma API do IAM. O valor de X-Subject-Token no cabeçalho de resposta é o token do usuário.  Mínimo: <b>1</b> Máximo: <b>32768</b>

**Tabela 3-364** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
scan_period	Sim	String	Período de verificação <ul style="list-style-type: none"><li>● one_day</li><li>● three_day</li><li>● one_week</li></ul> Mínimo: <b>1</b> Máximo: <b>32</b>

Parâmetro	Obrigatório	Tipo	Descrição
scan_range_type	Sim	String	Intervalo de hosts a serem verificados. As opções são as seguintes: -all_host -specific_host Mínimo: <b>0</b> Máximo: <b>32</b>
host_ids	Não	Array of strings	Especifica a lista de IDs de host. Este parâmetro é obrigatório quando scan_range_type é definido como specific_host. Mínimo: <b>1</b> Máximo: <b>128</b> Comprimento da matriz: <b>0–20000</b>
scan_vul_types	Não	Array of strings	Lista de tipos de vulnerabilidades verificados Mínimo: <b>0</b> Máximo: <b>32</b> Comprimento da matriz: <b>0–2147483647</b>
status	Sim	String	Status da política de verificação. As opções são as seguintes: -open: ativado -close: desativado Mínimo: <b>0</b> Máximo: <b>32</b>

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Modificar uma política de verificação de vulnerabilidades. O período de verificação é diário, o escopo da verificação é o host especificado, o ID do host é xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx e o status da política é ativado.

```
PUT https://{endpoint}/v5/2b31ed520xxxxxxebedb6e57xxxxxxx/vulnerability/scan-policy?enterprise_project_id=all_granted_eps
```

```
{
  "scan_period" : "one_day",
  "scan_range_type" : "specific_host",
  "host_ids" : [ "xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" ],
  "status" : "open"
}
```

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

Modificar uma política de verificação de vulnerabilidades. O período de verificação é diário, o escopo da verificação é o host especificado, o ID do host é xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx e o status da política é ativado.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class ChangeVulScanPolicySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in
        // plaintext, which has great security risks. It is recommended that the AK and SK
        // be stored in ciphertext in configuration files or environment variables and
        // decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for
        // authentication. Before running this example, set environment variables
        // CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();

        ChangeVulScanPolicyRequest request = new ChangeVulScanPolicyRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        ChangeVulScanPolicyRequestInfo body = new
        ChangeVulScanPolicyRequestInfo();
        List<String> listbodyHostIds = new ArrayList<>();
        listbodyHostIds.add("xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx");
        body.withStatus("open");
        body.withHostIds(listbodyHostIds);
        body.withScanRangeType("specific_host");
        body.withScanPeriod("one_day");
        request.withBody(body);
        try {
            ChangeVulScanPolicyResponse response =
            client.changeVulScanPolicy(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
        }
    }
}
```

```
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
```

## Python

Modificar uma política de verificação de vulnerabilidades. O período de verificação é diário, o escopo da verificação é o host especificado, o ID do host é xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx e o status da política é ativado.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
    # plaintext, which has great security risks. It is recommended that the AK and SK
    # be stored in ciphertext in configuration files or environment variables and
    # decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for
    # authentication. Before running this example, set environment variables
    # CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ChangeVulScanPolicyRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        listHostIdsbody = [
            "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
        ]
        request.body = ChangeVulScanPolicyRequestInfo(
            status="open",
            host_ids=listHostIdsbody,
            scan_range_type="specific_host",
            scan_period="one_day"
        )
        response = client.change_vul_scan_policy(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Modificar uma política de verificação de vulnerabilidades. O período de verificação é diário, o escopo da verificação é o host especificado, o ID do host é xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx e o status da política é ativado.

```
package main
```

```
import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
    be stored in ciphertext in configuration files or environment variables and
    decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for
    authentication. Before running this example, set environment variables
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ChangeVulScanPolicyRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        var listHostIdsbody = []string{
            "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
        }
    }
    request.Body = &model.ChangeVulScanPolicyRequestInfo{
        Status: "open",
        HostIds: &listHostIdsbody,
        ScanRangeType: "specific_host",
        ScanPeriod: "one_day",
    }
    response, err := client.ChangeVulScanPolicy(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Resposta bem-sucedida

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.11.8 Consulta das tarefas de verificação de vulnerabilidades

### Função

Essa API é usada para consultar as tarefas de verificação de vulnerabilidades.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/vulnerability/scan-tasks

**Tabela 3-365** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário. Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-366** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como all_granted_eps. Padrão: <b>0</b> Mínimo: <b>0</b> Máximo: <b>256</b>
limit	Não	Integer	Número de registros exibidos em cada página. Mínimo: <b>0</b> Máximo: <b>200</b> Padrão: <b>10</b>



Parâmetro	Obrigatório	Tipo	Descrição
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é <b>0</b> . Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
scan_type	Não	String	Tipo de uma tarefa de verificação. As opções são as seguintes: - manual -schedule Mínimo: <b>0</b> Máximo: <b>32</b>
task_id	Não	String	ID da tarefa de verificação. Mínimo: <b>0</b> Máximo: <b>32</b>
min_start_time	Não	Long	Hora mínima de início de uma tarefa de verificação. Mínimo: <b>0</b> Máximo: <b>9999999999999</b>
max_start_time	Não	Long	Hora máxima de início de uma tarefa de verificação. Mínimo: <b>0</b> Máximo: <b>9999999999999</b>

## Parâmetros de solicitação

**Tabela 3-367** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando uma API do IAM. O valor de X-Subject-Token no cabeçalho de resposta é o token do usuário. Mínimo: <b>1</b> Máximo: <b>32768</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-368** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Long	Número total Mínimo: <b>0</b> Máximo: <b>2147483647</b>
data_list	Array of <b>VulScanTaskInfo</b> objects	Tarefas de verificação de vulnerabilidades Comprimento da matriz: <b>0–2147483647</b>

**Tabela 3-369** VulScanTaskInfo

Parâmetro	Tipo	Descrição
id	String	ID da tarefa Mínimo: <b>1</b> Máximo: <b>256</b>
scan_type	String	Tipo de uma tarefa de verificação. As opções são as seguintes: -manual -schedule Mínimo: <b>0</b> Máximo: <b>128</b>
start_time	Long	Hora de início de uma tarefa de verificação. Mínimo: <b>0</b> Máximo: <b>2147483647</b>
end_time	Long	Hora de término de uma tarefa de verificação. Mínimo: <b>0</b> Máximo: <b>2147483647</b>
scan_vul_types	Array of strings	Lista de tipos de vulnerabilidades verificados pela tarefa Mínimo: <b>1</b> Máximo: <b>32</b> Comprimento da matriz: <b>1–2147483647</b>
status	String	Status de execução de uma tarefa de verificação. As opções são as seguintes: -running -finished Mínimo: <b>1</b> Máximo: <b>32</b>

Parâmetro	Tipo	Descrição
scanning_host_num	Integer	O número de servidores que estão sendo verificados Mínimo: <b>0</b> Máximo: <b>2147483647</b>
success_host_num	Integer	Número de servidores que foram verificados com sucesso Mínimo: <b>0</b> Máximo: <b>2147483647</b>
failed_host_num	Integer	Número de servidores que não foram verificados Mínimo: <b>0</b> Máximo: <b>2147483647</b>

## Exemplo de solicitações

Consultar informações sobre a tarefa de verificação de vulnerabilidades cujo tipo é verificação manual e task\_id é 195db604-2008-4e8b-a49e-389ab0175beb. Por padrão, 10 registros na primeira página são consultados.

```
GET https://{endpoint}/v5/{project_id}/vulnerability/scan-tasks?
offset=0&limit=10&enterprise_project_id=XXX

{
  "scan_type" : "manual",
  "task_id" : "195db604-2008-4e8b-a49e-389ab0175beb"
}
```

