Host Security Service

Referencia de la API

Edición 01

Fecha 2022-12-30

HUAWEI TECHNOLOGIES CO., LTD.

Marcas y permisos


y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd.
Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

Aviso

Las funciones, los productos y los servicios adquiridos están estipulados en el contrato celebrado entre Huawei y el cliente. Es posible que la totalidad o parte de los productos, las funciones y los servicios descritos en el presente documento no se encuentren dentro del alcance de compra o de uso. A menos que el contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en este documento constituye garantía alguna, ni expresa ni implícita.

La información contenida en este documento se encuentra sujeta a cambios sin previo aviso. En la preparación de este documento se realizaron todos los esfuerzos para garantizar la precisión de sus contenidos. Sin embargo, ninguna declaración, información ni recomendación contenida en el presente constituye garantía alguna, ni expresa ni implícita.

Huawei Technologies Co., Ltd.

Dirección: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Sitio web: https://www.huawei.com

Email: support@huawei.com

Índice

1 Antes de empezar

1.1 Descripción general

Host Security Service (HSS) le ayuda a identificar y gestionar los activos de sus servidores, eliminar riesgos y defenderse de intrusiones y manipulación de páginas web. También hay funciones avanzadas de protección y operaciones de seguridad disponibles para ayudarle a detectar y prevenir fácilmente las amenazas.

Este documento describe cómo utilizar las interfaces de programación de aplicaciones (API) para realizar operaciones en HSS.

Si planea acceder a HSS a través de una API, asegúrese de estar familiarizado con los conceptos de HSS. Para obtener más información, consulte **Descripción general de servicio**.

1.2 Puntos de conexión

Un punto de conexión es la **request address** para llamar a una API. Los puntos de conexión varían según los servicios y las regiones.

En la siguiente tabla se describen los puntos de conexión de HSS. Seleccione el que desee en función de los requisitos de servicio.

Tabla 1-1 Puntos de conexión de HSS

Nombre	Región	Punto de conexión	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

Un punto de conexión es la **request address** para llamar a una API. Los puntos de conexión varían según los servicios y las regiones. Para ver los puntos de conexión de todos los servicios, consulte **Regiones y puntos de conexción**.

1.3 Limitaciones y Restricciones

Se puede acceder a una API hasta 600 veces/minuto, en la que un solo usuario o dirección IP puede acceder a una API hasta cinco veces/minuto.

Consulte las descripciones de las API específicas.

1.4 Conceptos Básicos

- Cuenta

  Un dominio se crea después de su registro. El dominio tiene permisos de acceso completos para todos sus servicios y recursos en la nube. Se puede utilizar para restablecer contraseñas de usuario y conceder permisos de usuario. La cuenta es una entidad de pago y no debe usarse para realizar una gestión rutinaria. Por motivos de seguridad, cree usuarios de IAM y concédeles permisos para la gestión rutinaria.

- Account

  A domain is created upon successful registration. The domain has full access permissions for all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity and should not be used to perform routine management. For security purposes, create IAM users and grant them permissions for routine management.

- **Usuario**

  Se crea un usuario de IAM mediante una cuenta para utilizar los servicios en la nube. Cada usuario de IAM tiene sus propias credenciales de identidad (contraseña y claves de acceso).

  The account name, username, and password are required for API authentication.

- **User**

  An IAM user is created using an account to use cloud services. Each IAM user has its own identity credentials (password and access keys).

  The account name, username, and password are required for API authentication.

- Región

  Las regiones se dividen en función de la ubicación geográfica y la latencia de la red. Los servicios públicos, como Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP) y Image Management Service (IMS), se comparten dentro de la misma región. Las regiones se clasifican como regiones universales y regiones dedicadas. Una región universal proporciona servicios en la nube universales para los tenants estándares. Una región dedicada proporciona servicios del mismo tipo solo o para inquilinos específicos.

- Zona de disponibilidad (AZ)

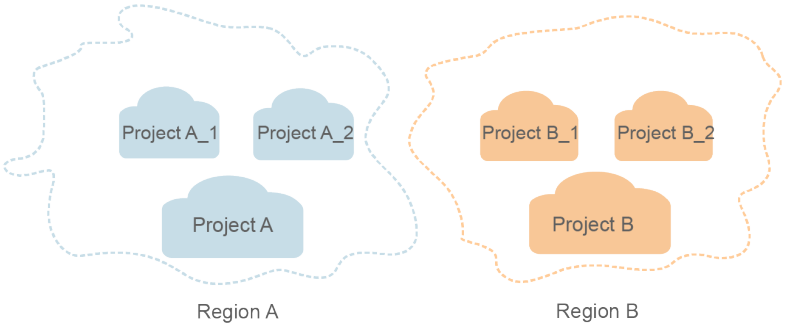
  Una zona de disponibilidad comprende uno o varios centros de datos físicos equipados con instalaciones independientes de ventilación, fuego, agua y electricidad. Los recursos de computación, red, almacenamiento y otros recursos en una zona de disponibilidad se dividen lógicamente en múltiples clústeres. Las zonas de disponibilidad dentro de una

región están conectadas usando fibras ópticas de alta velocidad para soportar sistemas de alta disponibilidad cruzada.

- Proyecto

  Los proyectos agrupan y aíslan recursos informáticos, de almacenamiento y de red en todas las regiones físicas. Para cada región se proporciona un proyecto predeterminado, y para cada uno de ellos se pueden crear subproyectos. Se pueden conceder permisos a los usuarios para acceder a todos los recursos de un proyecto específico. Para un control de acceso más refinado, cree subproyectos en un proyecto y compre recursos en los subproyectos. A los usuarios se les pueden asignar permisos para acceder solo a recursos específicos en los subproyectos.

  Figura 1-1 Modelo de aislamiento del proyecto

- Proyecto empresarial

  Los proyectos empresariales agrupan y gestionan recursos en distintas regiones. Los recursos de los proyectos empresariales están lógicamente aislados entre sí. Un proyecto de empresa puede contener recursos de varias regiones y los recursos se pueden agregar o quitar de los proyectos de empresa.

  Para obtener más información acerca de cómo obtener las características y los identificadores de proyecto empresarial, consulte **Guía de usuario de Enterprise Management**

2 Llamadas a APIs

2.1 Hacer una solicitud de API

Esta sección describe la estructura de una solicitud de API de REST y utiliza la API de IAM para **obtener un token de usuario** como ejemplo para demostrar cómo llamar a una API. El token obtenido se puede usar entonces para autenticar la llamada de otras API.

Solicitud de URI

Un URI de solicitud tiene el siguiente formato:

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

Aunque se incluye un URI de solicitud en la cabecera de solicitud, la mayoría de los lenguajes de programación o marcos requieren que el URI de solicitud se transmita por separado.

- **URI-scheme**:

  Protocolo utilizado para transmitir solicitudes. Todas las API usan HTTPS.

- **Endpoint**:

  Nombre de dominio o dirección IP del servidor que lleva el servicio REST. El punto de conexión varía entre los servicios en diferentes regiones. Se puede obtener de **Regiones y puntos de conexión**.

  Por ejemplo, el punto final de IAM en la región **CN North-Beijing1** es **iam.cn-north-1.myhuaweicloud.com**.

- **resource-path**:

  Ruta de acceso de una API para realizar una operación especificada. Obtener la ruta de acceso desde el URI de una API. Por ejemplo, la **resource-path** de la API utilizada para obtener un token de usuario es **/v3/auth/tokens**.

- **query-string**:

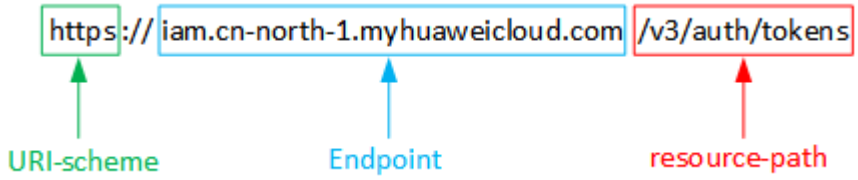
  Parámetro de consulta, que es opcional. Asegúrese de que se incluya un signo de interrogación (?) antes de cada parámetro de consulta que tenga el formato de "Nombre de parámetro=Valor de parámetro". Por ejemplo,**?limit=10** indica que se mostrará un máximo de 10 registros de datos.

Por ejemplo, para obtener el testigo IAM en la región **CN North-Beijing1**, obtener el punto final de IAM (**iam.cn-north-1.myhuaweicloud.com**) para esta región y la **resource-path**

(**/v3/auth/tokens**) en el URI de la API utilizada para **obtener un token de usuario**. A continuación, construya el URI de la siguiente manera:

```
https://iam.cn-north-1.myhuaweicloud.com/v3/auth/tokens
```

Figura 2-1 Ejemplo de URI



NOTA

Para simplificar la visualización de URI en este documento, cada API se proporciona solo con una **resource-path** y un método de solicitud. El **URI-scheme** de todas las API es **HTTPS**, y los puntos finales de todas las API de la misma región son idénticos.

