Host Security Service

API Reference

Edição 01

Data 30-12-2022

HUAWEI TECHNOLOGIES CO., LTD.

Marcas registadas e permissões


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

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 prevenir ameaças facilmente.

Este documento descreve como usar interfaces de programação de aplicativos (APIs) para executar operações no HSS.

Se você planeja acessar o HSS por meio de uma API, certifique-se de estar familiarizado com os conceitos do HSS. Para obter detalhes, consulte **Visão geral de serviço**.

1.2 Pontos de extremidade

Um ponto de extremidade é o **request address** 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
AP-Bangkok	ap-southeast-2	hss.ap-southeast-2.myhuaweicloud.com	HTTPS
AP-Singapore	ap-southeast-3	hss.ap-southeast-3.myhuaweicloud.com	HTTPS

Um ponto de extremidade é o **request address** para chamar uma API. Os pontos de extremidade variam de acordo com os serviços e as regiões. Para obter os pontos de extremidade de todos os serviços, consulte **Regiões e pontos de extremidade**.

1.3 Limitações e restrições

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

Veja as descrições de APIs específicas.

1.4 Conceitos básicos

- Conta

  Um domínio é criado após o seu registro. O domínio 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 utilizada para realizar a gestão de rotina. Para fins de segurança, crie usuários do IAM e conceda a eles permissões para o gerenciamento de rotina.
- Conta

  Um domínio é criado após o registro bem-sucedido. O domínio 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 utilizada para realizar a gestão 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 são necessários para a autenticação da API.
- **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 são necessários para a autenticação da API.
- Região

  As regiões são divididas com base na localização geográfica e na latência da rede. 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 universal para locatários comuns. Uma região dedicada fornece serviços do mesmo tipo apenas ou para locatários específicos.
- Zona de disponibilidade (AZ)

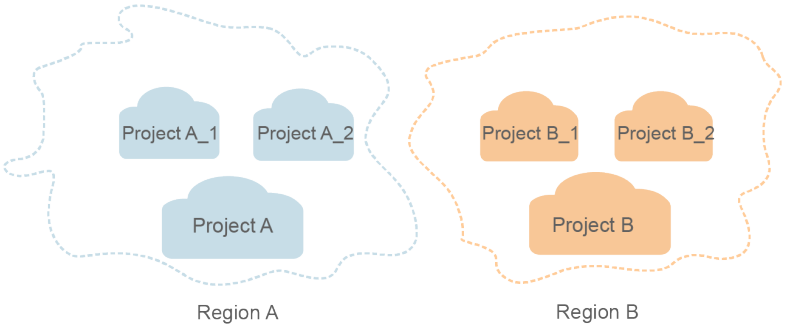
  Uma AZ compreende um ou vários centros de dados físicos equipados com instalações independentes de ventilação, incêndio, água e eletricidade. Computação, rede, armazenamento e outros recursos em uma AZ são logicamente divididos em vários

clusters. As AZs dentro de uma região são conectadas usando fibras ópticas de alta velocidade para suportar sistemas de alta disponibilidade entre AZs.

- Projeto

  Projetos agrupam e isolam recursos de computação, armazenamento e rede em regiões físicas. Um projeto padrão é fornecido para cada região, e subprojetos podem ser criados em cada projeto padrão. Os usuários podem receber permissões para acessar todos os recursos em um projeto específico. Para um controle de acesso mais refinado, crie subprojetos em um projeto e compre recursos nos subprojetos. Em seguida, os usuários podem 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 corporativo, 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 **obter 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 APIs.

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 APIs usam HTTPS.

- **Endpoint**:

  Nome de domínio ou endereço IP do servidor que possui o serviço REST. O ponto de extremidade varia entre serviços em diferentes regiões. Pode ser obtido em **Regiões e pontos de extremidade**.

  Por exemplo, o ponto de extremidade do IAM na região **CN North-Beijing1** é **iam.cn-north-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**.

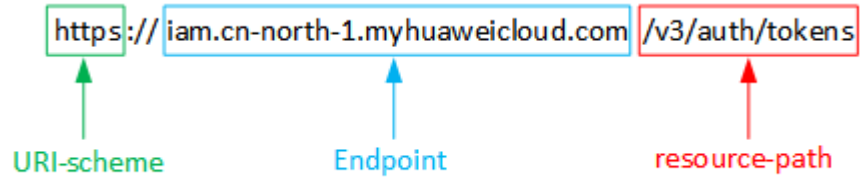
- **query-string**:

  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 o token IAM na região **CN North-Beijing1**, obter o ponto de extremidade do IAM (**iam.cn-north-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.cn-north-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 pontos de extremidade 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.cn-north-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 **application/json**. Outros valores deste campo serão fornecidos para 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 APIs 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.cn-north-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 APIs. Algumas APIs não exigem o corpo da solicitação, como as APIs 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*** como o nome de um usuário, ***domainname*** como o nome da conta à qual o usuário pertence, ******** como a senha de login do usuário e ***xxxxxxxxxxxxxxxxxx*** como o nome do projeto. Você pode obter mais informações sobre projetos em **Regiões e pontos de extremidade** 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, consulte **Obtenção de um token de usuário**.

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

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



```
        "scope": {
            "project": {
                "name": "xxxxxxxxxxxxxxxxx"
            }
        }
    }
}
```

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 APIs.