## Exemplo de respostas

**Código de status: 200**

Tarefas de verificação de vulnerabilidades

```
{
  "total_num" : 10,
  "data_list" : [ {
    "id" : "2b31ed520xxxxxxeb6e57xxxxxxx",
    "scan_type" : "manual",
    "start_time" : 1679042408195,
    "end_time" : 1679042408295,
    "scan_vul_types" : [ "linux_vul" ],
    "status" : "running",
    "scanning_host_num" : 1,
    "success_host_num" : 1,
    "failed_host_num" : 1
  } ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

Consultar informações sobre a tarefa de verificação de vulnerabilidades cujo tipo é verificação manual e `task_id` é 195db604-2008-4e8b-a49e-389ab0175beb. Por padrão, 10 registros na primeira página são consultados.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListVulScanTaskSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in
        // plaintext, which has great security risks. It is recommended that the AK and SK
        // be stored in ciphertext in configuration files or environment variables and
        // decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for
        // authentication. Before running this example, set environment variables
        // CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
            .build();

        ListVulScanTaskRequest request = new ListVulScanTaskRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withLimit("<limit>");
        request.withOffset("<offset>");
        request.withScanType("<scan_type>");
        request.withTaskId("<task_id>");
        request.withMinStartTime("<min_start_time>L");
        request.withMaxStartTime("<max_start_time>L");
        try {
            ListVulScanTaskResponse response = client.listVulScanTask(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Consultar informações sobre a tarefa de verificação de vulnerabilidades cujo tipo é verificação manual e `task_id` é 195db604-2008-4e8b-a49e-389ab0175beb. Por padrão, 10 registros na primeira página são consultados.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
    # plaintext, which has great security risks. It is recommended that the AK and SK
    # be stored in ciphertext in configuration files or environment variables and
    # decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for
    # authentication. Before running this example, set environment variables
    # CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListVulScanTaskRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.limit = <limit>
        request.offset = <offset>
        request.scan_type = "<scan_type>"
        request.task_id = "<task_id>"
        request.min_start_time = <min_start_time>
        request.max_start_time = <max_start_time>
        response = client.list_vul_scan_task(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Consultar informações sobre a tarefa de verificação de vulnerabilidades cujo tipo é verificação manual e `task_id` é 195db604-2008-4e8b-a49e-389ab0175beb. Por padrão, 10 registros na primeira página são consultados.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in
    // plaintext, which has great security risks. It is recommended that the AK and SK
```

```

be stored in ciphertext in configuration files or environment variables and
decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ListVulScanTaskRequest{
    enterpriseProjectIdRequest:= "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    limitRequest:= int32(<limit>)
    request.Limit = &limitRequest
    offsetRequest:= int32(<offset>)
    request.Offset = &offsetRequest
    scanTypeRequest:= "<scan_type>"
    request.ScanType = &scanTypeRequest
    taskIdRequest:= "<task_id>"
    request.TaskId = &taskIdRequest
    minStartTimeRequest:= int64(<min_start_time>)
    request.MinStartTime = &minStartTimeRequest
    maxStartTimeRequest:= int64(<max_start_time>)
    request.MaxStartTime = &maxStartTimeRequest
    response, err := client.ListVulScanTask(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}

```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Tarefas de verificação de vulnerabilidades

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.11.9 Consulta da lista de servidores correspondentes a uma tarefa de verificação de vulnerabilidade

### Função

Essa API é usada para consultar a lista de servidores correspondentes a uma tarefa de verificação de vulnerabilidade.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/vulnerability/scan-task/{task\_id}/hosts

**Tabela 3-370** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: <b>1</b> Máximo: <b>256</b>
task_id	Sim	String	ID da tarefa Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-371** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>0</b> Máximo: <b>256</b>
limit	Não	Integer	Número de registros exibidos em cada página. Mínimo: <b>0</b> Máximo: <b>200</b> Padrão: <b>10</b>

Parâmetro	Obrigatório	Tipo	Descrição
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é <b>0</b> . Mínimo: <b>0</b> Máximo: <b>2000000</b> Padrão: <b>0</b>
scan_status	Não	String	Status de verificação do servidor. As opções são as seguintes: <ul style="list-style-type: none"><li>● scanning</li><li>● success</li><li>● failed</li></ul> Mínimo: <b>0</b> Máximo: <b>32</b>

## Parâmetros de solicitação

Tabela 3-372 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando uma API do IAM. O valor de X-Subject-Token no cabeçalho de resposta é o token do usuário. Mínimo: <b>1</b> Máximo: <b>32768</b>

## Parâmetros de resposta

Código de status: **200**

Tabela 3-373 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Long	Número total Mínimo: <b>0</b> Máximo: <b>2147483647</b>



Parâmetro	Tipo	Descrição
data_list	Array of <b>VulScanTaskHostInfo</b> objects	Indica a lista de servidores correspondentes a uma tarefa de verificação de vulnerabilidades. Comprimento da matriz: <b>0-2147483647</b>

**Tabela 3-374** VulScanTaskHostInfo

Parâmetro	Tipo	Descrição
host_id	String	ID de servidor Mínimo: <b>1</b> Máximo: <b>128</b>
host_name	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
public_ip	String	EIP Mínimo: <b>0</b> Máximo: <b>128</b>
private_ip	String	Endereço IP privado Mínimo: <b>0</b> Máximo: <b>128</b>
asset_value	String	Importância de ativo. As opções são as seguintes: <ul style="list-style-type: none"> <li>● important</li> <li>● common</li> <li>● test</li> </ul> Mínimo: <b>0</b> Máximo: <b>128</b>
scan_status	String	Status de verificação do servidor. As opções são as seguintes: -scanning -success -failed Mínimo: <b>0</b> Máximo: <b>32</b>
failed_reasons	Array of <b>failed_reasons</b> objects	Lista de causas de falha de verificação Comprimento da matriz: <b>0-2147483647</b>

**Tabela 3-375** failed\_reasons

Parâmetro	Tipo	Descrição
vul_type	String	Tipo da vulnerabilidade que não foi verificada. As opções são as seguintes: -linux_vul: vulnerabilidade do Linux -windows_vul: vulnerabilidade do Windows -web_cms: vulnerabilidade de Web-CMS -app_vul: vulnerabilidade de aplicação Mínimo: <b>1</b> Máximo: <b>32</b>
failed_reason	String	Causa da falha de verificação. Mínimo: <b>0</b> Máximo: <b>128</b>

## Exemplo de solicitações

Essa API é usada para consultar detalhes da tarefa de verificação de vulnerabilidade cujo ID é 2b31ed520xxxxxxeb6e57xxxxxxx. A lista de servidores e causas de falha é exibida. Por padrão, 10 servidores na primeira página são consultados.

```
GET https://{endpoint}/v5/{project_id}/vulnerability/scan-task/{task_id}/hosts?
offset=0&limit=10&scan_status=failed&enterprise_project_id=XXX

{
  "scan_status" : "failed",
  "task_id" : "2b31ed520xxxxxxeb6e57xxxxxxx"
}
```

