Host Security Service

Guía del usuario

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.

Índice

1 Habilitación de HSS

1.1 Comprar Cuota de HSS

Puede comprar la cuota HSS en la consola.

Precauciones

- La cuota solo se puede utilizar en la región donde la compró.
- Una cuota puede estar vinculada a un servidor para protegerla, a condición de que el agente en el servidor esté en línea.
- HSS debe implementarse en todos sus servidores para que si un virus infecta a uno de ellos, no pueda propagarse a otros y dañar toda su red.
- Después de comprar la cuota, vaya a la página **Servers & Quota** para **habilitar HSS**.
- La edición premium se proporciona de forma gratuita si ha comprado la edición WTP.

AVISO

- Se recomienda implementar HSS en todos sus servidores para que si un virus infecta a uno de ellos, no pueda propagarse a otros y dañar toda su red.
- En el modo de **Pay-per-use**, la edición empresarial HSS deja de cargar si los servidores que protege están parados. La edición básica en modo de **Pay-per-use** no incurre en cargos durante el período de prueba gratuito o después de que el servidor que protege se detenga.

Regiones

Tabla 1-1 Elegir una región para comprar HSS

Servidor	Región del servidor	Región
ECS BMS HECS	Regiones donde HSS está disponible	Regiones en las que se implementan sus ECS/BMS/HECS HSS no se puede utilizar en todas las regiones. Si el servidor y la cuota de protección se encuentran en diferentes regiones, cancele la suscripción a la cuota y compre una cuota en la región donde se implemente el servidor.
Third-party cloud server	-	Comprar cuota de protección en la región CN South-Guangzhou, CN-Hong Kong o AP-Singapore. Para instalar el agente, realice el procedimiento de instalación para servidores que no sean de Huawei Cloud.
Offline server	-	

Prerrequisitos

Ha obtenido la cuenta de inicio de sesión (con los permisos **HSS Administrator** y **BSS Administrator**) y la contraseña para iniciar sesión en la consola de gestión.

Procedimiento

Paso 1 **Inicie sesión en la consola de gestión.**

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En la esquina superior derecha de la página **Dashboard**, haz clic en **Buy HSS**.

Paso 4 En la página **Buy HSS**, establezca las especificaciones de cuota.