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 AK/SK: as solicitações são criptografadas usando pares 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 de nível de projeto é necessário para chamar essa API. Ao chamar essa API, defina **auth.scope** para **project** no corpo da solicitação. Exemplo:

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


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 APIs. Por exemplo, se o token é **ABCDEFJ....**, **X-Auth-Token: ABCDEFJ....** pode ser adicionado a uma solicitação da seguinte forma:

```
POST https://iam.cn-north-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 SDKs fornecidos pelos serviços.

2.3 Resposta

Código de estado

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** é retornado para chamar a API usada para **obter um token de usuário**, a solicitação foi 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. Esse 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

(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**. Por uma questão de espaço, apenas parte do conteúdo é exibido 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. A seguir, mostra 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 da linha de base

3.1.1 Consulta da lista de resultados de detecção de senha fraca

Função

Essa API é usada para consultar a lista de resultados de detecção de senha fracos.

URI

GET /v5/{project_id}/baseline/weak-password-users

Tabela 3-1 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: **20** Máximo: **64**

Tabela 3-2 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Mínimo: **0** Máximo: **64**
host_name	Não	String	Nome do servidor Mínimo: **0** Máximo: **256**

Parâmetro	Obrigatório	Tipo	Descrição
host_ip	Não	String	Endereço IP do servidor Mínimo: **0** Máximo: **256**
user_name	Não	String	Nome da conta usando uma senha fraca Mínimo: **0** Máximo: **32**
host_id	Não	String	ID do host. Se esse parâmetro não for especificado, todos os hosts de um locatário serão consultados. Mínimo: **0** Máximo: **64**
limit	Não	Integer	Número de registros em cada página Mínimo: **0** Máximo: **200** Padrão: **10**
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: **0** Máximo: **100000** Padrão: **0**

Solicitação dos parâmetros

Tabela 3-3 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 **X-Subject-Token** no cabeçalho da resposta é o token do usuário. Mínimo: **32** Máximo: **2097152**

Parâmetros de resposta

Código de estado: 200

Tabela 3-4 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Long	Número total de senhas fracas Mínimo: **0** Máximo: **2147483647**
data_list	Array of **WeakPwdListInfoResponseInfo** objects	Lista de senhas fracas

Tabela 3-5 WeakPwdListInfoResponseInfo

Parâmetro	Tipo	Descrição
host_id	String	ID do servidor Mínimo: **0** Máximo: **64**
host_name	String	Nome do servidor Mínimo: **0** Máximo: **256**
host_ip	String	Endereço IP do servidor Mínimo: **0** Máximo: **256**
weak_pwd_accounts	Array of **WeakPwdAccountInfoResponseInfo** objects	Lista de contas com senhas fracas

Tabela 3-6 WeakPwdAccountInfoResponseInfo

Parâmetro	Tipo	Descrição
user_name	String	Nome de contas com senhas fracas Mínimo: **0** Máximo: **32**

Parâmetro	Tipo	Descrição
service_type	String	Tipo de conta Mínimo: **0** Máximo: **32**
duration	Integer	Período de validade de uma senha fraca, em dias. Mínimo: **0** Máximo: **2147483647**

Exemplos de solicitações

Nenhum

Exemplo de respostas

Nenhum

Códigos de estado

Código de estado	Descrição
200	A lista de resultados de detecção de senha fraca é retornada.

Códigos de erro

Consulte **Códigos de erro**.

3.1.2 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.

URI

GET /v5/{project_id}/baseline/password-complexity

Tabela 3-7 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: **1** Máximo: **256**

Tabela 3-8 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Mínimo: **0** Máximo: **256**
host_name	Não	String	Nome do servidor Mínimo: **0** Máximo: **128**
host_ip	Não	String	Endereço IP do servidor Mínimo: **0** Máximo: **128**
host_id	Não	String	ID do servidor. Se esse parâmetro não for especificado, todos os hosts de um locatário serão consultados. Mínimo: **0** Máximo: **128**
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é **10**. Mínimo: **0** Máximo: **200** Padrão: **10**
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: **0** Máximo: **100000** Padrão: **0**

Solicitação dos parâmetros

Tabela 3-9 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 o token do usuário. Mínimo: **1** Máximo: **32768**

Parâmetros de resposta

Código de estado: 200

Tabela 3-10 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Long	Número total de políticas de complexidade de senha Mínimo: **0** Máximo: **2147483647**
data_list	Array of **PwdPolicyInfoResponseInfo** objects	Lista de detecção de política de complexidade de senha

Tabela 3-11 PwdPolicyInfoResponseInfo

Parâmetro	Tipo	Descrição
host_id	String	ID do servidor (exibido quando o cursor é colocado em um nome de servidor) Mínimo: **0** Máximo: **64**
host_name	String	Nome do servidor Mínimo: **0** Máximo: **256**

Parâmetro	Tipo	Descrição
host_ip	String	Endereço IP do servidor Mínimo: **0** Máximo: **256**
min_length	Boolean	Comprimento mínimo da senha
uppercase_letter	Boolean	Letra maiúscula
lowercase_letter	Boolean	Letra minúscula
number	Boolean	Painel
special_character	Boolean	Caracteres especiais
suggestion	String	Sugestão de modificação Mínimo: **0** Máximo: **65534**

Exemplos de solicitações

Nenhum

Exemplo de respostas

Nenhum

Códigos de estado

Código de estado	Descrição
200	Resposta bem-sucedida

Códigos de erro

Consulte **Códigos de erro**.

3.1.3 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 locatário.

URI

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

Tabela 3-12 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: **1** Máximo: **256**