Métodos de solicitud

El protocolo HTTP define los siguientes métodos de solicitud que se pueden usar para enviar una solicitud al servidor:

- **GET**: solicita al servidor que devuelva los recursos especificados.
- **PUT**: solicita al servidor que actualice los recursos especificados.
- **POST**: solicita al servidor que añada recursos o realice operaciones especiales.
- **DELETE**: solicita al servidor que elimine los recursos especificados, por ejemplo, un objeto.
- **HEAD**: igual que GET excepto que el servidor debe devolver solo el encabezado de respuesta.
- **PATCH**: solicita al servidor que actualice el contenido parcial de un recurso especificado. Si el recurso no existe, se creará un nuevo recurso.

Por ejemplo, en el caso de la API usada para **obtener un token de usuario**, el método de solicitud es POST. La solicitud es la siguiente:

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

Encabezado de la solicitud

También puede agregar campos de encabezado adicionales a una solicitud, como los campos requeridos por un método URI o HTTP especificado. Por ejemplo, para solicitar la información de autenticación, agregue **Content-Type**, que especifica el tipo de cuerpo de la solicitud.

Los campos de encabezado de solicitud comunes son los siguientes:

- **Content-Type**: especifica el tipo o formato del cuerpo de la solicitud. Este campo es obligatorio y su valor predeterminado es **application/json**. Otros valores de este campo se proporcionarán para APIs específicas si los hay.
- **X-Auth-Token**: especifica un token de usuario solo para la autenticación API basada en tokens. El token de usuario es una respuesta a la API utilizada para **obtener un token de usuario**. Esta API es la única que no requiere autenticación.

> **NOTA**
>
> Además de admitir la autenticación basada en tokens, las API también admiten la autenticación mediante ID de clave de acceso/clave de acceso secreta (AK/SK). Durante la autenticación basada en AK/SK, se utiliza un SDK para firmar la solicitud, y los campos de encabezado **Authorization** (información de firma) y **X-Sdk-Date** (hora en la que se envía la solicitud) se añaden automáticamente a la solicitud.
>
> Para obtener más información, consulte **Autenticación basada en AK/SK**.

La API usada para **obtener un token de usuario** no requiere autenticación. Por lo tanto, solo es necesario agregar el campo **Content-Type** a las solicitudes para llamar a la API. Un ejemplo de tales solicitudes es el siguiente:

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

Cuerpo de la solicitud

El cuerpo de una solicitud se envía a menudo en un formato estructurado como se especifica en el campo de encabezado **Content-Type**. El cuerpo de la solicitud transfiere contenido excepto el encabezado de la solicitud.

El cuerpo de la solicitud varía entre las API. Algunas API no requieren el cuerpo de la solicitud, como las API solicitadas mediante los métodos GET y DELETE.

En el caso de la API usada para **obtener un token de usuario**, los parámetros de solicitud y la descripción de parámetros se pueden obtener a partir de la solicitud de API. A continuación se proporciona una solicitud de ejemplo con un cuerpo incluido. Establezca ***username*** al nombre de un usuario, ***domainname*** al nombre de la cuenta a la que pertenece el usuario, ******** a la contraseña de inicio de sesión del usuario, y ***xxxxxxxxxxxxxxxxx*** al nombre del proyecto. Puede obtener más información sobre los proyectos en **Regiones y puntos de conexión**. Compruebe el valor de la columna **Region**.

> **NOTA**
>
> El parámetro de **scope** especifica dónde surte efecto un token. Puede establecer **scope** para una cuenta o un proyecto en una cuenta. En el siguiente ejemplo, el token solo tiene efecto para los recursos de un proyecto especificado. Para obtener más información, consulte **Obtener un token de usuario**.

```
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"
            }
        }
```



```
    }
}
```

Si todos los datos necesarios para la solicitud de API están disponibles, puedes enviar la solicitud para llamar a la API a través de **curl**, **Postman** o codificación. En la respuesta a la API utilizada para obtener un token de usuario, **x-subject-token** es el token de usuario deseado. Este token se puede utilizar para autenticar la llamada de otras API.

2.2 Autenticación

Las solicitudes para llamar a una API se pueden autenticar mediante cualquiera de los siguientes métodos:

- Autenticación basada en tokens: las solicitudes se autentican mediante un token.
- Autenticación AK/SK: Las solicitudes se cifran utilizando pares AK/SK. Se recomienda este método porque proporciona mayor seguridad que la autenticación basada en tokens.

Autenticación basada en tokens

NOTA

El período de validez de un token es de 24 horas. Cuando utilice un token para la autenticación, guarde en caché para evitar llamar con frecuencia a la API de IAM utilizada para obtener un token de usuario.

Un token especifica los permisos temporales en un sistema informático. Durante la autenticación de API mediante un token, el token se agrega a las solicitudes para obtener permisos para llamar a la API.

El token se puede obtener llamando a la API requerida. Para obtener más información, consulte **Obtención de un token de usuario**. Se requiere un token de nivel de proyecto para llamar a esta API. Cuando llames a esta API, configura **auth.scope** para **project** en el cuerpo de la solicitud. Ejemplo:

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

Después de obtener un token, el campo de encabezado **X-Auth-Token** debe agregarse a las solicitudes para especificar el token al llamar a otras API. Por ejemplo, si el token es **ABCDEFJ....**, **X-Auth-Token: ABCDEFJ....** se puede añadir a una solicitud de la siguiente manera:


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

Autenticación basada en AK/SK

NOTA

La autenticación basada en AK/SK admite solicitudes de API con un cuerpo de no más de 12 MB. Para las solicitudes de API con un cuerpo más grande, se recomienda la autenticación basada en tokens.

En la autenticación basada en AK/SK, AK/SK se utiliza para firmar solicitudes y la firma se añade a continuación a las solicitudes de autenticación.

- AK: ID de clave de acceso, que es un identificador único usado junto con una clave de acceso secreta para firmar solicitudes criptográficamente.
- SK: clave de acceso secreta usada junto con un AK para firmar solicitudes criptográficamente. Identifica un remitente de la solicitud y evita que la solicitud sea modificada.

En la autenticación basada en AK/SK, puede usar un AK/SK para firmar solicitudes basadas en el algoritmo de firma o usar el SDK de firma para firmar solicitudes. Para obtener más información sobre cómo firmar solicitudes y usar el SDK de firma, consulte **Guía de firma de API**.

AVISO

El SDK de firma solo se utiliza para firmar solicitudes y es diferente de los SDK proporcionados por los servicios.

2.3 Respuesta

Código de estado

Después de enviar una solicitud, recibirá una respuesta, que incluye un código de estado, un encabezado de respuesta y un cuerpo de respuesta.

Un código de estado es un grupo de dígitos, que van desde 1xx hasta 5xx. Indica el estado de una solicitud. Para obtener más información, consulte **Código de estado**.

Por ejemplo, si se devuelve el código de estado **201** para llamar a la API utilizada para **obtener un token de usuario**, la solicitud se realiza correctamente.

Encabezado de respuesta

Un encabezado de respuesta corresponde a un encabezado de solicitud, por ejemplo, **Content-Type**.

Figura 2-2 muestra la cabecera de respuesta para la API de **obtener un token de usuario**, en el que **x-subject-token** es el token de usuario deseado. Este token se puede utilizar para autenticar la llamada de otras API.

Figura 2-2 Encabezado de la respuesta a la solicitud de obtención de un token de usuario

(Opcional) Cuerpo de respuesta

Un cuerpo de respuesta se devuelve generalmente en un formato estructurado, correspondiente al **Content-Type** en el encabezado de respuesta, y se usa para transferir contenido distinto del encabezado de respuesta.

The following shows part of the response body for the API to **obtain a user token**. En aras del espacio, solo una parte del contenido se muestra aquí.

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

Si se produce un error durante la llamada a la API, el sistema le devuelve un código de error y un mensaje. A continuación se muestra el formato de un cuerpo de respuesta de error:

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

En la información anterior, **error_code** es un código de error, y **error_msg** describe el error.

3 Descripción de la API

3.1 Gestión de línea de base

3.1.1 Consulta de la lista de resultados de detección de contraseña débil

Función

Esta API se utiliza para consultar la lista de resultados de detección de contraseñas débiles.