## Exemplo de respostas

### Código de status: 200

Indica a lista de servidores correspondentes a uma tarefa de verificação de vulnerabilidades.

```
{
  "total_num" : 1,
  "data_list" : [ {
    "host_id" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "host_name" : "ecs-ubuntu-abc123",
    "public_ip" : "112.10.10.3",
    "private_ip" : "192.168.10.1",
    "asset_value" : "important",
    "scan_status" : "failed",
    "failed_reasons" : [ {
      "vul_type" : "linux_vul",
      "failed_reason" : "this_is_failed_reason"
    } ]
  } ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

Essa API é usada para consultar detalhes da tarefa de verificação de vulnerabilidade cujo ID é 2b31ed520xxxxxxebedb6e57xxxxxxx. A lista de servidores e causas de falha é exibida. Por padrão, 10 servidores na primeira página são consultados.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListVulScanTaskHostSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in
        // plaintext, which has great security risks. It is recommended that the AK and SK
        // be stored in ciphertext in configuration files or environment variables and
        // decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for
        // authentication. Before running this example, set environment variables
        // CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
            .build();

        ListVulScanTaskHostRequest request = new ListVulScanTaskHostRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withLimit("<limit>");
        request.withOffset("<offset>");
        request.withScanStatus("<scan_status>");
        try {
            ListVulScanTaskHostResponse response =
                client.listVulScanTaskHost(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Essa API é usada para consultar detalhes da tarefa de verificação de vulnerabilidade cujo ID é 2b31ed520xxxxxxebedb6e57xxxxxxx. A lista de servidores e causas de falha é exibida. Por padrão, 10 servidores na primeira página são consultados.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
    be stored in ciphertext in configuration files or environment variables and
    decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for
    authentication. Before running this example, set environment variables
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListVulScanTaskHostRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.limit = <limit>
        request.offset = <offset>
        request.scan_status = "<scan_status>"
        response = client.list_vul_scan_task_host(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Essa API é usada para consultar detalhes da tarefa de verificação de vulnerabilidade cujo ID é 2b31ed520xxxxxxebdb6e57xxxxxxx. A lista de servidores e causas de falha é exibida. Por padrão, 10 servidores na primeira página são consultados.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
    be stored in ciphertext in configuration files or environment variables and
    decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for
    authentication. Before running this example, set environment variables
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
```

```
WithSk(sk).
Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ListVulScanTaskHostRequest{}
enterpriseProjectIdRequest := "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
limitRequest := int32(<limit>)
request.Limit = &limitRequest
offsetRequest := int32(<offset>)
request.Offset = &offsetRequest
scanStatusRequest := "<scan_status>"
request.ScanStatus = &scanStatusRequest
response, err := client.ListVulScanTaskHost(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Indica a lista de servidores correspondentes a uma tarefa de verificação de vulnerabilidades.

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.11.10 Consulta de estatísticas de gerenciamento de vulnerabilidades

### Função

Essa API é usada para consultar estatísticas de gerenciamento de vulnerabilidades.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

## URI

GET /v5/{project\_id}/vulnerability/statistics

**Tabela 3-376** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: <b>1</b> Máximo: <b>256</b>

**Tabela 3-377** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial. Para consultar todos os projetos empresariais, defina este parâmetro como <b>all_granted_eps</b> . Padrão: <b>0</b> Mínimo: <b>0</b> Máximo: <b>256</b>

## Parâmetros de solicitação

**Tabela 3-378** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>1</b> Máximo: <b>32768</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-379** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
need_urgent_repair	Integer	Número de vulnerabilidades que precisam ser corrigidas com urgência Mínimo: <b>0</b> Máximo: <b>2147483647</b>
unrepair	Integer	Número de vulnerabilidades não corrigidas Mínimo: <b>0</b> Máximo: <b>2147483647</b>
existed_vul_hosts	Integer	Número de servidores com vulnerabilidades Mínimo: <b>0</b> Máximo: <b>2147483647</b>
today_handle	Integer	Vulnerabilidades tratadas hoje Mínimo: <b>0</b> Máximo: <b>2147483647</b>
all_handle	Integer	Total de vulnerabilidades tratadas Mínimo: <b>0</b> Máximo: <b>2147483647</b>
supported	Integer	Vulnerabilidades suportadas Mínimo: <b>0</b> Máximo: <b>2147483647</b>
vul_library_update_time	Long	Biblioteca de vulnerabilidades atualizada Mínimo: <b>0</b> Máximo: <b>9223372036854775807</b>

## Exemplo de solicitações

Consultar estatísticas de vulnerabilidade cujo project\_id é  
2b31ed520xxxxxxebedb6e57xxxxxxx.

```
GET https://{endpoint}/v5/2b31ed520xxxxxxebedb6e57xxxxxxx/vulnerability/statistics
```

## Exemplo de respostas

**Código de status: 200**

Estatísticas de vulnerabilidade

```
{  
  "need_urgent_repair" : 22,  
  "unrepair" : 23,  
  "existed_vul_hosts" : 33,  
  "today_handle" : 77,  
}
```

```
"all_handle" : 44,  
"supported" : 78,  
"vul_library_update_time" : 1692170925188  
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;  
import com.huaweicloud.sdk.hss.v5.region.HssRegion;  
import com.huaweicloud.sdk.hss.v5.*;  
import com.huaweicloud.sdk.hss.v5.model.*;  
  
public class ShowVulStaticsSolution {  
  
    public static void main(String[] args) {  
        // The AK and SK used for authentication are hard-coded or stored in  
        plaintext, which has great security risks. It is recommended that the AK and SK  
        be stored in ciphertext in configuration files or environment variables and  
        decrypted during use to ensure security.  
        // In this example, AK and SK are stored in environment variables for  
        authentication. Before running this example, set environment variables  
        CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
        String ak = System.getenv("CLOUD_SDK_AK");  
        String sk = System.getenv("CLOUD_SDK_SK");  
  
        ICredential auth = new BasicCredentials()  
            .withAk(ak)  
            .withSk(sk);  
  
        HssClient client = HssClient.newBuilder()  
            .withCredential(auth)  
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))  
            .build();  
        ShowVulStaticsRequest request = new ShowVulStaticsRequest();  
        request.withEnterpriseProjectId("<enterprise_project_id>");  
        try {  
            ShowVulStaticsResponse response = client.showVulStatics(request);  
            System.out.println(response.toString());  
        } catch (ConnectionException e) {  
            e.printStackTrace();  
        } catch (RequestTimeoutException e) {  
            e.printStackTrace();  
        } catch (ServiceResponseException e) {  
            e.printStackTrace();  
            System.out.println(e.getHttpStatusCode());  
            System.out.println(e.getRequestId());  
            System.out.println(e.getErrorCode());  
            System.out.println(e.getErrorMsg());  
        }  
    }  
}
```

### Python

```
# coding: utf-8
```



```
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
    be stored in ciphertext in configuration files or environment variables and
    decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for
    authentication. Before running this example, set environment variables
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowVulStaticsRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        response = client.show_vul_statics(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
    be stored in ciphertext in configuration files or environment variables and
    decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for
    authentication. Before running this example, set environment variables
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowVulStaticsRequest{}
```

```
enterpriseProjectIdRequest:= "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
response, err := client.ShowVulStatics(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Estatísticas de vulnerabilidade

## Códigos de erro

Consulte [Códigos de erro](#).

# 3.12 Proteção contra adulteração da Web

## 3.12.1 Consulta da lista de proteção

### Função

Esta API é usada para consultar a lista de proteção.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/webtamper/hosts

Tabela 3-380 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>0</b> Máximo: <b>64</b>

Tabela 3-381 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Mínimo: <b>0</b> Máximo: <b>64</b>
host_name	Não	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>256</b>
host_id	Não	String	ID do host Mínimo: <b>0</b> Máximo: <b>128</b>
public_ip	Não	String	EIP Mínimo: <b>0</b> Máximo: <b>128</b>
private_ip	Não	String	Endereço IP privado Mínimo: <b>0</b> Máximo: <b>128</b>
group_name	Não	String	Nome do grupo de servidores Mínimo: <b>0</b> Máximo: <b>256</b>
os_type	Não	String	Tipo de SO. Seu valor pode ser: ● linux ● windows Mínimo: <b>0</b> Máximo: <b>32</b>
protect_status	Não	String	Status de proteção. ● closed: desativada ● opened: proteção ativada Mínimo: <b>0</b> Máximo: <b>32</b>

Parâmetro	Obrigatório	Tipo	Descrição
agent_status	Não	String	Status de agente. Seu valor pode ser: <ul style="list-style-type: none"> <li>● not_installed: o agente não está instalado.</li> <li>● online: o agente está on-line.</li> <li>● offline: o agente está off-line.</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>
limit	Não	Integer	Valor padrão: 10 Mínimo: <b>10</b> Máximo: <b>100</b> Padrão: <b>10</b>
offset	Não	Integer	Deslocamento, que especifica a posição inicial do registro a ser retornado. O valor deve ser um número não menor que 0. O valor padrão é <b>0</b> . Mínimo: <b>0</b> Máximo: <b>100</b> Padrão: <b>0</b>

## Parâmetros de solicitação

Tabela 3-382 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>32</b>

## Parâmetros de resposta

**Código de status: 200**

**Tabela 3-383** Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
data_list	Array of <a href="#">WtpProtectHostResponseInfo</a> objects	Lista de dados Comprimento da matriz: <b>0–200000</b>
total_num	Integer	Número total de servidores protegidos por WTP Mínimo: <b>0</b> Máximo: <b>65535</b>

**Tabela 3-384** WtpProtectHostResponseInfo

Parâmetro	Tipo	Descrição
host_name	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>256</b>
host_id	String	ID do host Mínimo: <b>0</b> Máximo: <b>128</b>
public_ip	String	EIP Mínimo: <b>0</b> Máximo: <b>128</b>
private_ip	String	Endereço IP privado Mínimo: <b>0</b> Máximo: <b>128</b>
ipv6	String	Endereço IPv6 privado Mínimo: <b>0</b> Máximo: <b>256</b>
group_name	String	Nome do grupo de servidores Mínimo: <b>0</b> Máximo: <b>256</b>
os_bit	String	Versão de bit do SO Mínimo: <b>0</b> Máximo: <b>8</b>