Tabela 3-13 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Mínimo: **0** Máximo: **256**
check_type	Não	String	Nome da linha de base Mínimo: **0** Máximo: **256**
severity	Não	String	Nível de risco. As opções são as seguintes: ● Segurança ● Baixo ● Médio ● Alto Mínimo: **1** Máximo: **32**
standard	Não	String	Tipo padrão. As opções são as seguintes: ● **cn_standard**: padrão de certificação de segurança ● **hw_standard**: padrão da Huawei ● **qt_standard**: padrão de Qingteng Mínimo: **1** Máximo: **32**
host_id	Não	String	ID do servidor Mínimo: **0** Máximo: **128**

Parâmetro	Obrigatório	Tipo	Descrição
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é **10**. Mínimo: **0** Máximo: **200** Padrão: **10**
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: **0** Máximo: **100000** Padrão: **0**

Solicitação dos parâmetros

Tabela 3-14 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 o token do usuário. Mínimo: **1** Máximo: **32768**

Parâmetros de resposta

Código de estado: 200

Tabela 3-15 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Long	Número total de registros Mínimo: **0** Máximo: **2147483647**

Parâmetro	Tipo	Descrição
data_list	Array of **SecurityCheckInfoResponseInfo** objects	Lista de resultados da verificação de configuração do servidor

Tabela 3-16 SecurityCheckInfoResponseInfo

Parâmetro	Tipo	Descrição
severity	String	Nível de risco. As opções são as seguintes: ● Baixo ● Médio ● Alto Mínimo: **1** Máximo: **32**
check_name	String	Nome da linha de base Mínimo: **0** Máximo: **256**
check_type	String	Tipo de linha de base Mínimo: **0** Máximo: **256**
standard	String	Tipo padrão. As opções são as seguintes: ● **cn_standard**: padrão de certificação de segurança ● **hw_standard**: padrão da Huawei ● **qt_standard**: padrão de Qingteng Mínimo: **1** Máximo: **32**
check_rule_num	Integer	Número de itens de verificação Mínimo: **0** Máximo: **2097152**
failed_rule_num	Integer	Número de elementos de risco Mínimo: **0** Máximo: **2097152**
host_num	Integer	Número de servidores afetados Mínimo: **0** Máximo: **2097152**

Parâmetro	Tipo	Descrição
scan_time	Long	Hora da última varredura Mínimo: **0** Máximo: **2097152**
check_type_desc	String	Descrição da linha de base Mínimo: **0** Máximo: **65534**

Exemplos de solicitações

Nenhum

Exemplo de respostas

Nenhum

Códigos de estado

Código de estado	Descrição
200	A lista de resultados de uma verificação de configuração de segurança do servidor é retornada.

Códigos de erro

Consulte **Códigos de erro**.

3.1.4 Consulta do resultado da verificação de um item de configuração de segurança especificado

Função

Essa API é usada para consultar o resultado da verificação de um item de configuração de segurança especificado.

URI

GET /v5/{project_id}/baseline/risk-config/{check_type}/detail

Tabela 3-17 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: **20** Máximo: **64**
check_type	Sim	String	Nome da linha de base Mínimo: **0** Máximo: **256**

Tabela 3-18 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Mínimo: **0** Máximo: **64**
standard	Sim	String	Tipo padrão. As opções são as seguintes: ● **cn_standard**: padrão de certificação de segurança ● **hw_standard**: padrão da Huawei ● **qt_standard**: padrão de Qingteng Mínimo: **0** Máximo: **32**
host_id	Não	String	ID do host. Se esse parâmetro não for especificado, todos os hosts de um locatário serão consultados. Mínimo: **0** Máximo: **64**
limit	Não	Integer	Número de registros em cada página Mínimo: **0** Máximo: **200** Padrão: **10**

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 **0**. Mínimo: **0** Máximo: **100000** Padrão: **0**

Solicitação dos parâmetros

Tabela 3-19 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 **X-Subject-Token** no cabeçalho da resposta é o token do usuário. Mínimo: **32** Máximo: **2097152**

Parâmetros de resposta

Código de estado: 200

Tabela 3-20 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
severity	String	Nível de risco. As opções são as seguintes: ● Baixo ● Médio ● Alto Mínimo: **0** Máximo: **65534**
check_type_desc	String	Descrição da linha de base Mínimo: **0** Máximo: **65534**

Parâmetro	Tipo	Descrição
check_rule_num	Integer	Número total de itens de verificação Mínimo: **0** Máximo: **2147483647**
failed_rule_num	Integer	Número de itens de verificação com falha Mínimo: **0** Máximo: **2147483647**
passed_rule_num	Integer	Número de itens de verificação passados Mínimo: **0** Máximo: **2147483647**
ignored_rule_num	Integer	Número de itens de verificação ignorados Mínimo: **0** Máximo: **2147483647**
host_num	Long	Número de servidores afetados Mínimo: **0** Máximo: **2147483647**

Exemplos de solicitações

Nenhum

Exemplo de respostas

Nenhum

Códigos de estado

Código de estado	Descrição
200	O resultado da verificação de um item de configuração de segurança especificado é retornado.

Códigos de erro

Consulte **Códigos de erro**.

3.1.5 Consulta da lista de itens de verificação de um item de configuração de segurança especificada

Função

Essa API é usada para consultar a lista de itens de verificação de um item de configuração de segurança especificado.

URI

GET /v5/{project_id}/baseline/risk-config/{check_type}/check-rules

Tabela 3-21 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: **20** Máximo: **64**
check_type	Sim	String	Nome da linha de base Mínimo: **0** Máximo: **256**

Tabela 3-22 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Mínimo: **0** Máximo: **64**
standard	Sim	String	Tipo padrão. As opções são as seguintes: ● **cn_standard**: padrão de certificação de segurança ● **hw_standard**: padrão da Huawei ● **qt_standard**: padrão de Qingteng Mínimo: **0** Máximo: **32**

Parâmetro	Obrigatório	Tipo	Descrição
result_type	Não	String	Tipo de resultado. As opções são as seguintes: ● safe ● unhandled ● ignored Padrão: **unhandled** Mínimo: **0** Máximo: **64**