URI

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

Tabla 3-1 Parámetros de path

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto del inquilino Mínimo: **20** Máximo: **64**

Tabla 3-2 Parámetros de Query

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto empresarial Mínimo: **0** Máximo: **64**

Parámetro	Obligatorio	Tipo	Descripción
host_name	No	String	Nombre del servidor Mínimo: **0** Máximo: **256**
host_ip	No	String	Dirección IP del servidor Mínimo: **0** Máximo: **256**
user_name	No	String	Nombre de la cuenta usando una contraseña débil Mínimo: **0** Máximo: **32**
host_id	No	String	Host ID. Si no se especifica este parámetro, se consultan todos los hosts de un inquilino. Mínimo: **0** Máximo: **64**
limit	No	Integer	Número de registros en cada página Mínimo: **0** Máximo: **200** Predeterminado: **10**
offset	No	Integer	Desfase, que especifica la posición inicial del registro que se va a devolver. El valor debe ser un número no menor que 0. El valor predeterminado es **0**. Mínimo: **0** Máximo: **100000** Predeterminado: **0**

Parámetros de solicitud

Tabla 3-3 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
x-auth-token	Sí	String	Token de usuario, que se puede obtener llamando a la API de IAM utilizada para obtener un token de usuario. El valor de **X-Subject-Token** en el encabezado de respuesta es el token de usuario. Mínimo: **32** Máximo: **2097152**

Parámetros de respuesta

Código de estado: 200

Tabla 3-4 Parámetros de body de respuesta

Parámetro	Tipo	Descripción
total_num	Long	Número total de contraseñas débiles Mínimo: **0** Máximo: **2147483647**
data_list	Array of **WeakPwdListInfoResponseInfo** objects	Lista de contraseñas débiles

Tabla 3-5 WeakPwdListInfoResponseInfo

Parámetro	Tipo	Descripción
host_id	String	ID del servidor Mínimo: **0** Máximo: **64**
host_name	String	Nombre del servidor Mínimo: **0** Máximo: **256**
host_ip	String	Dirección IP del servidor Mínimo: **0** Máximo: **256**

Parámetro	Tipo	Descripción
weak_pwd_accounts	Array of **WeakPwdAccountInfoResponseInfo** objects	Lista de cuentas con contraseñas débiles

Tabla 3-6 WeakPwdAccountInfoResponseInfo

Parámetro	Tipo	Descripción
user_name	String	Nombre de las cuentas con contraseñas débiles Mínimo: **0** Máximo: **32**
service_type	String	Tipo de cuenta Mínimo: **0** Máximo: **32**
duration	Integer	Período de validez de una contraseña débil, en días. Mínimo: **0** Máximo: **2147483647**

Solicitudes de ejemplo

Ninguno

Ejemplo de respuestas

Ninguno

Códigos de estado

Código de estado	Descripción
200	Se devuelve la lista de resultados de detección de contraseña débil.

Códigos de error

Consulte **Códigos de error**.

3.1.2 Consulta del informe Detección de políticas de complejidad de contraseñas

Función

Esta API se utiliza para consultar el informe de detección de políticas de complejidad de contraseñas.

URI

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

Tabla 3-7 Parámetros de path

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto del inquilino Mínimo: **1** Máximo: **256**

Tabla 3-8 Parámetros de Query

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto empresarial Mínimo: **0** Máximo: **256**
host_name	No	String	Nombre del servidor Mínimo: **0** Máximo: **128**
host_ip	No	String	Dirección IP del servidor Mínimo: **0** Máximo: **128**
host_id	No	String	ID del servidor. Si no se especifica este parámetro, se consultan todos los hosts de un inquilino. Mínimo: **0** Máximo: **128**

Parámetro	Obligatorio	Tipo	Descripción
limit	No	Integer	Número de registros mostrados en cada página. El valor predeterminado es **10**. Mínimo: **0** Máximo: **200** Predeterminado: **10**
offset	No	Integer	Desfase, que especifica la posición inicial del registro que se va a devolver. El valor debe ser un número no menor que 0. El valor predeterminado es **0**. Mínimo: **0** Máximo: **100000** Predeterminado: **0**

Parámetros de solicitud

Tabla 3-9 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
x-auth-token	Sí	String	Token de usuario. Se puede obtener llamando a la API de IAM utilizada para obtener un token de usuario. El valor de **X-Subject-Token** en el encabezado de respuesta es el token de usuario. Mínimo: **1** Máximo: **32768**

Parámetros de respuesta

Código de estado: 200

Tabla 3-10 Parámetros de body de respuesta

Parámetro	Tipo	Descripción
total_num	Long	Número total de directivas de complejidad de contraseñas Mínimo: **0** Máximo: **2147483647**

Parámetro	Tipo	Descripción
data_list	Array of **PwdPolicyInfoResponseInfo** objects	Lista de detección de políticas de complejidad de contraseñas

Tabla 3-11 PwdPolicyInfoResponseInfo

Parámetro	Tipo	Descripción
host_id	String	ID del servidor (se muestra cuando el cursor se coloca en un nombre de servidor) Mínimo: **0** Máximo: **64**
host_name	String	Nombre del servidor Mínimo: **0** Máximo: **256**
host_ip	String	Dirección IP del servidor Mínimo: **0** Máximo: **256**
min_length	Boolean	Longitud mínima de la contraseña
uppercase_letter	Boolean	Letras en mayúscula
lowercase_letter	Boolean	Letra minúscula
number	Boolean	Digital
special_character	Boolean	Caracteres especiales
suggestion	String	Sugerencia de modificación Mínimo: **0** Máximo: **65534**

Solicitudes de ejemplo

Ninguno

Ejemplo de respuestas

Ninguno

Códigos de estado

Código de estado	Descripción
200	Respuesta exitosa

Códigos de error

Consulte **Códigos de error**.

3.1.3 Consulta de la lista de resultados de la comprobación de configuración de seguridad del servidor

Función

Esta API se utiliza para consultar la lista de resultados de la comprobación de configuración de seguridad del servidor de un inquilino.

URI

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

Tabla 3-12 Parámetros de path

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto del inquilino Mínimo: **1** Máximo: **256**

Tabla 3-13 Parámetros de Query

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto empresarial Mínimo: **0** Máximo: **256**
check_type	No	String	Nombre de línea base Mínimo: **0** Máximo: **256**

Parámetro	Obligatorio	Tipo	Descripción
severity	No	String	Nivel de riesgo. Las opciones son las siguientes: ● Security ● Low ● Medium ● High Mínimo: **1** Máximo: **32**
standard	No	String	Tipo estándar. Las opciones son las siguientes: ● **cn_standard**: Norma de cumplimiento de seguridad ● **hw_standard**: Estándar de Huawei ● **qt_standard**: Estándar de Qingteng Mínimo: **1** Máximo: **32**
host_id	No	String	ID del servidor Mínimo: **0** Máximo: **128**
limit	No	Integer	Número de registros mostrados en cada página. El valor predeterminado es **10**. Mínimo: **0** Máximo: **200** Predeterminado: **10**
offset	No	Integer	Desfase, que especifica la posición inicial del registro que se va a devolver. El valor debe ser un número no menor que 0. El valor predeterminado es **0**. Mínimo: **0** Máximo: **100000** Predeterminado: **0**

Parámetros de solicitud

Tabla 3-14 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
x-auth-token	Sí	String	Token de usuario. Se puede obtener llamando a la API de IAM utilizada para obtener un token de usuario. El valor de **X-Subject-Token** en el encabezado de respuesta es el token de usuario. Mínimo: **1** Máximo: **32768**

Parámetros de respuesta

Código de estado: 200

Tabla 3-15 Parámetros de body de respuesta

Parámetro	Tipo	Descripción
total_num	Long	Número total de registros Mínimo: **0** Máximo: **2147483647**
data_list	Array of **SecurityCheckInfoResponseInfo** objects	Lista de resultados de comprobación de configuración del servidor

Tabla 3-16 SecurityCheckInfoResponseInfo

Parámetro	Tipo	Descripción
severity	String	Nivel de riesgo. Las opciones son las siguientes: ● Low ● Medium ● High Mínimo: **1** Máximo: **32**
check_name	String	Nombre de línea base Mínimo: **0** Máximo: **256**

Parámetro	Tipo	Descripción
check_type	String	Tipo de línea base Mínimo: **0** Máximo: **256**
standard	String	Tipo estándar. Las opciones son las siguientes: ● **cn_standard**: Norma de cumplimiento de seguridad ● **hw_standard**: Estándar de Huawei ● **qt_standard**: Estándar de Qingteng Mínimo: **1** Máximo: **32**
check_rule_num	Integer	Número de elementos de comprobación Mínimo: **0** Máximo: **2097152**
failed_rule_num	Integer	Número de elementos de riesgo Mínimo: **0** Máximo: **2097152**
host_num	Integer	Cantidad de servidores afectados Mínimo: **0** Máximo: **2097152**
scan_time	Long	Último tiempo de escaneo Mínimo: **0** Máximo: **2097152**
check_type_desc	String	Descripción de la línea de base Mínimo: **0** Máximo: **65534**

Solicitudes de ejemplo

Ninguno

Ejemplo de respuestas

Ninguno

Códigos de estado

Código de estado	Descripción
200	Se devuelve la lista de resultados de una comprobación de configuración de seguridad del servidor.

Códigos de error

Consulte **Códigos de error**.

3.1.4 Consulta del resultado de comprobación de un elemento de configuración de seguridad especificado

Función

Esta API se utiliza para consultar el resultado de la comprobación de un elemento de configuración de seguridad especificado.