Parâmetro	Tipo	Descrição
os_type	String	SO (linux ou windows) Mínimo: <b>0</b> Máximo: <b>32</b>
protect_status	String	Status de proteção. Seu valor pode ser: <ul style="list-style-type: none"> <li>● closed</li> <li>● opened</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>
rasp_protect_status	String	Status da WTP dinâmica. <ul style="list-style-type: none"> <li>● closed</li> <li>● opened</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>
anti_tampering_times	Long	Número de ataques de adulteração bloqueados Mínimo: <b>0</b> Máximo: <b>2000000000</b>
detect_tampering_times	Long	Número de ataques de adulteração detectados Mínimo: <b>0</b> Máximo: <b>2000000000</b>
last_detect_time	Long	Hora da última detecção (ms) Mínimo: <b>0</b> Máximo: <b>4070880000000</b>
scheduled_shutdown_status	String	Status da proteção agendada. <ul style="list-style-type: none"> <li>● opened</li> <li>● closed</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>
agent_status	String	Status de agente. <ul style="list-style-type: none"> <li>● not_installed: o agente não está instalado.</li> <li>● online: o agente está on-line.</li> <li>● offline: o agente está off-line.</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>

## Exemplo de solicitações

Esta API é usada para consultar os 10 registros na primeira página da lista de status de WTP de servidores cujo status está ativado e o ID do projeto empresarial é XX por padrão.

```
GET https://{endpoint}/v5/{project_id}/webtamper/hosts?
offset=XX&limit=XX&protect_status=opened&enterprise_project_id=XX

{
  "protect_status" : "opened"
}
```

## Exemplo de respostas

**Código de status: 200**

OK

```
{
  "total_num" : 1,
  "data_list" : [ {
    "host_name" : "test",
    "host_id" : "000411f9-42a7-4acd-80e6-f7b9d3db895f",
    "public_ip" : "",
    "private_ip" : "192.168.0.70,fe80::f816:3eff:fed4:c4d7",
    "ipv6" : "fe80::f816:3eff:fed4:c4d7",
    "group_name" : "testGroup",
    "os_bit" : "64",
    "os_type" : "Linux",
    "protect_status" : "opened",
    "rasp_protect_status" : "opened",
    "anti_tampering_times" : 0,
    "detect_tampering_times" : 0,
    "last_detect_time" : 0,
    "agent_status" : "online"
  } ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

Esta API é usada para consultar os 10 registros na primeira página da lista de status de WTP de servidores cujo status está ativado e o ID do projeto empresarial é XX por padrão.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListWtpProtectHostSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in
plaintext, which has great security risks. It is recommended that the AK and SK
be stored in ciphertext in configuration files or environment variables and
```

```
decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");

ICredential auth = new BasicCredentials()
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
    .build();
ListWtpProtectHostRequest request = new ListWtpProtectHostRequest();
request.withEnterpriseProjectId("<enterprise_project_id>");
request.withHostName("<host_name>");
request.withHostId("<host_id>");
request.withPublicIp("<public_ip>");
request.withPrivateIp("<private_ip>");
request.withGroupName("<group_name>");
request.withOsType("<os_type>");
request.withProtectStatus("<protect_status>");
request.withAgentStatus("<agent_status>");
request.withLimit(<limit>);
request.withOffset(<offset>);
try {
    ListWtpProtectHostResponse response =
client.listWtpProtectHost(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

Esta API é usada para consultar os 10 registros na primeira página da lista de status de WTP de servidores cujo status está ativado e o ID do projeto empresarial é XX por padrão.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
plaintext, which has great security risks. It is recommended that the AK and SK
be stored in ciphertext in configuration files or environment variables and
decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \
```



```
client = HssClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(HssRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListWtpProtectHostRequest()
    request.enterprise_project_id = "<enterprise_project_id>"
    request.host_name = "<host_name>"
    request.host_id = "<host_id>"
    request.public_ip = "<public_ip>"
    request.private_ip = "<private_ip>"
    request.group_name = "<group_name>"
    request.os_type = "<os_type>"
    request.protect_status = "<protect_status>"
    request.agent_status = "<agent_status>"
    request.limit = <limit>
    request.offset = <offset>
    response = client.list_wtp_protect_host(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

Esta API é usada para consultar os 10 registros na primeira página da lista de status de WTP de servidores cujo status está ativado e o ID do projeto empresarial é XX por padrão.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
    be stored in ciphertext in configuration files or environment variables and
    decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for
    authentication. Before running this example, set environment variables
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListWtpProtectHostRequest{
        enterpriseProjectIdRequest:= "<enterprise_project_id>"
        request.EnterpriseProjectId = &enterpriseProjectIdRequest
        hostNameRequest:= "<host_name>"
        request.HostName = &hostNameRequest
    }
```

```
hostIdRequest:= "<host_id>"
request.HostId = &hostIdRequest
publicIpRequest:= "<public_ip>"
request.PublicIp = &publicIpRequest
privateIpRequest:= "<private_ip>"
request.PrivateIp = &privateIpRequest
groupNameRequest:= "<group_name>"
request.GroupName = &groupNameRequest
osTypeRequest:= "<os_type>"
request.OsType = &osTypeRequest
protectStatusRequest:= "<protect_status>"
request.ProtectStatus = &protectStatusRequest
agentStatusRequest:= "<agent_status>"
request.AgentStatus = &agentStatusRequest
limitRequest:= int32(<limit>)
request.Limit = &limitRequest
offsetRequest:= int32(<offset>)
request.Offset = &offsetRequest
response, err := client.ListWtpProtectHost(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	OK

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.12.2 Ativação ou desativação de WTP

#### Função

Essa API é usada para ativar ou desativar a WTP.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

POST /v5/{project\_id}/webtamper/static/status

**Tabela 3-385** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>0</b> Máximo: <b>64</b>

**Tabela 3-386** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Mínimo: <b>0</b> Máximo: <b>64</b>

## Parâmetros de solicitação

**Tabela 3-387** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>1</b> Máximo: <b>32768</b>
Content-Type	Não	String	Valor padrão: application/json; charset=utf-8 Mínimo: <b>0</b> Máximo: <b>128</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>32</b>

**Tabela 3-388** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
status	Sim	Boolean	Status (ativado ou desativado)

Parâmetro	Obrigatório	Tipo	Descrição
host_id_list	Sim	Array of strings	O valor na matriz é o ID do servidor e o ID do servidor não pode ficar vazio. Mínimo: <b>0</b> Máximo: <b>128</b> Comprimento da matriz: <b>1–20000</b>
resource_id	Não	String	ID do recurso Mínimo: <b>0</b> Máximo: <b>64</b>
charging_mode	Não	String	Modo de cobrança. ● packet_cycle: anual/mensal Mínimo: <b>0</b> Máximo: <b>32</b>

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Ativar a WTP, definir os IDs do servidor de destino como a e b e pagar pelo modo de cobrança anual/mensal.

```
POST https://{endpoint}/v5/{project_id}/webtamper/static/status
{
  "status" : true,
  "host_id_list" : [ "a", "b" ],
  "resource_id" : "aaxxx",
  "charging_mode" : "packet_cycle"
}
```

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

Ativar a WTP, definir os IDs do servidor de destino como a e b e pagar pelo modo de cobrança anual/mensal.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
```

```
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class SetWtpProtectionStatusInfoSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in
plaintext, which has great security risks. It is recommended that the AK and SK
be stored in ciphertext in configuration files or environment variables and
decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
            .build();

        SetWtpProtectionStatusInfoRequest request = new
SetWtpProtectionStatusInfoRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        SetWtpProtectionStatusRequestInfo body = new
SetWtpProtectionStatusRequestInfo();
        List<String> listbodyHostIdList = new ArrayList<>();
        listbodyHostIdList.add("a");
        listbodyHostIdList.add("b");
        body.withChargingMode("packet_cycle");
        body.withResourceId("aaxxx");
        body.withHostIdList(listbodyHostIdList);
        body.withStatus(true);
        request.withBody(body);
        try {
            SetWtpProtectionStatusInfoResponse response =
client.setWtpProtectionStatusInfo(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Ativar a WTP, definir os IDs do servidor de destino como a e b e pagar pelo modo de cobrança anual/mensal.