check_rule_name	Não	String	Verifique o nome do item. A correspondência difusa é suportada. Mínimo: **0** Máximo: **2048**
severity	Não	String	Nível de risco. As opções são as seguintes: ● Security ● Low ● Medium ● High ● Critical Mínimo: **0** Máximo: **255**
host_id	Não	String	ID do host. Se esse parâmetro não for especificado, todos os hosts de um locatário serão consultados. Mínimo: **0** Máximo: **64**
limit	Não	Integer	Número de registros em cada página Mínimo: **0** Máximo: **200** Padrão: **10**
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: **0** Máximo: **100000** Padrão: **0**

Solicitação dos parâmetros

Tabela 3-23 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 **X-Subject-Token** no cabeçalho da resposta é o token do usuário. Mínimo: **32** Máximo: **2097152**

Parâmetros de resposta

Código de estado: 200

Tabela 3-24 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Long	Total dos riscos Mínimo: **0** Máximo: **9223372036854775807**
data_list	Array of **CheckRuleRiskInfoResponseInfo** objects	Lista de dados

Tabela 3-25 CheckRuleRiskInfoResponseInfo

Parâmetro	Tipo	Descrição
severity	String	Nível de risco. As opções são as seguintes: ● Low ● Medium ● High Mínimo: **0** Máximo: **255**

Parâmetro	Tipo	Descrição
check_type	String	Nome da linha de base Mínimo: **0** Máximo: **255**
standard	String	Tipo padrão. As opções são as seguintes: ● **cn_standard**: padrão de certificação de segurança ● **hw_standard**: padrão da Huawei ● **qt_standard**: padrão de Qingteng Mínimo: **0** Máximo: **32**
check_rule_name	String	Item de verificação Mínimo: **0** Máximo: **2048**
check_rule_id	String	Verificar ID do item Mínimo: **0** Máximo: **255**
host_num	Integer	Número de servidores afetados Mínimo: **0** Máximo: **2147483647**
scan_result	String	Resultado da detecção. As opções são as seguintes: ● pass ● failed Mínimo: **0** Máximo: **64**
status	String	Estado. As opções são as seguintes: ● safe ● ignored ● unhandled Mínimo: **0** Máximo: **64**

Exemplos de solicitações

Nenhum

Exemplo de respostas

Nenhum

Códigos de estado

Código de estado	Descrição
200	A lista de itens de verificação de um item de configuração de segurança especificado é retornada.

Códigos de erro

Consulte **Códigos de erro**.

3.1.6 Consulta da lista de servidores afetados de um item de configuração de segurança especificado

Função

Essa API é usada para consultar a lista de servidores afetados de um item de configuração de segurança especificado.

URI

GET /v5/{project_id}/baseline/risk-config/{check_type}/hosts

Tabela 3-26 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: **20** Máximo: **64**
check_type	Sim	String	Nome da linha de base Mínimo: **0** Máximo: **256**

Tabela 3-27 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Mínimo: **0** Máximo: **64**

Parâmetro	Obrigatório	Tipo	Descrição
standard	Sim	String	Tipo padrão. As opções são as seguintes: ● **cn_standard**: padrão de certificação de segurança ● **hw_standard**: padrão da Huawei ● **qt_standard**: padrão de Qingteng Mínimo: **0** Máximo: **32**
host_name	Não	String	Nome do servidor Mínimo: **0** Máximo: **256**
host_ip	Não	String	Endereço IP do servidor Mínimo: **0** Máximo: **256**
limit	Não	Integer	Número de registros em cada página Mínimo: **0** Máximo: **200** Padrão: **10**
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: **0** Máximo: **100000** Padrão: **0**

Solicitação dos parâmetros

Tabela 3-28 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 **X-Subject-Token** no cabeçalho da resposta é o token do usuário. Mínimo: **32** Máximo: **2097152**

Parâmetros de resposta

Código de estado: 200

Tabela 3-29 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Long	Volume total de dados Mínimo: **0** Máximo: **2147483647**
data_list	Array of **SecurityCheckHostInfoResponseInfo** objects	Lista de dados

Tabela 3-30 SecurityCheckHostInfoResponseInfo

Parâmetro	Tipo	Descrição
host_id	String	ID do servidor Mínimo: **0** Máximo: **64**
host_name	String	Nome do servidor Mínimo: **0** Máximo: **256**
host_public_ip	String	Endereço IP público do servidor Mínimo: **0** Máximo: **128**

Parâmetro	Tipo	Descrição
host_private_ip	String	Endereço IP privado do servidor Mínimo: **0** Máximo: **256**
scan_time	Long	Tempo de varredura Mínimo: **0** Máximo: **9223372036854775807**
failed_num	Integer	Número de elementos de risco Mínimo: **0** Máximo: **2147483647**
passed_num	Integer	Número de itens passados Mínimo: **0** Máximo: **2147483647**

Exemplos de solicitações

Nenhum

Exemplo de respostas

Nenhum

Códigos de estado

Código de estado	Descrição
200	A lista de servidores afetados por um item de configuração de segurança especificado é retornada.

Códigos de erro

Consulte **Códigos de erro**.

3.1.7 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.

URI

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

Tabela 3-31 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: **20** Máximo: **64**

Tabela 3-32 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Mínimo: **0** Máximo: **64**
check_type	Sim	String	Nome da linha de base Mínimo: **0** Máximo: **255**
check_rule_id	Sim	String	Verificar ID do item Mínimo: **0** Máximo: **255**
standard	Sim	String	Tipo padrão. As opções são as seguintes: ● **cn_standard**: padrão de certificação de segurança ● **hw_standard**: padrão da Huawei ● **qt_standard**: padrão de Qingteng Mínimo: **0** Máximo: **32**
host_id	Não	String	ID do host Mínimo: **0** Máximo: **64**

Solicitação dos parâmetros

Tabela 3-33 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 **X-Subject-Token** no cabeçalho da resposta é o token do usuário. Mínimo: **32** Máximo: **2097152**

Parâmetros de resposta

Código de estado: 200

Tabela 3-34 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
description	String	Descrição Mínimo: **0** Máximo: **2048**
reference	String	Cenário Mínimo: **0** Máximo: **255**
audit	String	Descrição da auditoria Mínimo: **0** Máximo: **65534**