URI

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

Tabla 3-17 Parámetros de path

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto del inquilino Mínimo: **20** Máximo: **64**
check_type	Sí	String	Nombre de línea base Mínimo: **0** Máximo: **256**

Tabla 3-18 Parámetros de Query

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto empresarial Mínimo: **0** Máximo: **64**

Parámetro	Obligatorio	Tipo	Descripción
standard	Sí	String	Tipo estándar. Las opciones son las siguientes: ● **cn_standard**: Norma de cumplimiento de seguridad ● **hw_standard**: Estándar de Huawei ● **qt_standard**: Estándar de Qingteng Mínimo: **0** Máximo: **32**
host_id	No	String	Host ID. Si no se especifica este parámetro, se consultan todos los hosts de un inquilino. Mínimo: **0** Máximo: **64**
limit	No	Integer	Número de registros en cada página Mínimo: **0** Máximo: **200** Predeterminado: **10**
offset	No	Integer	Desfase, que especifica la posición inicial del registro que se va a devolver. El valor debe ser un número no menor que 0. El valor predeterminado es **0**. Mínimo: **0** Máximo: **100000** Predeterminado: **0**

Parámetros de solicitud

Tabla 3-19 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
x-auth-token	Sí	String	Token de usuario, que se puede obtener llamando a la API de IAM utilizada para obtener un token de usuario. El valor de **X-Subject-Token** en el encabezado de respuesta es el token de usuario. Mínimo: **32** Máximo: **2097152**

Parámetros de respuesta

Código de estado: 200

Tabla 3-20 Parámetros de body de respuesta

Parámetro	Tipo	Descripción
severity	String	Nivel de riesgo. Las opciones son las siguientes: ● Low ● Medium ● High Mínimo: **0** Máximo: **65534**
check_type_desc	String	Descripción de la línea de base Mínimo: **0** Máximo: **65534**
check_rule_num	Integer	Número total de artículos de comprobación Mínimo: **0** Máximo: **2147483647**
failed_rule_num	Integer	Número de artículos de comprobación fallidos Mínimo: **0** Máximo: **2147483647**
passed_rule_num	Integer	Número de artículos de comprobación aprobados Mínimo: **0** Máximo: **2147483647**

Parámetro	Tipo	Descripción
ignored_rule_num	Integer	Número de elementos de comprobación ignorados Mínimo: **0** Máximo: **2147483647**
host_num	Long	Cantidad de servidores afectados Mínimo: **0** Máximo: **2147483647**

Solicitudes de ejemplo

Ninguno

Ejemplo de respuestas

Ninguno

Códigos de estado

Código de estado	Descripción
200	Se devuelve el resultado de la comprobación de un elemento de configuración de seguridad especificado.

Códigos de error

Consulte **Códigos de error**.

3.1.5 Consulta de la lista de elementos de comprobación de un elemento de configuración de seguridad especificado

Función

Esta API se utiliza para consultar la lista de elementos de comprobación de un elemento de configuración de seguridad especificado.

URI

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

Tabla 3-21 Parámetros de path

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto del inquilino Mínimo: **20** Máximo: **64**
check_type	Sí	String	Nombre de línea base Mínimo: **0** Máximo: **256**

Tabla 3-22 Parámetros de Query

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto empresarial Mínimo: **0** Máximo: **64**
standard	Sí	String	Tipo estándar. Las opciones son las siguientes: ● **cn_standard**: Norma de cumplimiento de seguridad ● **hw_standard**: Estándar de Huawei ● **qt_standard**: Estándar de Qingteng Mínimo: **0** Máximo: **32**
result_type	No	String	Tipo de resultado. Las opciones son las siguientes: ● safe ● unhandled ● ignored Predeterminado: **unhandled** Mínimo: **0** Máximo: **64**
check_rule_name	No	String	Compruebe el nombre del elemento. Se admite la coincidencia difusa. Mínimo: **0** Máximo: **2048**

Parámetro	Obligatorio	Tipo	Descripción
severity	No	String	Nivel de riesgo. Las opciones son las siguientes: ● Security ● Low ● Medium ● High ● Critical Mínimo: **0** Máximo: **255**
host_id	No	String	Host ID. Si no se especifica este parámetro, se consultan todos los hosts de un inquilino. Mínimo: **0** Máximo: **64**
limit	No	Integer	Número de registros en cada página Mínimo: **0** Máximo: **200** Predeterminado: **10**
offset	No	Integer	Desfase, que especifica la posición inicial del registro que se va a devolver. El valor debe ser un número no menor que 0. El valor predeterminado es **0**. Mínimo: **0** Máximo: **100000** Predeterminado: **0**

Parámetros de solicitud

Tabla 3-23 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
x-auth-token	Sí	String	Token de usuario, que se puede obtener llamando a la API de IAM utilizada para obtener un token de usuario. El valor de **X-Subject-Token** en el encabezado de respuesta es el token de usuario. Mínimo: **32** Máximo: **2097152**

Parámetros de respuesta

Código de estado: 200

Tabla 3-24 Parámetros de body de respuesta

Parámetro	Tipo	Descripción
total_num	Long	Riesgos totales Mínimo: **0** Máximo: **9223372036854775807**
data_list	Array of **CheckRuleRiskInfoResponseInfo** objects	Lista de datos

Tabla 3-25 CheckRuleRiskInfoResponseInfo

Parámetro	Tipo	Descripción
severity	String	Nivel de riesgo. Las opciones son las siguientes: ● Low ● Medium ● High Mínimo: **0** Máximo: **255**
check_type	String	Nombre de línea base Mínimo: **0** Máximo: **255**

Parámetro	Tipo	Descripción
standard	String	Tipo estándar. Las opciones son las siguientes: ● **cn_standard**: Norma de cumplimiento de seguridad ● **hw_standard**: Estándar de Huawei ● **qt_standard**: Estándar de Qingteng Mínimo: **0** Máximo: **32**
check_rule_name	String	Elemento de comprobación Mínimo: **0** Máximo: **2048**
check_rule_id	String	Comprobar ID de artículo Mínimo: **0** Máximo: **255**
host_num	Integer	Cantidad de servidores afectados Mínimo: **0** Máximo: **2147483647**
scan_result	String	Resultado de la detección. Las opciones son las siguientes: ● pass ● failed Mínimo: **0** Máximo: **64**
status	String	Estado. Las opciones son las siguientes: ● safe ● ignored ● unhandled Mínimo: **0** Máximo: **64**

Solicitudes de ejemplo

Ninguno

Ejemplo de respuestas

Ninguno

Códigos de estado

Código de estado	Descripción
200	Se devuelve la lista de elementos de comprobación de un elemento de configuración de seguridad especificado.

Códigos de error

Consulte **Códigos de error**.

3.1.6 Consulta de la lista de servidores afectados de un elemento de configuración de seguridad especificado

Función

Esta API se utiliza para consultar la lista de servidores afectados de un elemento de configuración de seguridad especificado.

URI

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

Tabla 3-26 Parámetros de path

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto del inquilino Mínimo: **20** Máximo: **64**
check_type	Sí	String	Nombre de línea base Mínimo: **0** Máximo: **256**

Tabla 3-27 Parámetros de Query

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto empresarial Mínimo: **0** Máximo: **64**

Parámetro	Obligatorio	Tipo	Descripción
standard	Sí	String	Tipo estándar. Las opciones son las siguientes: ● **cn_standard**: Norma de cumplimiento de seguridad ● **hw_standard**: Estándar de Huawei ● **qt_standard**: Estándar de Qingteng Mínimo: **0** Máximo: **32**
host_name	No	String	Nombre del servidor Mínimo: **0** Máximo: **256**
host_ip	No	String	Dirección IP del servidor Mínimo: **0** Máximo: **256**
limit	No	Integer	Número de registros en cada página Mínimo: **0** Máximo: **200** Predeterminado: **10**
offset	No	Integer	Desfase, que especifica la posición inicial del registro que se va a devolver. El valor debe ser un número no menor que 0. El valor predeterminado es **0**. Mínimo: **0** Máximo: **100000** Predeterminado: **0**

Parámetros de solicitud

Tabla 3-28 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
x-auth-token	Sí	String	Token de usuario, que se puede obtener llamando a la API de IAM utilizada para obtener un token de usuario. El valor de **X-Subject-Token** en el encabezado de respuesta es el token de usuario. Mínimo: **32** Máximo: **2097152**

Parámetros de respuesta

Código de estado: 200

Tabla 3-29 Parámetros de body de respuesta

Parámetro	Tipo	Descripción
total_num	Long	Volumen total de datos Mínimo: **0** Máximo: **2147483647**
data_list	Array of **SecurityCheckHostInfoResponseInfo** objects	Lista de datos

Tabla 3-30 SecurityCheckHostInfoResponseInfo

Parámetro	Tipo	Descripción
host_id	String	ID del servidor Mínimo: **0** Máximo: **64**
host_name	String	Nombre del servidor Mínimo: **0** Máximo: **256**
host_public_ip	String	Dirección IP pública del servidor Mínimo: **0** Máximo: **128**

Parámetro	Tipo	Descripción
host_private_ip	String	Dirección IP privada del servidor Mínimo: **0** Máximo: **256**
scan_time	Long	Tiempo de escaneo Mínimo: **0** Máximo: **9223372036854775807**
failed_num	Integer	Número de elementos de riesgo Mínimo: **0** Máximo: **2147483647**
passed_num	Integer	Número de artículos aprobados Mínimo: **0** Máximo: **2147483647**

Solicitudes de ejemplo

Ninguno

Ejemplo de respuestas

Ninguno

Códigos de estado

Código de estado	Descripción
200	Se devuelve la lista de servidores afectados por un elemento de configuración de seguridad especificado.