```
# coding: utf-8
```

```
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
    # plaintext, which has great security risks. It is recommended that the AK and SK
    # be stored in ciphertext in configuration files or environment variables and
    # decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for
    # authentication. Before running this example, set environment variables
    # CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = SetWtpProtectionStatusInfoRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        listHostIdListbody = [
            "a",
            "b"
        ]
        request.body = SetWtpProtectionStatusRequestInfo(
            charging_mode="packet_cycle",
            resource_id="aaxxx",
            host_id_list=listHostIdListbody,
            status=True
        )
        response = client.set_wtp_protection_status_info(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Ativar a WTP, definir os IDs do servidor de destino como a e b e pagar pelo modo de cobrança anual/mensal.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in
    // plaintext, which has great security risks. It is recommended that the AK and SK
    // be stored in ciphertext in configuration files or environment variables and
    // decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for
    // authentication. Before running this example, set environment variables
    // CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
```

```
auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.SetWtpProtectionStatusInfoRequest{}
enterpriseProjectIdRequest := "<enterprise_project_id>"
request.EnterpriseProjectId = &enterpriseProjectIdRequest
var listHostIdListbody = []string{
    "a",
    "b",
}
chargingModeSetWtpProtectionStatusRequestInfo := "packet_cycle"
resourceIdSetWtpProtectionStatusRequestInfo := "aaxxx"
request.Body = &model.SetWtpProtectionStatusRequestInfo{
    ChargingMode: &chargingModeSetWtpProtectionStatusRequestInfo,
    ResourceId: &resourceIdSetWtpProtectionStatusRequestInfo,
    HostIdList: listHostIdListbody,
    Status: true,
}
response, err := client.SetWtpProtectionStatusInfo(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Resposta de sucesso

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.12.3 Ativação ou desativação da WTP dinâmica

#### Função

Essa API é usada para ativar ou desativar a WTP dinâmica.

## Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

## URI

POST /v5/{project\_id}/webtamper/rasp/status

**Tabela 3-389** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>0</b> Máximo: <b>64</b>

**Tabela 3-390** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Mínimo: <b>0</b> Máximo: <b>64</b>

## Parâmetros de solicitação

**Tabela 3-391** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>1</b> Máximo: <b>32768</b>
Content-Type	Não	String	Valor padrão: application/json; charset=utf-8 Mínimo: <b>0</b> Máximo: <b>128</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>32</b>



**Tabela 3-392** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
host_id_list	Não	Array of strings	Lista de HostId Mínimo: <b>0</b> Máximo: <b>128</b> Comprimento da matriz: <b>0–20000</b>
status	Não	Boolean	Status da WTP dinâmica

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Ativar a WTP dinâmica para os servidores a e b.

```
POST https://{endpoint}/v5/{project_id}/webtamper/rasp/status
{
  "host_id_list" : [ "a", "b" ],
  "status" : true
}
```

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

Ativar a WTP dinâmica para os servidores a e b.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class SetRaspSwitchSolution {

    public static void main(String[] args) {
```

```
// The AK and SK used for authentication are hard-coded or stored in
plaintext, which has great security risks. It is recommended that the AK and SK
be stored in ciphertext in configuration files or environment variables and
decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");

ICredential auth = new BasicCredentials()
    .withAk(ak)
    .withSk(sk);

HssClient client = HssClient.newBuilder()
    .withCredential(auth)
    .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
    .build();
SetRaspSwitchRequest request = new SetRaspSwitchRequest();
request.withEnterpriseProjectId("<enterprise_project_id>");
SetRaspSwitchRequestInfo body = new SetRaspSwitchRequestInfo();
List<String> listbodyHostIdList = new ArrayList<>();
listbodyHostIdList.add("a");
listbodyHostIdList.add("b");
body.withStatus(true);
body.withHostIdList(listbodyHostIdList);
request.withBody(body);
try {
    SetRaspSwitchResponse response = client.setRaspSwitch(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

Ativar a WTP dinâmica para os servidores a e b.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
    be stored in ciphertext in configuration files or environment variables and
    decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for
    authentication. Before running this example, set environment variables
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = HssClient.new_builder() \
```

```
.with_credentials(credentials) \  
.with_region(HssRegion.value_of("<YOUR REGION>")) \  
.build()  
  
try:  
    request = SetRaspSwitchRequest()  
    request.enterprise_project_id = "<enterprise_project_id>"  
    listHostIdListbody = [  
        "a",  
        "b"  
    ]  
    request.body = SetRaspSwitchRequestInfo(  
        status=True,  
        host_id_list=listHostIdListbody  
    )  
    response = client.set_rasp_switch(request)  
    print(response)  
except exceptions.ClientRequestException as e:  
    print(e.status_code)  
    print(e.request_id)  
    print(e.error_code)  
    print(e.error_msg)
```

## Go

Ativar a WTP dinâmica para os servidores a e b.

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in  
    plaintext, which has great security risks. It is recommended that the AK and SK  
    be stored in ciphertext in configuration files or environment variables and  
    decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for  
    authentication. Before running this example, set environment variables  
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        Build()  
  
    client := hss.NewHssClient(  
        hss.HssClientBuilder().  
            WithRegion(region.ValueOf("<YOUR REGION>")).  
            WithCredential(auth).  
            Build())  
  
    request := &model.SetRaspSwitchRequest{  
        enterpriseProjectIdRequest:= "<enterprise_project_id>"  
        request.EnterpriseProjectId = &enterpriseProjectIdRequest  
        var listHostIdListbody = List<String>{  
            "a",  
            "b",  
        }  
    }  
    statusSetRaspSwitchRequestInfo:= true  
    request.Body = &model.SetRaspSwitchRequestInfo{  
        Status: &statusSetRaspSwitchRequestInfo,  
    }
```

```
HostIdList: &listHostIdListbody,  
}  
response, err := client.SetRaspSwitch(request)  
if err == nil {  
    fmt.Printf("%+v\n", response)  
} else {  
    fmt.Println(err)  
}  
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Resposta de sucesso

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.12.4 Consulta do status de WTP estática para um servidor

#### Função

Essa API é usada para consultar o status de WTP estática de um servidor.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

GET /v5/{project\_id}/webtamper/static/protect-history

Tabela 3-393 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>0</b> Máximo: <b>64</b>

**Tabela 3-394** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Mínimo: <b>0</b> Máximo: <b>64</b>
host_id	Não	String	ID do servidor. Se esse parâmetro for deixado em branco, todos os servidores serão consultados. Mínimo: <b>0</b> Máximo: <b>128</b>
start_time	Sim	Long	Hora de início (ms) Mínimo: <b>0</b> Máximo: <b>4070880000000</b>
end_time	Sim	Long	Hora de término (ms) Mínimo: <b>0</b> Máximo: <b>4070880000000</b>
limit	Sim	Integer	Limite Mínimo: <b>0</b> Máximo: <b>100</b>
offset	Sim	Integer	Deslocamento Mínimo: <b>0</b> Máximo: <b>100</b>
host_name	Não	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>128</b>
host_ip	Não	String	Endereço IP do servidor Mínimo: <b>0</b> Máximo: <b>128</b>
file_path	Não	String	Arquivo protegido Mínimo: <b>0</b> Máximo: <b>128</b>

Parâmetro	Obrigatório	Tipo	Descrição
file_operation	Não	String	Tipos de operações de arquivo, incluindo: <ul style="list-style-type: none"><li>● add</li><li>● delete</li><li>● modify</li><li>● attribute</li></ul> Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de solicitação

Tabela 3-395 Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>1</b> Máximo: <b>32768</b>
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>32</b>

## Parâmetros de resposta

Código de status: **200**

Tabela 3-396 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
host_name	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>256</b>

Parâmetro	Tipo	Descrição
protect_status	String	Status de proteção. Seu valor pode ser: <ul style="list-style-type: none"> <li>● close</li> <li>● opened</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>
total_num	Long	Número total de WTPs estáticas Mínimo: <b>0</b> Máximo: <b>20000000</b>
data_list	Array of <b>HostProtectHistoryResponseInfo</b> objects	Lista de dados Comprimento da matriz: <b>0–20000</b>

**Tabela 3-397** HostProtectHistoryResponseInfo

Parâmetro	Tipo	Descrição
occur_time	Long	Tempo de detecção de WTP estática (ms) Mínimo: <b>0</b> Máximo: <b>4070880000000</b>
file_path	String	Caminho de arquivo adulterado Mínimo: <b>0</b> Máximo: <b>2000</b>
file_operation	String	Tipos de operações de arquivo <ul style="list-style-type: none"> <li>● add</li> <li>● delete</li> <li>● modify</li> <li>● attribute</li> <li>● unknown</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>
host_name	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>64</b>
host_ip	String	Endereço IP do servidor Mínimo: <b>0</b> Máximo: <b>64</b>

Parâmetro	Tipo	Descrição
process_id	String	ID do processo Mínimo: <b>0</b> Máximo: <b>8</b>
process_name	String	Nome do processo Mínimo: <b>0</b> Máximo: <b>200</b>
process_cmd	String	Linha de comando do processo Mínimo: <b>0</b> Máximo: <b>8191</b>

## Exemplo de solicitações

Consultar o status de WTP estática de um servidor em que o ID de destino é caa958ad-a481-4d46-b51e-6861b8864515, a hora de início é 1668563099000 e a hora de término é 1668563199000.