remediation	String	Sugestão de modificação Mínimo: **0** Máximo: **65534**
check_info_list	Array of **CheckRuleCheckCaseResponseInfo** objects	Casos de teste

Tabela 3-35 CheckRuleCheckCaseResponseInfo

Parâmetro	Tipo	Descrição
check_description	String	Descrição do caso de teste Mínimo: **0** Máximo: **65534**
current_value	String	Resultado atual Mínimo: **0** Máximo: **65534**
suggest_value	String	Resultado esperado Mínimo: **0** Máximo: **65534**

Exemplos de solicitações

Nenhum

Exemplo de respostas

Nenhum

Códigos de estado

Código de estado	Descrição
200	O relatório de item de verificação de uma verificação de configuração de segurança é retornado.

Códigos de erro

Consulte **Códigos de erro**.

3.2 Detecção de intrusão

3.2.1 Consulta da lista de intrusões detectadas

Função

Essa API é usada para consultar a lista de intrusões detectadas.

URI

GET /v5/{project_id}/event/events

Tabela 3-36 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: **1** Máximo: **256**

Tabela 3-37 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial de um locatário Padrão: **0** Mínimo: **1** Máximo: **256**
last_days	Não	Integer	Número de dias a serem consultados. Este parâmetro é mutuamente exclusivo com **begin_time** e **end_time**. Mínimo: **1** Máximo: **30**
host_name	Não	String	Nome do servidor
host_id	Não	String	ID do servidor
private_ip	Não	String	Endereço IP do servidor
container_name	Não	String	Nome do container
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: **0** Máximo: **100000** Padrão: **0**
limit	Não	Integer	Número de registros exibidos em cada página Mínimo: **10** Máximo: **200** Padrão: **10**

Parâmetro	Obrigatório	Tipo	Descrição
event_types	Não	Array	Tipo de intrusão. As opções são as seguintes: ● 1001: Malware ● 1010: Rootkit ● 1011: Ransomware ● 1015: Web shell ● 1017: Reverse shell ● 2001: Common vulnerability exploit ● 3002: File privilege escalation ● 3003: Process privilege escalation ● 3004: Important file change ● 3005: File/Directory change ● 3007: Abnormal process behavior ● 3015: High-risk command execution ● 3018: Abnormal shell ● 3027: Suspicious crontab tasks ● 4002: Brute-force attack ● 4004: Abnormal login ● 4006: Invalid system account Mínimo: **1000** Máximo: **30000**
handle_status	Não	String	Estado. As opções são as seguintes: ● unhandled ● handled Mínimo: **1** Máximo: **32**

Parâmetro	Obrigatório	Tipo	Descrição
severity	Não	String	Nível de ameaça. As opções são as seguintes: ● Security ● Low ● Medium ● High ● Critical Mínimo: **1** Máximo: **32**
category	Sim	String	Categoria do evento. As opções são as seguintes: ● host: evento de segurança do host ● container: evento de segurança do container Mínimo: **0** Máximo: **32**
begin_time	Não	String	Hora de início personalizada de um segmento. O timestamp é preciso em segundos. O **begin_time** não deve ser mais do que dois dias antes do **end_time**. Este parâmetro é mutuamente exclusivo com a duração consultada. Mínimo: **13** Máximo: **13**
end_time	Não	String	Hora final personalizada de um segmento. O timestamp é preciso em segundos. O **begin_time** não deve ser mais do que dois dias antes do **end_time**. Este parâmetro é mutuamente exclusivo com a duração consultada. Mínimo: **13** Máximo: **13**

Solicitação dos parâmetros

Tabela 3-38 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: **1** Máximo: **32768**
region	Sim	String	id da região Mínimo: **0** Máximo: **128**

Parâmetros de resposta

Código de estado: 200

Tabela 3-39 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total
data_list	Array of **EventManagementResponseInfo** objects	Lista de eventos

Tabela 3-40 EventManagementResponseInfo

Parâmetro	Tipo	Descrição
event_id	String	ID do evento

Parâmetro	Tipo	Descrição
event_class_id	String	Categoria do evento. As opções são as seguintes: ● container_1001: namespace do container ● container_1002: porta aberta do container ● container_1003: opção de segurança de container ● container_1004: diretório raiz do container ● containerescape_0001: chamada de sistema de alto risco ● containerescape_0002: ataque de Shocker ● containerescape_0003: ataque de Dirty Cow ● containerescape_0004: escape do arquivo do container ● dockerfile_001: modificação do arquivo de container protegido definido pelo usuário ● dockerfile_002: modificação de arquivos executáveis no sistema de arquivos container ● dockerproc_001: processo de container anormal ● fileprotect_0001: escalação de privilégio de arquivo ● fileprotect_0002: alteração do arquivo de chave ● fileprotect_0003: authorizedKeysFile mudança de caminho ● fileprotect_0004: alteração do diretório de arquivos ● login_0001: tentativa de ataque com força bruta ● login_0002: ataque de força bruta foi bem sucedido ● login_1001: login bem-sucedido ● login_1002: login remoto ● login_1003: senha fraca ● malware_0001: mudança de shell ● malware_0002: shell reverso ● malware_1001: programa malicioso ● procdet_0001: comportamento anormal do processo ● procdet_0002: escalação de privilégio do processo ● procreport_0001: comando de alto risco ● user_1001: alteração de conta ● user_1002: conta insegura ● vmescape_0001: comando sensível executado na VM

Parâmetro	Tipo	Descrição
		● vmescape_0002: arquivo sensível acessado pelo processo de virtualização ● vmescape_0003: acesso anormal à porta VM ● webshell_0001: webshell ● network_1001: mineração ● network_1002: ataques DDoS ● network_1003: varredura maliciosa ● network_1004: ataque em áreas sensíveis ● crontab_1001: tarefa suspeita do crontab
event_type	Integer	Tipo de intrusão. As opções são as seguintes: ● 1001: Malware ● 1010: Rootkit ● 1011: Ransomware ● 1015: Web shell ● 1017: Reverse shell ● 2001: Common vulnerability exploit ● 3002: File privilege escalation ● 3003: Process privilege escalation ● 3004: Important file change ● 3005: File/Directory change ● 3007: Abnormal process behavior ● 3015: High-risk command execution ● 3018: Abnormal shell ● 3027: Suspicious crontab tasks ● 4002: Brute-force attack ● 4004: Abnormal login ● 4006: Invalid system account