Códigos de error

Consulte **Códigos de error**.

3.1.7 Consulta del informe de un elemento de comprobación en una comprobación de configuración de seguridad

Función

Esta API se utiliza para consultar el informe de un elemento de comprobación en una comprobación de configuración de seguridad.

URI

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

Tabla 3-31 Parámetros de path

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto del inquilino Mínimo: **20** Máximo: **64**

Tabla 3-32 Parámetros de Query

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto empresarial Mínimo: **0** Máximo: **64**
check_type	Sí	String	Nombre de línea base Mínimo: **0** Máximo: **255**
check_rule_id	Sí	String	Comprobar ID de artículo Mínimo: **0** Máximo: **255**
standard	Sí	String	Tipo estándar. Las opciones son las siguientes: ● **cn_standard**: Norma de cumplimiento de seguridad ● **hw_standard**: Estándar de Huawei ● **qt_standard**: Estándar de Qingteng Mínimo: **0** Máximo: **32**
host_id	No	String	ID de host Mínimo: **0** Máximo: **64**

Parámetros de solicitud

Tabla 3-33 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
x-auth-token	Sí	String	Token de usuario, que se puede obtener llamando a la API de IAM utilizada para obtener un token de usuario. El valor de **X-Subject-Token** en el encabezado de respuesta es el token de usuario. Mínimo: **32** Máximo: **2097152**

Parámetros de respuesta

Código de estado: 200

Tabla 3-34 Parámetros de body de respuesta

Parámetro	Tipo	Descripción
description	String	Descripción Mínimo: **0** Máximo: **2048**
reference	String	Escenario Mínimo: **0** Máximo: **255**
audit	String	Descripción de la auditoría Mínimo: **0** Máximo: **65534**
remediation	String	Sugerencia de modificación Mínimo: **0** Máximo: **65534**
check_info_list	Array of **CheckRuleCheckCaseResponseInfo** objects	Casos de prueba

Tabla 3-35 CheckRuleCheckCaseResponseInfo

Parámetro	Tipo	Descripción
check_description	String	Descripción del caso de prueba Mínimo: **0** Máximo: **65534**
current_value	String	Resultado actual Mínimo: **0** Máximo: **65534**
suggest_value	String	Resultado esperado Mínimo: **0** Máximo: **65534**

Solicitudes de ejemplo

Ninguno

Ejemplo de respuestas

Ninguno

Códigos de estado

Código de estado	Descripción
200	Se devuelve el informe de elemento de comprobación de una comprobación de configuración de seguridad.

Códigos de error

Consulte **Códigos de error**.

3.2 Detección de intrusiones

3.2.1 Consulta de la lista de intrusiones detectadas

Función

Esta API se utiliza para consultar la lista de intrusión detectada.

URI

GET /v5/{project_id}/event/events

Tabla 3-36 Parámetros de path

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto del inquilino Mínimo: **1** Máximo: **256**

Tabla 3-37 Parámetros de Query

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID de proyecto de empresa de un inquilino Predeterminado: **0** Mínimo: **1** Máximo: **256**
last_days	No	Integer	Número de días a consultar. Este parámetro es mutuamente excluyente con **begin_time** y **end_time**. Mínimo: **1** Máximo: **30**
host_name	No	String	Nombre del servidor
host_id	No	String	ID del servidor
private_ip	No	String	Dirección IP del servidor
container_name	No	String	Nombre del contenedor
offset	No	Integer	Desfase, que especifica la posición inicial del registro que se va a devolver. El valor debe ser un número no menor que 0. El valor predeterminado es **0**. Mínimo: **0** Máximo: **100000** Predeterminado: **0**
limit	No	Integer	Número de registros mostrados en cada página Mínimo: **10** Máximo: **200** Predeterminado: **10**

Parámetro	Obligatorio	Tipo	Descripción
event_types	No	Array	Tipo de intrusión. Las opciones son las siguientes: ● 1001: Malware ● 1010: Rootkit ● 1011: Ransomware ● 1015: Web shell ● 1017: Reverse shell ● 2001: Explotación de vulnerabilidades comunes ● 3002: escalada de privilegios de archivo ● 3003: Escalada de privilegios de proceso ● 3004: Cambio importante de archivo ● 3005: Cambio de archivo/ directorio ● 3007: Comportamiento del proceso anormal ● 3015: Ejecución de comandos de alto riesgo ● 3018: Abnormal shell ● 3027: Tareas crontab sospechosas ● 4002: Ataque de fuerza bruta ● 4004: Inicio de sesión anormal ● 4006: Cuenta del sistema no válida Mínimo: **1000** Máximo: **30000**
handle_status	No	String	Estado. Las opciones son las siguientes: ● unhandled ● handled Mínimo: **1** Máximo: **32**

Parámetro	Obligatorio	Tipo	Descripción
severity	No	String	Nivel de amenaza. Las opciones son las siguientes: ● Security ● Low ● Medium ● High ● Critical Mínimo: **1** Máximo: **32**
category	Sí	String	Categoría de evento. Las opciones son las siguientes: ● host: evento de seguridad del host ● contenedor: evento de seguridad de contenedor Mínimo: **0** Máximo: **32**
begin_time	No	String	Hora de inicio personalizada de un segmento. La marca de tiempo es precisa en segundos. El **begin_time** no debe ser más de dos días antes que el **end_time**. Este parámetro es mutuamente excluyente con la duración consultada. Mínimo: **13** Máximo: **13**
end_time	No	String	Hora de finalización personalizada de un segmento. La marca de tiempo es precisa en segundos. El **begin_time** no debe ser más de dos días antes que el **end_time**. Este parámetro es mutuamente excluyente con la duración consultada. Mínimo: **13** Máximo: **13**

Parámetros de solicitud

Tabla 3-38 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
x-auth-token	Sí	String	Token de usuario. Se puede obtener llamando a la API de IAM utilizada para obtener un token de usuario. El valor de **X-Subject-Token** en el encabezado de respuesta es un token. Mínimo: **1** Máximo: **32768**
region	Sí	String	id de región Mínimo: **0** Máximo: **128**

Parámetros de respuesta

Código de estado: 200

Tabla 3-39 Parámetros de body de respuesta

Parámetro	Tipo	Descripción
total_num	Integer	Cantidad total
data_list	Array of **EventManagementResponseInfo** objects	Lista de eventos

Tabla 3-40 EventManagementResponseInfo

Parámetro	Tipo	Descripción
event_id	String	ID del evento

Parámetro	Tipo	Descripción
event_class_id	String	Categoría de evento. Las opciones son las siguientes: ● container_1001: Espacio de nombres de contenedor ● container_1002: Puerto abierto del contenedor ● container_1003: Opción de seguridad del contenedor ● container_1004: Directorio de montaje de contenedores ● containerescape_0001: Llamada al sistema de alto riesgo ● containerescape_0002: Shocker attack ● containerescape_0003: Dirty Cow attack ● containerescape_0004: Escape de archivo contenedor ● dockerfile_001: Modificación del archivo contenedor protegido definido por el usuario ● dockerfile_002: Modificación de archivos ejecutables en el sistema de archivos contenedor ● dockerproc_001: Proceso anormal del contenedor ● fileprotect_0001: escalada de privilegios de archivo ● fileprotect_0002: Cambio de archivo clave ● fileprotect_0003: cambio de ruta de acceso de AuthorizedKeysFile ● fileprotect_0004: Cambio de directorio de archivo ● login_0001: Intento de ataque de fuerza bruta ● login_0002: Ataque de fuerza bruta realizado correctamente ● login_1001: Inicio de sesión exitoso ● login_1002: Inicio de sesión remoto ● login_1003: Contraseña débil ● malware_0001: Cambio de Shell ● malware_0002: shell inverso ● malware_1001: Programa malicioso ● procdet_0001: Comportamiento anormal del proceso ● procdet_0002: escalada de privilegios de proceso ● procreport_0001: comando de alto riesgo ● user_1001: Cambio de cuenta ● user_1002: Cuenta insegura

Parámetro	Tipo	Descripción
		● vmescape_0001: Comando sensible ejecutado en la máquina virtual ● vmescape_0002: Archivo sensible al que se accede mediante el proceso de virtualización ● vmescape_0003: acceso a un puerto de máquina virtual anormal ● webshell_0001: Web shell ● network_1001: Minería ● network_1002: ataques DDoS ● network_1003: Análisis malicioso ● network_1004: Ataque en zonas sensibles ● crontab_1001: tarea crontab sospechosa
event_type	Integer	Tipo de intrusión. Las opciones son las siguientes: ● 1001: Malware ● 1010: Rootkit ● 1011: Ransomware ● 1015: Web shell ● 1017: Reverse shell ● 2001: Explotación de vulnerabilidad común ● 3002: escalada de privilegios de archivo ● 3003: Escalada de privilegios de proceso ● 3004: Cambio importante de archivo ● 3005: Cambio de archivo/directorio ● 3007: Comportamiento del proceso anormal ● 3015: Ejecución de comandos de alto riesgo ● 3018: Abnormal shell ● 3027: Tareas crontab sospechosas ● 4002: Ataque de fuerza bruta ● 4004: Inicio de sesión anormal ● 4006: Cuenta del sistema no válida
event_name	String	Nombre del evento
severity	String	Nivel de amenaza. Las opciones son las siguientes: ● Seguridad ● Low ● Medium ● High ● Critical
container_name	String	Nombre de instancia de contenedor