```
GET https://{endpoint}/v5/{project_id}/webtamper/static/protect-history

{
  "host_id" : "caa958ad-a481-4d46-b51e-6861b8864515",
  "start_time" : 1668563099000,
  "end_time" : 1668563199000,
  "limit" : 10,
  "offset" : 0
}
```

## Exemplo de respostas

**Código de status: 200**

Resposta bem-sucedida

```
{
  "host_name" : "ecs-ubuntu",
  "protect_status" : "opened",
  "total_num" : 1,
  "data_list" : [ {
    "occur_time" : 1668156691000,
    "file_path" : "/root/test/tamper/test.xml",
    "host_name" : "hss-test",
    "host_ip" : "192.168.5.98",
    "file_operation" : "add",
    "process_id" : "18672",
    "process_name" : "program1",
    "process_cmd" : "del test.xml"
  } ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.



## Java

Consultar o status de WTP estática de um servidor em que o ID de destino é caa958ad-a481-4d46-b51e-6861b8864515, a hora de início é 1668563099000 e a hora de término é 1668563199000.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListHostProtectHistoryInfoSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in
        // plaintext, which has great security risks. It is recommended that the AK and SK
        // be stored in ciphertext in configuration files or environment variables and
        // decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for
        // authentication. Before running this example, set environment variables
        // CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
            .build();

        ListHostProtectHistoryInfoRequest request = new
        ListHostProtectHistoryInfoRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withHostId("<host_id>");
        request.withStartTime("<start_time>L");
        request.withEndTime("<end_time>L");
        request.withLimit("<limit>");
        request.withOffset("<offset>");
        request.withHostName("<host_name>");
        request.withHostIp("<host_ip>");
        request.withFilePath("<file_path>");
        request.withFileOperation("<file_operation>");
        try {
            ListHostProtectHistoryInfoResponse response =
            client.listHostProtectHistoryInfo(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

## Python

Consultar o status de WTP estática de um servidor em que o ID de destino é caa958ad-a481-4d46-b51e-6861b8864515, a hora de início é 1668563099000 e a hora de término é 1668563199000.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
    # plaintext, which has great security risks. It is recommended that the AK and SK
    # be stored in ciphertext in configuration files or environment variables and
    # decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for
    # authentication. Before running this example, set environment variables
    # CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListHostProtectHistoryInfoRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.host_id = "<host_id>"
        request.start_time = <start_time>
        request.end_time = <end_time>
        request.limit = <limit>
        request.offset = <offset>
        request.host_name = "<host_name>"
        request.host_ip = "<host_ip>"
        request.file_path = "<file_path>"
        request.file_operation = "<file_operation>"
        response = client.list_host_protect_history_info(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Consultar o status de WTP estática de um servidor em que o ID de destino é caa958ad-a481-4d46-b51e-6861b8864515, a hora de início é 1668563099000 e a hora de término é 1668563199000.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)
```

```
func main() {
    // The AK and SK used for authentication are hard-coded or stored in
    // plaintext, which has great security risks. It is recommended that the AK and SK
    // be stored in ciphertext in configuration files or environment variables and
    // decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for
    // authentication. Before running this example, set environment variables
    // CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListHostProtectHistoryInfoRequest{}
    enterpriseProjectIdRequest := "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    hostIdRequest := "<host_id>"
    request.HostId = &hostIdRequest
    request.StartTime = int64(<start_time>)
    request.EndTime = int64(<end_time>)
    request.Limit = int32(<limit>)
    request.Offset = int32(<offset>)
    hostNameRequest := "<host_name>"
    request.HostName = &hostNameRequest
    hostIpRequest := "<host_ip>"
    request.HostIp = &hostIpRequest
    filePathRequest := "<file_path>"
    request.FilePath = &filePathRequest
    fileOperationRequest := "<file_operation>"
    request.FileOperation = &fileOperationRequest
    response, err := client.ListHostProtectHistoryInfo(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Resposta bem-sucedida

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.12.5 Consulta do status da WTP dinâmica para um servidor

### Função

Essa API é usada para consultar o status de WTP dinâmica de um servidor.

### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

### URI

GET /v5/{project\_id}/webtamper/rasp/protect-history

**Tabela 3-398** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>0</b> Máximo: <b>64</b>

**Tabela 3-399** Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Mínimo: <b>0</b> Máximo: <b>64</b>
host_id	Não	String	ID do servidor. Se esse parâmetro for deixado em branco, todos os servidores serão consultados. Mínimo: <b>0</b> Máximo: <b>128</b>
start_time	Sim	Long	Hora de início (ms) Mínimo: <b>0</b> Máximo: <b>4070880000000</b>
end_time	Sim	Long	Hora de término (ms) Mínimo: <b>0</b> Máximo: <b>4070880000000</b>
limit	Sim	Integer	Limite Mínimo: <b>0</b> Máximo: <b>100</b>

Parâmetro	Obrigatório	Tipo	Descrição
offset	Sim	Integer	Deslocamento Mínimo: <b>0</b> Máximo: <b>100</b>
alarm_level	Não	Integer	Gravidade do alarme. As opções são as seguintes: <ul style="list-style-type: none"> <li>● 1: baixo risco</li> <li>● 2: risco médio</li> <li>● 3: alto risco</li> <li>● 4: grave</li> </ul> Mínimo: <b>0</b> Máximo: <b>100</b>
severity	Não	String	Nível de ameaça. Seu valor pode ser: <ul style="list-style-type: none"> <li>● Security</li> <li>● Low: baixo risco</li> <li>● Medium: risco médio</li> <li>● High: alto risco</li> <li>● Critical</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>
protect_status	Não	String	Status de proteção. <ul style="list-style-type: none"> <li>● closed: desativada</li> <li>● opened: proteção ativada</li> </ul> Mínimo: <b>0</b> Máximo: <b>32</b>

## Parâmetros de solicitação

**Tabela 3-400** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token de usuário. Mínimo: <b>1</b> Máximo: <b>32768</b>

Parâmetro	Obrigatório	Tipo	Descrição
region	Sim	String	ID da região Mínimo: <b>0</b> Máximo: <b>32</b>

## Parâmetros de resposta

Código de status: **200**

Tabela 3-401 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Long	Número total de WTPs dinâmicas Mínimo: <b>0</b> Máximo: <b>200000</b>
data_list	Array of <a href="#">HostRaspProtectHistoryResponseInfo</a> objects	Lista de dados Comprimento da matriz: <b>0–200000</b>

Tabela 3-402 HostRaspProtectHistoryResponseInfo

Parâmetro	Tipo	Descrição
host_ip	String	Endereço IP do servidor Mínimo: <b>0</b> Máximo: <b>64</b>
host_name	String	Nome de servidor Mínimo: <b>0</b> Máximo: <b>64</b>
alarm_time	Long	Tempo de alarme de WTP dinâmica (ms) Mínimo: <b>0</b> Máximo: <b>4070880000000</b>
threat_type	String	Tipo de ameaça Mínimo: <b>0</b> Máximo: <b>64</b>

Parâmetro	Tipo	Descrição
alarm_level	Integer	Gravidade do alarme Mínimo: <b>0</b> Máximo: <b>100</b>
source_ip	String	Endereço IP de origem do servidor atacante Mínimo: <b>0</b> Máximo: <b>128</b>
attacked_url	String	URL da solicitação de ataque Mínimo: <b>0</b> Máximo: <b>2000</b>

## Exemplo de solicitações

Consultar o status de WTP dinâmica de um servidor em que o ID de destino é caa958ad-a481-4d46-b51e-6861b8864515, a hora de início é 1668563099000 e a hora de término é 1668563199000.

```
GET https://{endpoint}/v5/{project_id}/webtamper/rasp/protect-history

{
  "host_id" : "caa958ad-a481-4d46-b51e-6861b8864515",
  "start_time" : 1668563099000,
  "end_time" : 1668563199000,
  "limit" : 10,
  "offset" : 0
}
```

## Exemplo de respostas

**Código de status: 200**

Resposta bem-sucedida

```
{
  "total_num" : 1,
  "data_list" : [ {
    "host_ip" : "192.168.5.98",
    "host_name" : "hss-test",
    "alarm_level" : 2,
    "alarm_time" : 1668394634000,
    "attacked_url" : "/vulns/001-dir-1.jsp",
    "source_ip" : "10.100.30.200",
    "threat_type" : "Path Traversal"
  } ]
}
```