event_name	String	Nome do evento
severity	String	Nível de ameaça. As opções são as seguintes: ● Security ● Low ● Medium ● High ● Critical
container_name	String	Nome da instância do container
image_name	String	Nomes das imagens
host_name	String	Nome do servidor

Parâmetro	Tipo	Descrição
host_id	String	ID do servidor
private_ip	String	Endereço IP privado do servidor
public_ip	String	Endereço IP elástico
attack_phase	String	Fase de ataque. As opções são as seguintes: ● reconnaissance ● weaponization ● delivery ● exploit ● installation ● command_and_control ● actions
attack_tag	String	Tag de ataque. As opções são as seguintes: ● attack_success ● attack_attempt ● attack_blocked ● abnormal_behavior ● collapsible_host ● system_vulnerability
occur_time	Integer	Tempo de ocorrência, com precisão de milissegundos.
handle_time	Integer	Tempo de manuseio, com precisão de milissegundos.
handle_status	String	Status de processamento. As opções são as seguintes: ● não tratado ● manipulado
handle_method	String	Método de manipulação. As opções são as seguintes: ● mark_as_handled ● ignore ● add_to_alarm_whitelist ● add_to_login_whitelist ● isolate_and_kill
handler	String	Observações para manuseio manual
operate_accept_list	Array of strings	Operação de processamento suportada
operate_detail_list	Array of **EventDetailResponseInfo** objects	Lista de detalhes da operação (não exibida na página)

Parâmetro	Tipo	Descrição
forensic_info	Object	Informações de ataque, em formato JSON.
resource_info	**EventResourceResponseInfo** object	Informações sobre o 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	Informação da aplicação, em formato JSON.
system_info	Object	Informações do sistema, em formato JSON.
recommendation	String	Manipulação de sugestões
process_info_list	Array of **EventProcessResponseInfo** objects	Lista de informações do processo
user_info_list	Array of **EventUserResponseInfo** objects	Lista de informações do usuário
file_info_list	Array of **EventFileResponseInfo** objects	Lista de informações do arquivo

Tabela 3-41 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 do servidor
login_ip	String	Endereço IP de origem de login

Parâmetro	Tipo	Descrição
login_user_name	String	Nome de usuário de login

Tabela 3-42 EventResourceResponseInfo

Parâmetro	Tipo	Descrição
domain_id	String	ID da conta do inquilino
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	UUID da VM
container_id	String	ID do container
image_id	String	ID da imagem
image_name	String	Nomes das imagens
host_attr	String	Atributo do host
service	String	Serviço
micro_service	String	Microsserviço
sys_arch	String	Arquitetura da CPU do sistema
os_bit	String	Versão de bits do SO
os_type	String	Tipo de SO
os_name	String	Nome do SO
os_version	String	Versão de SO

Tabela 3-43 EventProcessResponseInfo

Parâmetro	Tipo	Descrição
process_name	String	Nome do processo
process_path	String	Caminho do arquivo de processo

Parâmetro	Tipo	Descrição
process_pid	Integer	ID do processo Mínimo: **0** Máximo: **2147483647**
process_uid	Integer	ID do usuário do processo Mínimo: **0** Máximo: **2147483647**
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: **0** Máximo: **9223372036854775807**
process_gid	Integer	ID do grupo de processos Mínimo: **0** Máximo: **2147483647**
process_egid	Integer	ID de grupo de processos válido Mínimo: **0** Máximo: **2147483647**
process_euid	Integer	ID de usuário do processo válido Mínimo: **0** Máximo: **2147483647**
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: **0** Máximo: **2147483647**
parent_process_uid	Integer	ID de usuário do processo pai Mínimo: **0** Máximo: **2147483647**
parent_process_cmdline	String	Linha de comando do arquivo do processo pai

Parâmetro	Tipo	Descrição
parent_process_filename	String	Nome do arquivo do processo pai
parent_process_start_time	Long	Hora de início do processo pai Mínimo: **0** Máximo: **9223372036854775807**
parent_process_gid	Integer	ID do grupo de processos pai Mínimo: **0** Máximo: **2147483647**
parent_process_egid	Integer	ID válida do grupo de processos pai Mínimo: **0** Máximo: **2147483647**
parent_process_euid	Integer	ID de usuário válido do processo pai Mínimo: **0** Máximo: **2147483647**
child_process_name	String	Nome do subprocesso
child_process_path	String	Caminho do arquivo do subprocesso
child_process_pid	Integer	ID do subprocesso Mínimo: **0** Máximo: **2147483647**
child_process_uid	Integer	ID do usuário do subprocesso Mínimo: **0** Máximo: **2147483647**
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: **0** Máximo: **9223372036854775807**
child_process_gid	Integer	ID do grupo de subprocessos Mínimo: **0** Máximo: **2147483647**

Parâmetro	Tipo	Descrição
child_process_egid	Integer	ID válida do grupo de subprocessos Mínimo: **0** Máximo: **2147483647**
child_process_euid	Integer	ID de usuário de subprocesso válido Mínimo: **0** Máximo: **2147483647**
virt_cmd	String	comando Virtualização
virt_process_name	String	Nome do processo de virtualização
escape_mode	String	Modo de escape
escape_cmd	String	Comandos executados após a fuga
process_hash	String	Processar hash do arquivo de inicialização

Tabela 3-44 EventUserResponseInfo

Parâmetro	Tipo	Descrição
user_id	Integer	UID do usuário Mínimo: **0** Máximo: **2147483647**
user_gid	Integer	GID do usuário Mínimo: **0** Máximo: **2147483647**
user_name	String	Nome de usuário
user_group_name	String	Nome do grupo de usuários
user_home_dir	String	Diretório home do usuário
login_ip	String	Endereço IP de login do usuário
service_type	String	Tipo de serviço de login
service_port	Integer	Porta de serviço de login Mínimo: **0** Máximo: **2147483647**
login_mode	Integer	Modo de acesso Mínimo: **0** Máximo: **2147483647**

Parâmetro	Tipo	Descrição
login_last_time	Long	Hora do último login Mínimo: **0** Máximo: **9223372036854775807**