Parámetro	Tipo	Descripción
image_name	String	Nombre de la imagen
host_name	String	Nombre del servidor
host_id	String	ID del servidor
private_ip	String	Dirección IP privada del servidor
public_ip	String	Dirección IP elástica
attack_phase	String	Fase de ataque. Las opciones son las siguientes: ● reconnaissance ● weaponization ● delivery ● exploit ● installation ● command_and_control ● actions
attack_tag	String	Etiqueta de ataque. Las opciones son las siguientes: ● attack_success ● attack_attempt ● attack_blocked ● abnormal_behavior ● collapsible_host ● system_vulnerability
occur_time	Integer	Tiempo de ocurrencia, exacto a milisegundos.
handle_time	Integer	Tiempo de manejo, exacto en milisegundos.
handle_status	String	Estado de procesamiento. Las opciones son las siguientes: ● unhandled ● handled
handle_method	String	Método de manejo. Las opciones son las siguientes: ● mark_as_handled ● ignore ● add_to_alarm_whitelist ● add_to_login_whitelist ● isolate_and_kill
handler	String	Observaciones para el manejo manual
operate_accept_list	Array of strings	Operación de procesamiento compatible

Parámetro	Tipo	Descripción
operate_detail_list	Array of **EventDetailResponseInfo** objects	Lista de detalles de operación (no se muestra en la página)
forensic_info	Object	Información de ataque, en formato JSON.
resource_info	**EventResourceResponseInfo** object	Información del recurso
geo_info	Object	Ubicación geográfica, en formato JSON.
malware_info	Object	Información de malware, en formato JSON.
network_info	Object	Información de red, en formato JSON.
app_info	Object	Información de la aplicación, en formato JSON.
system_info	Object	Información del sistema, en formato JSON.
recommendation	String	Sugerencias sobre el manejo
process_info_list	Array of **EventProcessResponseInfo** objects	Lista de información de proceso
user_info_list	Array of **EventUserResponseInfo** objects	Lista de información de usuario
file_info_list	Array of **EventFileResponseInfo** objects	Lista de información de archivos

Tabla 3-41 EventDetailResponseInfo

Parámetro	Tipo	Descripción
agent_id	String	ID de agente
process_pid	Integer	ID de proceso
is_parent	Boolean	Si un proceso es un proceso de principales
file_hash	String	Hash de archivo
file_path	String	Ruta del archivo
file_attr	String	Atributo de archivo

Parámetro	Tipo	Descripción
private_ip	String	Dirección IP privada del servidor
login_ip	String	Dirección IP de origen de inicio de sesión
login_user_name	String	Iniciar sesión nombre de usuario

Tabla 3-42 EventResourceResponseInfo

Parámetro	Tipo	Descripción
domain_id	String	ID de cuenta del inquilino
project_id	String	ID del proyecto
enterprise_project_id	String	ID del proyecto empresarial
region_name	String	Nombre de la región
vpc_id	String	VPC ID
cloud_id	String	ECS ID
vm_name	String	Nombre de la VM
vm_uuid	String	VM UUID
container_id	String	ID del contenedor
image_id	String	ID de imagen
image_name	String	Nombre de la imagen
host_attr	String	Atributo de host
service	String	Servicio
micro_service	String	Microservicio
sys_arch	String	Arquitectura de CPU del sistema
os_bit	String	Versión del bit del sistema operativo
os_type	String	Tipo de sistema operativo
os_name	String	Nombre del sistema operativo
os_version	String	Versión del sistema operativo

Tabla 3-43 EventProcessResponseInfo

Parámetro	Tipo	Descripción
process_name	String	Nombre del proceso
process_path	String	Ruta del archivo de proceso
process_pid	Integer	ID de proceso Mínimo: **0** Máximo: **2147483647**
process_uid	Integer	ID de usuario de proceso Mínimo: **0** Máximo: **2147483647**
process_username	String	Nombre de usuario del proceso
process_cmdline	String	Línea de comandos del archivo de proceso
process_filename	String	Nombre de archivo de proceso
process_start_time	Long	Hora de inicio del proceso Mínimo: **0** Máximo: **9223372036854775807**
process_gid	Integer	ID de grupo de proceso Mínimo: **0** Máximo: **2147483647**
process_egid	Integer	ID de grupo de procesos válido Mínimo: **0** Máximo: **2147483647**
process_euid	Integer	ID de usuario de proceso válido Mínimo: **0** Máximo: **2147483647**
parent_process_name	String	Nombre del proceso principal
parent_process_path	String	Ruta del archivo de proceso principal
parent_process_pid	Integer	ID de proceso principal Mínimo: **0** Máximo: **2147483647**

Parámetro	Tipo	Descripción
parent_process_uid	Integer	ID de usuario del proceso principal Mínimo: **0** Máximo: **2147483647**
parent_process_cmdline	String	Línea de comandos del archivo de proceso principal
parent_process_filename	String	Nombre de archivo de proceso principal
parent_process_start_time	Long	Hora de inicio del proceso principal Mínimo: **0** Máximo: **9223372036854775807**
parent_process_gid	Integer	ID de grupo de proceso principal Mínimo: **0** Máximo: **2147483647**
parent_process_egid	Integer	ID de grupo de proceso principal válido Mínimo: **0** Máximo: **2147483647**
parent_process_euid	Integer	ID de usuario de proceso principal válido Mínimo: **0** Máximo: **2147483647**
child_process_name	String	Nombre del subproceso
child_process_path	String	Ruta del archivo de subproceso
child_process_pid	Integer	ID de subproceso Mínimo: **0** Máximo: **2147483647**
child_process_uid	Integer	ID de usuario de subproceso Mínimo: **0** Máximo: **2147483647**
child_process_cmdline	String	Línea de comandos del archivo de subproceso
child_process_filename	String	Nombre de archivo de subproceso
child_process_start_time	Long	Hora de inicio del subproceso Mínimo: **0** Máximo: **9223372036854775807**

Parámetro	Tipo	Descripción
child_process_gid	Integer	ID de grupo de subprocesos Mínimo: **0** Máximo: **2147483647**
child_process_egid	Integer	Id. de grupo de subprocesos válido Mínimo: **0** Máximo: **2147483647**
child_process_euid	Integer	ID de usuario de subproceso válido Mínimo: **0** Máximo: **2147483647**
virt_cmd	String	Comando de virtualización
virt_process_name	String	Nombre del proceso de virtualización
escape_mode	String	Modo de escape
escape_cmd	String	Comandos ejecutados después del escape
process_hash	String	Procesar el hash del archivo de inicio

Tabla 3-44 EventUserResponseInfo

Parámetro	Tipo	Descripción
user_id	Integer	UID de usuario Mínimo: **0** Máximo: **2147483647**
user_gid	Integer	GID de usuario Mínimo: **0** Máximo: **2147483647**
user_name	String	Nombre de usuario
user_group_name	String	Nombre del grupo de usuarios
user_home_dir	String	Directorio principal del usuario
login_ip	String	Dirección IP de inicio de sesión del usuario
service_type	String	Tipo de servicio de inicio de sesión
service_port	Integer	Puerto de servicio de inicio de sesión Mínimo: **0** Máximo: **2147483647**

Parámetro	Tipo	Descripción
login_mode	Integer	modo de inicio de sesión Mínimo: **0** Máximo: **2147483647**
login_last_time	Long	Hora del último inicio de sesión Mínimo: **0** Máximo: **9223372036854775807**
login_fail_count	Integer	Cantidad de intentos fallidos de inicio de sesión Mínimo: **0** Máximo: **2147483647**
pwd_hash	String	Hash de contraseña
pwd_with_fuzzing	String	Contraseña enmascarada
pwd_used_days	Integer	Vigencia de la contraseña (días) Mínimo: **0** Máximo: **2147483647**
pwd_min_days	Integer	Período mínimo de validez de la contraseña Mínimo: **0** Máximo: **2147483647**
pwd_max_days	Integer	Período máximo de validez de la contraseña Mínimo: **0** Máximo: **2147483647**
pwd_warn_left_days	Integer	Advertencia anticipada de caducidad de la contraseña (días) Mínimo: **0** Máximo: **2147483647**

Tabla 3-45 EventFileResponseInfo

Parámetro	Tipo	Descripción
file_path	String	Ruta del archivo
file_alias	String	Alias de archivo
file_size	Integer	Tamaño del archivo Mínimo: **0** Máximo: **2147483647**

Parámetro	Tipo	Descripción
file_mtime	Long	Hora en la que se modificó por última vez un archivo Mínimo: **0** Máximo: **9223372036854775807**
file_atime	Long	Hora en la que se accedió por última vez a un archivo Mínimo: **0** Máximo: **9223372036854775807**
file_ctime	Long	Hora en la que se cambió por última vez el estado de un archivo Mínimo: **0** Máximo: **9223372036854775807**
file_hash	String	Hash de archivo
file_md5	String	Archivo MD5
file_sha256	String	Archivo SHA256
file_type	String	Tipo de archivo
file_content	String	Contenido del archivo
file_attr	String	Atributo de archivo
file_operation	Integer	Tipo de operación de archivo Mínimo: **0** Máximo: **2147483647**
file_action	String	Acción de archivo
file_change_attr	String	Atributo Antiguo/Nuevo
file_new_path	String	Nueva ruta de archivo
file_desc	String	Descripción del archivo
file_key_word	String	Palabra clave de archivo
is_dir	Boolean	Si se trata de un directorio
fd_info	String	Información de manejo de archivo
fd_count	Integer	Número de identificadores de archivo Mínimo: **0** Máximo: **2147483647**

Solicitudes de ejemplo

Ninguno

Ejemplo de respuestas

Ninguno

Códigos de estado

Código de estado	Descripción
200	Respuesta exitosa

Códigos de error

Consulte **Códigos de error**.