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

## Java

Consultar o status de WTP dinâmica de um servidor em que o ID de destino é caa958ad-a481-4d46-b51e-6861b8864515, a hora de início é 1668563099000 e a hora de término é 1668563199000.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

public class ListHostRaspProtectHistoryInfoSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in
        // plaintext, which has great security risks. It is recommended that the AK and SK
        // be stored in ciphertext in configuration files or environment variables and
        // decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for
        // authentication. Before running this example, set environment variables
        // CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR_REGION>"))
            .build();

        ListHostRaspProtectHistoryInfoRequest request = new
        ListHostRaspProtectHistoryInfoRequest();
        request.withEnterpriseProjectId("<enterprise_project_id>");
        request.withHostId("<host_id>");
        request.withStartTime("<start_time>L");
        request.withEndTime("<end_time>L");
        request.withLimit("<limit>");
        request.withOffset("<offset>");
        request.withAlarmLevel("<alarm_level>");
        request.withSeverity("<severity>");
        request.withProtectStatus("<protect_status>");
        try {
            ListHostRaspProtectHistoryInfoResponse response =
            client.listHostRaspProtectHistoryInfo(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```



## Python

Consultar o status de WTP dinâmica de um servidor em que o ID de destino é caa958ad-a481-4d46-b51e-6861b8864515, a hora de início é 1668563099000 e a hora de término é 1668563199000.

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
    # plaintext, which has great security risks. It is recommended that the AK and SK
    # be stored in ciphertext in configuration files or environment variables and
    # decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for
    # authentication. Before running this example, set environment variables
    # CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListHostRaspProtectHistoryInfoRequest()
        request.enterprise_project_id = "<enterprise_project_id>"
        request.host_id = "<host_id>"
        request.start_time = <start_time>
        request.end_time = <end_time>
        request.limit = <limit>
        request.offset = <offset>
        request.alarm_level = <alarm_level>
        request.severity = "<severity>"
        request.protect_status = "<protect_status>"
        response = client.list_host_rasp_protect_history_info(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

Consultar o status de WTP dinâmica de um servidor em que o ID de destino é caa958ad-a481-4d46-b51e-6861b8864515, a hora de início é 1668563099000 e a hora de término é 1668563199000.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
```

```
// The AK and SK used for authentication are hard-coded or stored in
plaintext, which has great security risks. It is recommended that the AK and SK
be stored in ciphertext in configuration files or environment variables and
decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    Build()

client := hss.NewHssClient(
    hss.HssClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ListHostRaspProtectHistoryInfoRequest{
    enterpriseProjectIdRequest:= "<enterprise_project_id>"
    request.EnterpriseProjectId = &enterpriseProjectIdRequest
    requestIdRequest:= "<host_id>"
    request.HostId = &hostIdRequest
    request.StartTime = int64(<start_time>)
    request.EndTime = int64(<end_time>)
    request.Limit = int32(<limit>)
    request.Offset = int32(<offset>)
    alarmLevelRequest:= int32(<alarm_level>)
    request.AlarmLevel = &alarmLevelRequest
    severityRequest:= "<severity>"
    request.Severity = &severityRequest
    protectStatusRequest:= "<protect_status>"
    request.ProtectStatus = &protectStatusRequest
    response, err := client.ListHostRaspProtectHistoryInfo(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Resposta bem-sucedida

## Códigos de erro

Consulte [Códigos de erro](#).

## 3.13 Gerenciamento de tags

### 3.13.1 Criação de tags em lotes

#### Função

Essa API é usada para criar tags em lotes.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

POST /v5/{project\_id}/{resource\_type}/{resource\_id}/tags/create

Tabela 3-403 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>
resource_type	Sim	String	Tipo de recurso definido pelo TMS. Quando o HSS chama a API, o tipo de recurso é HSS. Mínimo: <b>1</b> Máximo: <b>64</b>
resource_id	Sim	String	ID do recurso definido pelo TMS. Quando o HSS chama a API, o ID do recurso é o ID da cota. Mínimo: <b>0</b> Máximo: <b>128</b>

## Parâmetros de solicitação

**Tabela 3-404** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>32</b> Máximo: <b>512</b>
Content-Type	Não	String	Valor padrão: application/json; charset=utf-8 Mínimo: <b>0</b> Máximo: <b>128</b>

**Tabela 3-405** Parâmetros do corpo da solicitação

Parâmetro	Obrigatório	Tipo	Descrição
tags	Sim	Array of <b>ResourceTagInfo</b> objects	Lista de tags Comprimento da matriz: <b>0-1024</b>

**Tabela 3-406** ResourceTagInfo

Parâmetro	Obrigatório	Tipo	Descrição
key	Sim	String	Chave. Pode conter até 128 caracteres Unicode. O key não pode ser deixado em branco. Mínimo: <b>1</b> Máximo: <b>128</b>
value	Sim	String	Valor Mínimo: <b>1</b> Máximo: <b>128</b>

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Criar uma chave de tag TESTKEY20220831190155 (o valor da tag é 2) e um teste de chave de tag (o valor da tag é hss).

```
POST https://{endpoint}/v5/05e1e8b7ba8010dd2f80c01070a8d4cd/hss/
fbaa9aca-2b5f-11ee-8c64-fa163e139e02/tags/create
```

```
{
  "tags" : [ {
    "key" : "TESTKEY20220831190155",
    "value" : "2"
  }, {
    "key" : "test",
    "value" : "hss"
  } ]
}
```

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

Criar uma chave de tag TESTKEY20220831190155 (o valor da tag é 2) e um teste de chave de tag (o valor da tag é hss).

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.hss.v5.region.HssRegion;
import com.huaweicloud.sdk.hss.v5.*;
import com.huaweicloud.sdk.hss.v5.model.*;

import java.util.List;
import java.util.ArrayList;

public class BatchCreateTagsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in
plaintext, which has great security risks. It is recommended that the AK and SK
be stored in ciphertext in configuration files or environment variables and
decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for
authentication. Before running this example, set environment variables
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");

        ICredential auth = new BasicCredentials()
            .withAk(ak)
            .withSk(sk);

        HssClient client = HssClient.newBuilder()
            .withCredential(auth)
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))
```

```
        .build();
BatchCreateTagsRequest request = new BatchCreateTagsRequest();
BatchCreateTagsRequestInfo body = new BatchCreateTagsRequestInfo();
List<ResourceTagInfo> listbodyTags = new ArrayList<>();
listbodyTags.add(
    new ResourceTagInfo()
        .withKey("TESTKEY20220831190155")
        .withValue("2")
);
listbodyTags.add(
    new ResourceTagInfo()
        .withKey("test")
        .withValue("hss")
);
body.withTags(listbodyTags);
request.withBody(body);
try {
    BatchCreateTagsResponse response = client.batchCreateTags(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

## Python

Criar uma chave de tag TESTKEY20220831190155 (o valor da tag é 2) e um teste de chave de tag (o valor da tag é hss).

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
    be stored in ciphertext in configuration files or environment variables and
    decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for
    authentication. Before running this example, set environment variables
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchCreateTagsRequest()
        listTagsbody = [
            ResourceTagInfo(
                key="TESTKEY20220831190155",
                value="2"
            )
        ]
        body = BatchCreateTagsRequestInfo()
        body.with_tags(listTagsbody)
        request.with_body(body)
        try:
            response = client.batch_create_tags(request)
            print(response.to_dict())
        except exceptions.ServiceResponseException as e:
            print(e.get_http_status_code())
            print(e.get_request_id())
            print(e.get_error_code())
            print(e.get_error_msg())
    except exceptions.ConnectionException as e:
        print(e.get_error_msg())
    except exceptions.RequestTimeoutException as e:
        print(e.get_error_msg())
```

```
    ),
    ResourceTagInfo(
        key="test",
        value="hss"
    )
]
request.body = BatchCreateTagsRequestInfo(
    tags=listTagsbody
)
response = client.batch_create_tags(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

## Go

Criar uma chave de tag TESTKEY20220831190155 (o valor da tag é 2) e um teste de chave de tag (o valor da tag é hss).

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
    be stored in ciphertext in configuration files or environment variables and
    decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for
    authentication. Before running this example, set environment variables
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchCreateTagsRequest{}
    var listTagsbody = []model.ResourceTagInfo{
        {
            Key: "TESTKEY20220831190155",
            Value: "2",
        },
        {
            Key: "test",
            Value: "hss",
        },
    }
    request.Body = &model.BatchCreateTagsRequestInfo{
        Tags: listTagsbody,
    }
    response, err := client.BatchCreateTags(request)
```

```
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Bem-sucedido
400	Parâmetro inválido.
401	Falha na autenticação.
403	Permissão insuficiente.
404	Recursos não encontrados.
500	Erro de sistema.