login_fail_count	Integer	Número de tentativas de login com falha Mínimo: **0** Máximo: **2147483647**
pwd_hash	String	Hash de senha
pwd_with_fuzzing	String	Palavra-passe mascarada
pwd_used_days	Integer	Idade da senha (dias) Mínimo: **0** Máximo: **2147483647**
pwd_min_days	Integer	Período mínimo de validade da senha Mínimo: **0** Máximo: **2147483647**
pwd_max_days	Integer	Período máximo de validade da senha Mínimo: **0** Máximo: **2147483647**
pwd_warn_left_days	Integer	Aviso prévio de expiração da senha (dias) Mínimo: **0** Máximo: **2147483647**

Tabela 3-45 EventFileResponseInfo

Parâmetro	Tipo	Descrição
file_path	String	Caminho do arquivo
file_alias	String	Alias do arquivo
file_size	Integer	Tamanho do arquivo Mínimo: **0** Máximo: **2147483647**
file_mtime	Long	Hora em que um arquivo foi modificado pela última vez Mínimo: **0** Máximo: **9223372036854775807**

Parâmetro	Tipo	Descrição
file_atime	Long	Hora em que um arquivo foi acessado pela última vez Mínimo: **0** Máximo: **9223372036854775807**
file_ctime	Long	Hora em que o status de um arquivo foi alterado pela última vez Mínimo: **0** Máximo: **9223372036854775807**
file_hash	String	Hash de arquivo
file_md5	String	Ficheiro MD5
file_sha256	String	Ficheiro 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: **0** Máximo: **2147483647**
file_action	String	Ação de arquivo
file_change_attr	String	Atributo antigo/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 do manipulador de arquivo
fd_count	Integer	Número de alças de arquivo Mínimo: **0** Máximo: **2147483647**

Exemplos de solicitações

Nenhum

Exemplo de respostas

Nenhum

Códigos de estado

Código de estado	Descrição
200	Resposta bem-sucedida

Códigos de erro

Consulte **Códigos de erro**.

3.3 Gerenciamento de host

3.3.1 Consulta dos ECSs

Função

Essa API é usada para consultar ECSs.

URI

GET /v5/{project_id}/host-management/hosts

Tabela 3-46 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: **1** Máximo: **256**

Tabela 3-47 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do projeto empresarial Padrão: **0** Mínimo: **0** Máximo: **256**

Parâmetro	Obrigatório	Tipo	Descrição
version	Não	String	Edição HSS. As opções são as seguintes: ● hss.version.null: nenhum ● hss.version.basic: edição básica ● hss.version.enterprise: edição empresarial ● hss.version.premium: edição premium ● hss.version.wtp: edição WTP ● hss.version.container.enterprise : edição de container Mínimo: **1** Máximo: **64**
agent_status	Não	String	Estado do agente. As opções são as seguintes: ● not_ installed ● online ● offline ● install_failed ● installing ● not_online: todos os status exceto **online**, que é usado somente como uma condição de consulta. Mínimo: **1** Máximo: **12**
detect_result	Não	String	Resultado da detecção. As opções são as seguintes: ● undetected ● clean ● risk ● scanning Mínimo: **1** Máximo: **32**
host_name	Não	String	Nome do servidor Mínimo: **0** Máximo: **128**

Parâmetro	Obrigatório	Tipo	Descrição
host_id	Não	String	ID do servidor Mínimo: **0** Máximo: **128**
host_status	Não	String	Status do host. As opções são as seguintes: ● ACTIVE ● SHUTOFF ● BUILDING ● ERROR Mínimo: **1** Máximo: **32**
os_type	Não	String	Tipo de SO. As opções são as seguintes: ● Linux ● Windows Mínimo: **0** Máximo: **64**
private_ip	Não	String	Endereço IP privado do servidor Mínimo: **0** Máximo: **128**
public_ip	Não	String	Endereço IP público do servidor Mínimo: **0** Máximo: **128**
ip_addr	Não	String	Endereço IP público ou privado Mínimo: **0** Máximo: **128**
protect_status	Não	String	Estado da proteção As opções são as seguintes: ● closed ● opened Mínimo: **1** Máximo: **32**
group_id	Não	String	ID do grupo de servidores Mínimo: **0** Máximo: **128**

Parâmetro	Obrigatório	Tipo	Descrição
group_name	Não	String	Nome do grupo de servidores Mínimo: **0** Máximo: **256**
policy_group_id	Não	String	ID do grupo de políticas Mínimo: **0** Máximo: **128**
policy_group_name	Não	String	Nome do grupo de políticas Mínimo: **0** Máximo: **256**
charging_mode	Não	String	Modo de cobrança. As opções são as seguintes: ● packet_cycle: anual/mensal ● on_demand: pagamento por uso Mínimo: **1** Máximo: **32**
refresh	Não	Boolean	Se for preciso sincronizar servidores a partir de ECSs
above_version	Não	Boolean	Se deseja retornar todas as versões posteriores à versão atual
outside_host	Não	Boolean	Se um servidor é um servidor da Huawei Cloud
asset_value	Não	String	Importância patrimonial. As opções são as seguintes: ● important ● common ● test Mínimo: **0** Máximo: **128**
label	Não	String	Etiqueta de ativo Mínimo: **1** Máximo: **64**
limit	Não	Integer	Número de registros exibidos em cada página. O valor padrão é **10**. Mínimo: **0** Máximo: **200** Padrão: **10**

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 **0**. Mínimo: **0** Máximo: **100000** Padrão: **0**

Solicitação dos parâmetros

Tabela 3-48 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: **1** Máximo: **32768**
region	Não	String	id da região Mínimo: **0** Máximo: **128**

Parâmetros de resposta

Código de estado: 200

Tabela 3-49 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Integer	Número total de registros Mínimo: **0** Máximo: **2097152**
data_list	Array of **Host** objects	Consulta sobre o status e a lista do servidor de nuvem

Tabela 3-50 Host

Parâmetro	Tipo	Descrição
host_name	String	Nome do servidor Mínimo: **0** Máximo: **128**
host_id	String	ID do servidor Mínimo: **0** Máximo: **128**
agent_id	String	ID do agente Mínimo: **0** Máximo: **128**
private_ip	String	Endereço IP privado Mínimo: **0** Máximo: **128**
public_ip	String	endereço IP elástico Mínimo: **0** Máximo: **128**
enterprise_project_name	String	Nome do projeto empresarial Mínimo: **0** Máximo: **256**
host_status	String	Status do servidor. As opções são as seguintes: ● ACTIVE ● SHUTOFF ● BUILDING ● ERROR Mínimo: **1** Máximo: **32**