3.3 Gestión de host

3.3.1 Consulta de ECS

Función

Esta API se utiliza para consultar ECS.

URI

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

Tabla 3-46 Parámetros de path

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto del inquilino Mínimo: **1** Máximo: **256**

Tabla 3-47 Parámetros de Query

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID del proyecto empresarial Predeterminado: **0** Mínimo: **0** Máximo: **256**

Parámetro	Obligatorio	Tipo	Descripción
version	No	String	Edición HSS. Las opciones son las siguientes: ● hss.version.null: ninguna ● hss.version.basic: edición básica ● hss.version.enterprise: edición empresarial ● hss.version.premium: edición premium ● hss.version.wtp: edición WTP ● hss.version.container.company: edición de contenedor Mínimo: **1** Máximo: **64**
agent_status	No	String	Estado de agente. Las opciones son las siguientes: ● not_ installed ● online ● offline ● install_failed ● installing ● not_online: todo el estado excepto **online**, que se utiliza solo como una condición de consulta. Mínimo: **1** Máximo: **12**
detect_result	No	String	Resultado de la detección. Las opciones son las siguientes: ● undetected ● clean ● risk ● scanning Mínimo: **1** Máximo: **32**
host_name	No	String	Nombre del servidor Mínimo: **0** Máximo: **128**

Parámetro	Obligatorio	Tipo	Descripción
host_id	No	String	ID del servidor Mínimo: **0** Máximo: **128**
host_status	No	String	Estado del host. Las opciones son las siguientes: ● ACTIVE ● SHUTOFF ● BUILDING ● ERROR Mínimo: **1** Máximo: **32**
os_type	No	String	Tipo de sistema operativo. Las opciones son las siguientes: ● Linux ● Windows Mínimo: **0** Máximo: **64**
private_ip	No	String	Dirección IP privada del servidor Mínimo: **0** Máximo: **128**
public_ip	No	String	Dirección IP pública del servidor Mínimo: **0** Máximo: **128**
ip_addr	No	String	Dirección IP pública o privada Mínimo: **0** Máximo: **128**
protect_status	No	String	Estado de protección. Las opciones son las siguientes: ● closed ● opened Mínimo: **1** Máximo: **32**
group_id	No	String	ID de grupo de servidores Mínimo: **0** Máximo: **128**

Parámetro	Obligatorio	Tipo	Descripción
group_name	No	String	Nombre del grupo de servidores Mínimo: **0** Máximo: **256**
policy_group_id	No	String	ID de grupo de política Mínimo: **0** Máximo: **128**
policy_group_name	No	String	Nombre del grupo de políticas Mínimo: **0** Máximo: **256**
charging_mode	No	String	Modo de facturación. Las opciones son las siguientes: ● packet_cycle: yearly/monthly ● on_demand: pay-per-use Mínimo: **1** Máximo: **32**
refresh	No	Boolean	Si se deben sincronizar a la fuerza los servidores de los ECS
above_version	No	Boolean	Si se devuelven todas las versiones posteriores a la versión actual
outside_host	No	Boolean	Si un servidor es un servidor Huawei Cloud
asset_value	No	String	Importancia de los activos. Las opciones son las siguientes: ● important ● common ● test Mínimo: **0** Máximo: **128**
label	No	String	Etiqueta de activo Mínimo: **1** Máximo: **64**
limit	No	Integer	Número de registros mostrados en cada página. El valor predeterminado es **10**. Mínimo: **0** Máximo: **200** Predeterminado: **10**

Parámetro	Obligatorio	Tipo	Descripción
offset	No	Integer	Desfase, que especifica la posición inicial del registro que se va a devolver. El valor debe ser un número no menor que 0. El valor predeterminado es **0**. Mínimo: **0** Máximo: **100000** Predeterminado: **0**

Parámetros de solicitud

Tabla 3-48 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
x-auth-token	Sí	String	Token de usuario. Se puede obtener llamando a la API de IAM utilizada para obtener un token de usuario. El valor de **X-Subject-Token** en el encabezado de respuesta es un token. Mínimo: **1** Máximo: **32768**
region	No	String	id de región Mínimo: **0** Máximo: **128**

Parámetros de respuesta

Código de estado: 200

Tabla 3-49 Parámetros de body de respuesta

Parámetro	Tipo	Descripción
total_num	Integer	Número total de registros Mínimo: **0** Máximo: **2097152**
data_list	Array of **Host** objects	Consulta sobre el estado y la lista del servidor en la nube

Tabla 3-50 Host

Parámetro	Tipo	Descripción
host_name	String	Nombre del servidor Mínimo: **0** Máximo: **128**
host_id	String	ID del servidor Mínimo: **0** Máximo: **128**
agent_id	String	ID de agente Mínimo: **0** Máximo: **128**
private_ip	String	Dirección IP privada Mínimo: **0** Máximo: **128**
public_ip	String	Dirección IP elástica Mínimo: **0** Máximo: **128**
enterprise_project_name	String	Nombre del proyecto de empresa Mínimo: **0** Máximo: **256**
host_status	String	Estado del servidor. Las opciones son las siguientes: ● ACTIVE ● SHUTOFF ● BUILDING ● ERROR Mínimo: **1** Máximo: **32**
agent_status	String	Estado de agente. Las opciones son las siguientes: ● not_ installed ● online ● offline ● install_failed ● installing Mínimo: **1** Máximo: **32**

Parámetro	Tipo	Descripción
install_result_code	String	Resultado de la instalación. Las opciones son las siguientes: ● install_succeed ● network_access_timeout: Se ha agotado el tiempo de espera de la conexión. Error de red. ● invalid_port ● auth_failed: Error de autenticación debido a una contraseña incorrecta. ● permission_denied: Permisos insuficientes. ● no_available_vpc: No hay servidores con un agente en línea en la VPC actual. ● install_exception ● invalid_param ● install_failed ● package_unavailable ● os_type_not_support: Tipo de sistema operativo incorrecto ● os_arch_not_support: arquitectura de sistema operativo incorrecta Mínimo: **1** Máximo: **32**
version	String	Edición HSS. Las opciones son las siguientes: ● hss.version.null: none ● hss.version.basic: edición básica ● hss.version.enterprise: edición empresarial ● hss.version.premium: edición premium ● hss.version.wtp: edición WTP ● hss.version.container.company: edición de contenedor Mínimo: **1** Máximo: **32**
protect_status	String	Estado de protección. Las opciones son las siguientes: ● closed ● opened Mínimo: **1** Máximo: **32**

Parámetro	Tipo	Descripción
os_image	String	Imagen de disco del sistema Mínimo: **0** Máximo: **128**
os_type	String	Tipo de sistema operativo. Las opciones son las siguientes: ● Linux ● Windows Mínimo: **0** Máximo: **128**
os_bit	String	Versión del bit del sistema operativo Mínimo: **0** Máximo: **128**
detect_result	String	Resultado del análisis del servidor. Las opciones son las siguientes: ● undetected ● clean ● risk ● scanning Mínimo: **1** Máximo: **32**
charging_mode	String	Modo de facturación. Las opciones son las siguientes: ● packet_cycle: yearly/monthly ● on_demand: pay-per-use Mínimo: **1** Máximo: **32**
resource_id	String	ID de instancia de recurso de servicio en la nube (UUID) Mínimo: **0** Máximo: **128**
outside_host	Boolean	Si un servidor es un servidor que no es de Huawei Cloud
group_id	String	ID de grupo de servidores Mínimo: **1** Máximo: **128**
group_name	String	Nombre del grupo de servidores Mínimo: **1** Máximo: **128**

Parámetro	Tipo	Descripción
policy_group_id	String	ID de grupo de política Mínimo: **1** Máximo: **128**
policy_group_name	String	Nombre del grupo de políticas Mínimo: **1** Máximo: **128**
asset	Integer	Riesgo de activos Mínimo: **0** Máximo: **2097152**
vulnerability	Integer	Vulnerabilidad Mínimo: **0** Máximo: **2097152**
baseline	Integer	Riesgos de línea base Mínimo: **0** Máximo: **2097152**
intrusion	Integer	Riesgo de intrusión Mínimo: **0** Máximo: **2097152**
asset_value	String	Importancia de los activos. Las opciones son las siguientes: ● important ● common ● test Mínimo: **0** Máximo: **128**
labels	Array of strings	Lista de etiquetas Mínimo: **0** Máximo: **64**

Solicitudes de ejemplo

Ninguno

Ejemplo de respuestas

Ninguno

Códigos de estado

Código de estado	Descripción
200	Respuesta exitosa

Códigos de error

Consulte **Códigos de error**.