## Códigos de erro

Consulte [Códigos de erro](#).

### 3.13.2 Exclusão de uma tag de recurso

#### Função

Essa API é usada para excluir uma tag de um recurso.

#### Método de chamada

Para obter detalhes, consulte [Chamada de APIs](#).

#### URI

DELETE /v5/{project\_id}/{resource\_type}/{resource\_id}/tags/{key}



**Tabela 3-407** Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto Mínimo: <b>1</b> Máximo: <b>256</b>
resource_type	Sim	String	Tipo de recurso definido pelo TMS. Quando o HSS chama a API, o tipo de recurso é HSS. Mínimo: <b>1</b> Máximo: <b>64</b>
resource_id	Sim	String	ID do recurso definido pelo TMS. Quando o HSS chama a API, o ID do recurso é o ID da cota. Mínimo: <b>0</b> Máximo: <b>128</b>
key	Sim	String	Chave a ser excluída Mínimo: <b>1</b> Máximo: <b>256</b>

## Parâmetros de solicitação

**Tabela 3-408** Parâmetros de cabeçalho de solicitação

Parâmetro	Obrigatório	Tipo	Descrição
X-Auth-Token	Sim	String	Token do usuário. Ele pode ser obtido chamando a API do IAM usada para obter um token de usuário. O valor de X-Subject-Token no cabeçalho da resposta é um token. Mínimo: <b>32</b> Máximo: <b>512</b>

## Parâmetros de resposta

Nenhum

## Exemplo de solicitações

Excluir a tag cuja chave é abc, project\_id é 94b5266c14ce489fa6549817f032dc61, resource\_type é hss e resource\_id é 2acc46ee-34c2-40c2-8060-dc652e6c672a.

```
DELETE https://{endpoint}/v5/94b5266c14ce489fa6549817f032dc61/hss/  
2acc46ee-34c2-40c2-8060-dc652e6c672a/tags/abc
```

## Exemplo de respostas

Nenhum

## Código de amostra do SDK

O código de amostra do SDK é o seguinte.

### Java

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;  
import com.huaweicloud.sdk.hss.v5.region.HssRegion;  
import com.huaweicloud.sdk.hss.v5.*;  
import com.huaweicloud.sdk.hss.v5.model.*;  
  
public class DeleteResourceInstanceTagSolution {  
  
    public static void main(String[] args) {  
        // The AK and SK used for authentication are hard-coded or stored in  
plaintext, which has great security risks. It is recommended that the AK and SK  
be stored in ciphertext in configuration files or environment variables and  
decrypted during use to ensure security.  
        // In this example, AK and SK are stored in environment variables for  
authentication. Before running this example, set environment variables  
CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
        String ak = System.getenv("CLOUD_SDK_AK");  
        String sk = System.getenv("CLOUD_SDK_SK");  
  
        ICredential auth = new BasicCredentials()  
            .withAk(ak)  
            .withSk(sk);  
  
        HssClient client = HssClient.newBuilder()  
            .withCredential(auth)  
            .withRegion(HssRegion.valueOf("<YOUR REGION>"))  
            .build();  
        DeleteResourceInstanceTagRequest request = new  
DeleteResourceInstanceTagRequest();  
        try {  
            DeleteResourceInstanceTagResponse response =  
client.deleteResourceInstanceTag(request);  
            System.out.println(response.toString());  
        } catch (ConnectionException e) {  
            e.printStackTrace();  
        } catch (RequestTimeoutException e) {  
            e.printStackTrace();  
        } catch (ServiceResponseException e) {  
            e.printStackTrace();  
            System.out.println(e.getHttpStatusCode());  
            System.out.println(e.getRequestId());  
            System.out.println(e.getErrorCode());  
            System.out.println(e.getErrorMsg());  
        }  
    }  
}
```

## Python

```
# coding: utf-8

from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkhss.v5.region.hss_region import HssRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkhss.v5 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
    be stored in ciphertext in configuration files or environment variables and
    decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for
    authentication. Before running this example, set environment variables
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = __import__('os').getenv("CLOUD_SDK_AK")
    sk = __import__('os').getenv("CLOUD_SDK_SK")

    credentials = BasicCredentials(ak, sk) \

    client = HssClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(HssRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteResourceInstanceTagRequest()
        response = client.delete_resource_instance_tag(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

## Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    hss "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/hss/v5/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in
    plaintext, which has great security risks. It is recommended that the AK and SK
    be stored in ciphertext in configuration files or environment variables and
    decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for
    authentication. Before running this example, set environment variables
    CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        Build()

    client := hss.NewHssClient(
        hss.HssClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
```

```
Build()  
  
request := &model.DeleteResourceInstanceTagRequest{}  
response, err := client.DeleteResourceInstanceTag(request)  
if err == nil {  
    fmt.Printf("%+v\n", response)  
} else {  
    fmt.Println(err)  
}  
}
```

## Mais

Para obter o código de amostra do SDK de mais linguagens de programação, consulte a guia Código de amostra no [API Explorer](#). O código de amostra do SDK pode ser gerado automaticamente.

## Códigos de status

Código de status	Descrição
200	Bem-sucedido
400	Parâmetro inválido.
401	Falha na autenticação.
403	Permissão insuficiente.
404	Recursos não encontrados.
500	Erro de sistema.

## Códigos de erro

Consulte [Códigos de erro](#).

# A Apêndices

## A.1 Código de status

Código de status	Status	Descrição
200	OK	Processamento da solicitação bem-sucedido.
400	Bad Request	Parâmetros de solicitação inválidos.
500	Internal Server Error	Erro de serviço interno.

## A.2 Códigos de erro

Se um código de erro começando com APIGW for retornado depois que você chamar uma API, corrija a falha consultando as instruções fornecidas em [Códigos de erro do API Gateway](#).

Código de status	Códigos de erro	Mensagem de erro	Descrição	Solução
400	HSS.0001	invalid param error	erro de parâmetro inválido	Verifique o parâmetro de entrada
500	HSS.0041	Query host extend info error	Erro de informações do host de consulta	Verifique o parâmetro de entrada

# B Histórico de alterações

Data	Descrição de alterações
27/10/2023	<p>Esta edição é o 5º lançamento oficial.</p> <p>Adição de:</p> <ul style="list-style-type: none"><li>● 3.1.6.1 Consulta da lista de endereços IP bloqueados</li><li>● 3.1.6.2 Desbloqueio de um endereço IP bloqueado</li><li>● 3.1.6.3 Consulta da lista de arquivos isolados</li><li>● 3.1.6.4 Restauração de arquivos isolados</li><li>● 3.1.9.1 Consulta da lista de imagens no repositório de imagens do SWR</li><li>● 3.1.9.2 Verificação de imagens no repositório de imagens em lotes</li><li>● 3.1.9.3 Consulta de informações de vulnerabilidade de imagem</li><li>● 3.1.9.4 Informações de CVE correspondentes à vulnerabilidade</li><li>● 3.1.9.5 Sincronização da lista de imagens do SWR</li><li>● 3.1.9.6 Consulta da lista de resultados de detecção de configuração de segurança de imagem</li><li>● 3.1.9.7 Consulta da lista de itens de verificação de um item de configuração de segurança especificado de uma imagem</li><li>● 3.1.9.8 Consulta do relatório de verificação da configuração de espelho</li><li>● 3.1.11.5 Consulta de uma política de verificação de vulnerabilidades</li></ul>

Data	Descrição de alterações
	<ul style="list-style-type: none"> <li>● 3.1.11.6 Modificação de uma política de verificação de vulnerabilidades</li> <li>● 3.1.11.7 Consulta de estatísticas de gerenciamento de vulnerabilidades</li> </ul>
25/07/2023	<p>Esta edição é o 4º lançamento oficial.</p> <p>Adição de:</p> <ul style="list-style-type: none"> <li>● 3.1.1.1 Consulta da lista de middleware</li> <li>● 3.1.1.2 Consulta da lista de servidores de um middleware especificado</li> <li>● 3.1.8.4 Consulta de informações de vulnerabilidade sobre um servidor</li> </ul>
14/12/2022	<p>Esta edição é o 3º lançamento oficial.</p> <p>Adição de APIs suportadas.</p>
31/10/2022	<p>Esta edição é o 2º lançamento oficial.</p> <p>Otimização da descrição sobre APIs.</p>
30/06/2022	<p>Esta edição é o 1º lançamento oficial.</p>