agent_status	String	Estado do agente. As opções são as seguintes: ● not_ installed ● online ● offline ● install_failed ● installing Mínimo: **1** Máximo: **32**

Parâmetro	Tipo	Descrição
install_result_code	String	Resultado da instalação. As opções são as seguintes: ● install_succeed ● network_access_timeout: tempo limite da conexão. Erro de rede. ● invalid_port ● auth_failed: a autenticação falhou devido à senha incorreta. ● permission_denied: permissões insuficientes. ● no_available_vpc: não há servidores com um agente on-line na VPC atual. ● install_exception ● invalid_param ● install_failed ● package_unavailable ● os_type_not_support: tipo de SO incorreto ● os_arch_not_support: arquitetura incorreta do SO Mínimo: **1** Máximo: **32**
version	String	Edição HSS. As opções são as seguintes: ● hss.version.null: nenhum ● hss.version.basic: edição básica ● hss.version.enterprise: edição empresarial ● hss.version.premium: edição premium ● hss.version.wtp: edição WTP ● hss.version.container.enterprise: edição de container Mínimo: **1** Máximo: **32**
protect_status	String	Estado da proteção As opções são as seguintes: ● closed ● opened Mínimo: **1** Máximo: **32**
os_image	String	Imagem de disco do sistema Mínimo: **0** Máximo: **128**

Parâmetro	Tipo	Descrição
os_type	String	Tipo de SO. As opções são as seguintes: ● Linux ● Windows Mínimo: **0** Máximo: **128**
os_bit	String	Versão de bit do SO Mínimo: **0** Máximo: **128**
detect_result	String	Resultado da varredura do servidor. As opções são as seguintes: ● undetected ● clean ● risk ● scanning Mínimo: **1** Máximo: **32**
charging_mode	String	Modo de cobrança. As opções são as seguintes: ● packet_cycle: anual/mensal ● on_demand: pagamento por uso Mínimo: **1** Máximo: **32**
resource_id	String	ID de instância de recurso de serviço de nuvem (UUID) Mínimo: **0** Máximo: **128**
outside_host	Boolean	Se um servidor é um servidor de não-Huawei Cloud
group_id	String	ID do grupo de servidores Mínimo: **1** Máximo: **128**
group_name	String	Nome do grupo de servidores Mínimo: **1** Máximo: **128**
policy_group_id	String	ID do grupo de políticas Mínimo: **1** Máximo: **128**

Parâmetro	Tipo	Descrição
policy_group_name	String	Nome do grupo de políticas Mínimo: **1** Máximo: **128**
asset	Integer	Risco patrimonial Mínimo: **0** Máximo: **2097152**
vulnerability	Integer	vulnerabilidade Mínimo: **0** Máximo: **2097152**
baseline	Integer	Riscos basais Mínimo: **0** Máximo: **2097152**
intrusion	Integer	Risco de intrusão Mínimo: **0** Máximo: **2097152**
asset_value	String	Importância patrimonial. As opções são as seguintes: ● important ● common ● test Mínimo: **0** Máximo: **128**
labels	Array of strings	Lista de tag Mínimo: **0** Máximo: **64**

Exemplos de solicitações

Nenhum

Exemplo de respostas

Nenhum

Códigos de estado

Código de estado	Descrição
200	Resposta bem-sucedida

Códigos de erro

Consulte **Códigos de erro**.

3.4 Gerenciamento de vulnerabilidades

3.4.1 Consulta da lista de vulnerabilidades

Função

Essa API é usada para consultar a lista de vulnerabilidades detectadas.

URI

GET /v5/{project_id}/vulnerability/vulnerabilities

Tabela 3-51 Parâmetros de caminho

Parâmetro	Obrigatório	Tipo	Descrição
project_id	Sim	String	ID do projeto do locatário Mínimo: **1** Máximo: **256**

Tabela 3-52 Parâmetros de consulta

Parâmetro	Obrigatório	Tipo	Descrição
enterprise_project_id	Não	String	ID do locatário da empresa Padrão: **0** Mínimo: **0** Máximo: **256**
type	Não	String	Tipo de vulnerabilidade. As opções são as seguintes: - linux_vul -windows_vul - web_cms Mínimo: **0** Máximo: **32**
vul_id	Sim	String	ID da vulnerabilidade Mínimo: **0** Máximo: **256**

Parâmetro	Obrigatório	Tipo	Descrição
vul_name	Não	String	Nome da vulnerabilidade Mínimo: **0** Máximo: **256**
limit	Não	Integer	Número de registros exibidos em cada página Mínimo: **0** Máximo: **200** Padrão: **10**
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: **0** Máximo: **100000** Padrão: **0**

Solicitação dos parâmetros

Tabela 3-53 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: **1** Máximo: **32768**

Parâmetros de resposta

Código de estado: 200

Tabela 3-54 Parâmetros do corpo de resposta

Parâmetro	Tipo	Descrição
total_num	Long	Número total de vulnerabilidades de software Mínimo: **0** Máximo: **2147483647**
data_list	Array of **VulInfo** objects	Lista de vulnerabilidades de software

Tabela 3-55 VulInfo

Parâmetro	Tipo	Descrição
vul_name	String	Nome da vulnerabilidade Mínimo: **0** Máximo: **256**
vul_id	String	ID da vulnerabilidade Mínimo: **0** Máximo: **64**
label_list	Array of strings	Tag de vulnerabilidade Mínimo: **0** Máximo: **65534**
repair_necessity	Integer	Necessidade de reparar Mínimo: **0** Máximo: **2147483647**
host_num	Integer	Número de servidores afetados Mínimo: **0** Máximo: **2147483647**
unhandle_host_num	Integer	Número de servidores não tratados Mínimo: **0** Máximo: **2147483647**
scan_time	Long	Hora da última varredura Mínimo: **0** Máximo: **9223372036854775807**
solution_detail	String	Solução Mínimo: **0** Máximo: **65534**

Parâmetro	Tipo	Descrição
url	String	URL de vulnerabilidade Mínimo: **0** Máximo: **2083**
description	String	Descrição da vulnerabilidade Mínimo: **0** Máximo: **65534**
type	String	Tipo de vulnerabilidade. As opções são as seguintes:-linux_vul -windows_vul -web_cms Mínimo: **0** Máximo: **128**
host_id_list	Array of strings	Lista de anfitriões Mínimo: **0** Máximo: **128**

Exemplos de solicitações

Nenhum

Exemplo de respostas

Nenhum

Códigos de estado

Código de estado	Descrição
200	A lista de vulnerabilidades detectadas é retornada.

Códigos de erro

Consulte**Códigos de erro**.

A Apêndices

A.1 Código de status

Código de status	Status	Descrição
200	OK	O processamento da solicitação foi 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 mudanças

Data	Descrição da mudança
30/06/2022	Este é o primeiro lançamento oficial.