3.4 Gestión de vulnerabilidades

3.4.1 Consulta de la lista de vulnerabilidades

Función

Esta API se utiliza para consultar la lista de vulnerabilidades detectadas.

URI

GET /v5/{project_id}/vulnerability/vulnerabilities

Tabla 3-51 Parámetros de path

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto del inquilino Mínimo: **1** Máximo: **256**

Tabla 3-52 Parámetros de Query

Parámetro	Obligatorio	Tipo	Descripción
enterprise_project_id	No	String	ID de inquilino de empresa Predeterminado: **0** Mínimo: **0** Máximo: **256**

Parámetro	Obligatorio	Tipo	Descripción
type	No	String	Tipo de vulnerabilidad. Las opciones son las siguientes: - linux_vul -windows_vul - web_cms Mínimo: **0** Máximo: **32**
vul_id	Yes	String	ID de vulnerabilidad Mínimo: **0** Máximo: **256**
vul_name	No	String	Nombre de la vulnerabilidad Mínimo: **0** Máximo: **256**
limit	No	Integer	Número de registros mostrados en cada página Mínimo: **0** Máximo: **200** Predeterminado: **10**
offset	No	Integer	Desfase, que especifica la posición inicial del registro que se va a devolver. El valor debe ser un número no menor que 0. El valor predeterminado es **0**. Mínimo: **0** Máximo: **100000** Predeterminado: **0**

Parámetros de solicitud

Tabla 3-53 Parámetros de encabezado de solicitud

Parámetro	Obligatorio	Tipo	Descripción
x-auth-token	Sí	String	Token de usuario. Se puede obtener llamando a la API de IAM utilizada para obtener un token de usuario. El valor de **X-Subject-Token** en el encabezado de respuesta es un token. Mínimo: **1** Máximo: **32768**

Parámetros de respuesta

Código de estado: 200

Tabla 3-54 Parámetros de body de respuesta

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

Tabla 3-55 VulInfo

Parámetro	Tipo	Descripción
vul_name	String	Nombre de la vulnerabilidad Mínimo: **0** Máximo: **256**
vul_id	String	ID de vulnerabilidad Mínimo: **0** Máximo: **64**
label_list	Array of strings	Etiqueta de vulnerabilidad Mínimo: **0** Máximo: **65534**
repair_necessity	Integer	Necesidad de reparar Mínimo: **0** Máximo: **2147483647**
host_num	Integer	Cantidad de servidores afectados Mínimo: **0** Máximo: **2147483647**
unhandle_host_num	Integer	Número de servidores no controlados Mínimo: **0** Máximo: **2147483647**
scan_time	Long	Último tiempo de escaneo Mínimo: **0** Máximo: **9223372036854775807**

Parámetro	Tipo	Descripción
solution_detail	String	Solución Mínimo: **0** Máximo: **65534**
url	String	URL de vulnerabilidad Mínimo: **0** Máximo: **2083**
description	String	Descripción de la vulnerabilidad Mínimo: **0** Máximo: **65534**
type	String	Tipo de vulnerabilidad. Las opciones son las siguientes:-linux_vul -windows_vul -web_cms Mínimo: **0** Máximo: **128**
host_id_list	Array of strings	Lista de hosts Mínimo: **0** Máximo: **128**

Solicitudes de ejemplo

Ninguno

Ejemplo de respuestas

Ninguno

Códigos de estado

Código de estado	Descripción
200	Se devuelve la lista de vulnerabilidades detectadas.

Códigos de error

Consulte **Códigos de error**.

4 APIs históricas

4.1 Gestión de servidores

4.1.1 Consulta de estado de ECS

Función

Esta API se utiliza para consultar el estado de ECS.

URI

GET /hss/v1/{project_id}/api/host-management/hosts

Tabla 4-1 Parámetros de URI

Parámetro	Obligatorio	Tipo	Descripción
project_id	Sí	String	ID del proyecto.

Tabla 4-2 Parámetros de Query

Parámetro	Obligatorio	Tipo	Descripción
version	No	String	Edición HSS. Sus valores y su significado son los siguientes: ● **hss.version.null**: ninguna ● **hss.version.basic**: edición básica ● **hss.version.enterprise**: edición empresarial ● **hss.version.premium**: edición premium ● **hss.version.wtp**: edición WTP
agent_status	No	String	Estado de agente. Su valor puede ser: ● **not_register** ● **online** ● **offline**
host_status	No	String	Estado de agente. Su valor puede ser: ● **ACTIVE** ● **SHUTOFF** ● **BUILDING** ● **ERROR**
protect_status	No	String	Estado de protección. Su valor puede ser: ● **closed** ● **opened**
detect_result	No	String	Estado de protección. Su valor puede ser: ● **undetect** (no escaneado) ● **clean** (sin riesgo) ● **risk** (riesgo detectado)
host_name	No	String	Nombre del servidor
host_ip	No	String	Dirección IP privada del servidor
public_ip	No	String	EIP del servidor
os_type	No	String	Tipo de sistema operativo

Parámetro	Obligatorio	Tipo	Descripción
charging_mode	No	String	Modo de facturación. Puede ser: ● **packet_cycle** (paquete mensual/anual) ● **on_demand** (pago por uso)
limit	No	Integer	Valor predeterminado: **10**
offset	No	Integer	Valor predeterminado: **0**

Parámetro de solicitud

Tabla 4-3 Parámetro de header de solicitud

Parámetro	Obligatorio	Tipo	Descripción
x-auth-token	Sí	String	Token de usuario. Se puede obtener llamando a la API IAM (valor de **X-Subject-Token** en el encabezado de respuesta).

Parámetros de respuesta

Código de estado: 200

Tabla 4-4 Parámetros de body de respuesta

Parámetro	Tipo	Descripción
total_num	Integer	Cantidad total
data_list	Array of objects	Consulta el estado de ECS.

Tabla 4-5 Host

Parámetro	Tipo	Descripción
agent_id	String	id de agente
host_id	String	ID del servidor
host_name	String	Nombre del servidor
host_ip	String	Dirección IP privada del servidor

Parámetro	Tipo	Descripción
public_ip	String	EIP del servidor
enterprise_project_name	String	Nombre del proyecto de empresa
group_name	String	Nombre del grupo de servidores
expire_time	Long	Tiempo de caducidad del servicio
policy_group_name	String	Nombre del grupo de políticas
host_status	String	Estado de agente. Su valor puede ser: ● **ACTIVE** ● **SHUTOFF** ● **BUILDING** ● **ERROR**
agent_status	String	Estado de agente. Su valor puede ser: ● **uninstall** ● **online** ● **offline**
version	String	Edición HSS. Sus valores y su significado son los siguientes: ● **hss.version.null**: ninguna ● **hss.version.basic**: edición básica ● **hss.version.enterprise**: edición empresarial ● **hss.version.premium**: edición premium ● **hss.version.wtp**: edición WTP
protect_status	String	Estado de protección. Su valor puede ser: ● **closed** ● **opened**
os_image	String	Imagen del sistema
os_type	String	Tipo de sistema operativo
os_bit	String	Versión del bit del sistema operativo
detect_result	String	Resultado del análisis del servidor. Su valor puede ser: ● **undetect** (no escaneado) ● **clean** (sin riesgo) ● **risk** (riesgo detectado)
risk_port_num	Integer	Número de riesgos de activos

Parámetro	Tipo	Descripción
risk_vul_num	Integer	Número de vulnerabilidades
risk_intrusion_num	Integer	Número de intrusiones
risk_baseline_num	Integer	Número de riesgos de línea de base
charging_mode	String	Modo de facturación. Puede ser: ● **packet_cycle** (paquete mensual/anual) ● **on_demand** (pago por uso)
resource_id	String	ID de instancia de recurso de servicio en la nube (UUID)

Ejemplo de solicitud

Ninguno.

Ejemplo de respuesta

Ninguno.

Código de estado

Código de estado	Descripción
200	Se ha obtenido la lista de servidores.

Código de error

Para obtener más información, consulte Códigos de error.

A Apéndices

A.1 Código de estado

Código de estado	Estado	Descripción
200	OK	El procesamiento de la solicitud se ha realizado correctamente.
400	Bad Request	Parámetros de solicitud no válidos.
500	Internal Server Error	Error interno del servicio.

A.2 Códigos de error

Si se devuelve un código de error que comienza con APIGW después de llamar a una API, corrija el error haciendo referencia a las instrucciones proporcionadas en **Códigos de error de puerta de enlace API**.

Código de estado	Códigos de error	Mensaje de error	Descripción	Solución
400	HSS.0001	invalid param error	invalid param error	Please check the input parameter
500	HSS.0041	Query host extend info error	Query host info error	Please check the input parameter