Figura 1-1 Comprar HSS

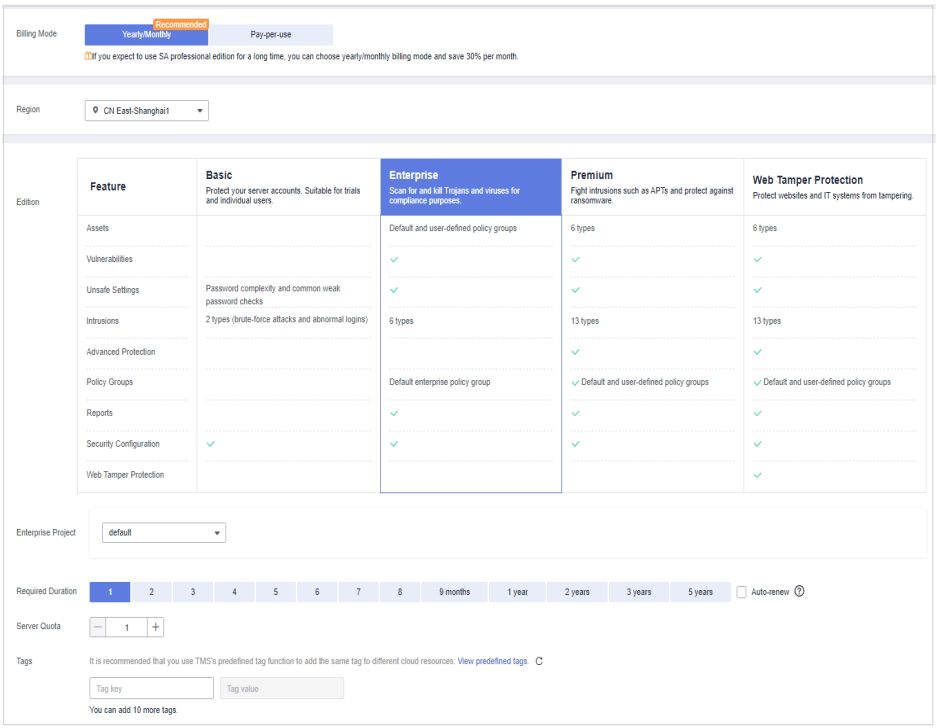


Tabla 1-2 Parámetros para la compra de HSS

Parámetro	Descripción	Valor de ejemplo
Billing Mode	Seleccione el modo de facturación de **Yearly/Monthly** o de **Pay-per-use** según sus requisitos. ● Anual/Mensual: puede seleccionar la edición empresarial, la edición definitiva o la edición de protección contra manipulaciones web. Puede comprar la edición por un período de tiempo fijo. La tarifa es un 30% más baja que la del pago por uso. Si utiliza la edición durante mucho tiempo, le aconsejamos que la compre periódicamente. ● En el modo de pago por uso, solo puede comprar la edición empresarial. Debe habilitar esta edición en la lista de servidores. Usted paga por la duración de uso de los recursos. Los precios se calculan por hora y no se requiere una tarifa mínima. **NOTA** Procedimiento para permitir la cuota de pago por uso: 1. En la página de compra, selecciona **Pay-per-use**. La edición **Enterprise** se seleccionará automáticamente. En la esquina inferior derecha, haz clic en **Enable Now**. Será redirigido a la lista de servidores. 2. En la columna **Operation** de un servidor, haga clic en **Enable**. Establezca **Billing Mode** en **Pay-per-use** y establezca **Edition** en **Enterprise**. También puede seleccionar **Basic**, que es gratuito durante 30 días. 3. Confirme la información y haga clic en **OK**.	Yearly/ Monthly

Parámetro	Descripción	Valor de ejemplo
Region	● Para minimizar los problemas de conexión, compre la cuota en la región de sus servidores.	CN-Hong Kong
Edition	Puede adquirir la edición **Basic (free)**, **Enterprise**, **Premium**, o **Web Tamper Protection**. Para obtener más información sobre las diferencias entre ediciones, consulte **Ediciones**. **AVISO** ● No es necesario adquirir la edición básica. Puede **habilitarlo** en la lista de servidores. ● Si adquirió la edición básica, empresarial o premium, habilítela en la página **Asset Management** > **Servers & Quota**. ● Si adquirió la edición WTP, habilitela en la lista de servidores de la página **Prevention** > **Web Tamper Protection**.	Enterprise
Enterprise Project	Esta opción sólo está disponible cuando ha iniciado sesión con una cuenta de empresa o cuando ha habilitado proyectos de empresa. Puede ponerse en contacto con su administrador de servicio para activar esta función y poner los recursos de la nube y los miembros en proyectos empresariales para una gestión centralizada. Seleccione un proyecto de empresa en la lista desplegable. **NOTA** ● Los recursos y los gastos incurridos se gestionan en el proyecto de empresa seleccionado. ● Valor **default** indica el proyecto de empresa predeterminado. Los recursos que no están asignados a ningún proyecto de empresa de su cuenta se muestran en el proyecto de empresa predeterminado. ● La opción **default** está disponible en la lista desplegable **Enterprise Project** solo después de comprar HSS en su cuenta de Huawei Cloud.	default
Required duration	● Seleccione una duración en función de sus requisitos. En el modo de **Pay-per-use**, no es necesario seleccionar una duración. ● Le recomendamos que seleccione **Auto-renew** para asegurarse de que sus servidores estén siempre protegidos. ● Si selecciona **Auto-renew**, el sistema renovará automáticamente tu suscripción siempre y cuando el saldo de tu cuenta sea suficiente. El período de renovación es el mismo que la duración requerida. ● Si no selecciona **Auto-renew**, renueve manualmente el servicio antes de que caduque.	1 year
Server Quota	Introduzca el número de cuotas de HSS que se van a comprar. En el modo de **Pay-per-use**, no es necesario configurar esta opción. **AVISO** ● Todos sus servidores deben estar protegidos, por lo que si un virus (como ransomware o un programa de minería) infecta uno de ellos, no será capaz de propagarse a otros y dañar toda su red. ● No se puede modificar la cuota de una edición una vez completada su compra. Puede darse de baja de él y comprar de nuevo.	20

Parámetro	Descripción	Valor de ejemplo
Tag	Puede poner etiquetas en los recursos de la nube del mismo tipo para ayudarle a buscar rápidamente recursos de la nube. En el modo de **Pay-per-use**, no es necesario configurar las etiquetas.	data

Paso 5 En la esquina inferior derecha de la página, haz clic en **Next**.

Para obtener más información sobre los precios, consulte **Detalles de precios del producto**.

Paso 6 Después de confirmar que el pedido, seleccione **I have read and agree to the Host Security Service Disclaimer** y haga clic en **Pay Now**.

Paso 7 En la página mostrada, haga clic en **Pay** y complete el pago.

----Fin

Procedimiento posterior

Cancelación de suscripción

Si compró HSS en la edición o región incorrecta, primero puede darse de baja de él y luego comprar la cuota correcta.

1.2 Comprar Cuota de CGS

Puede comprar CGS para comprobar la seguridad de las imágenes, los contenedores y el tiempo de ejecución del contenedor, manejando las amenazas de seguridad de manera oportuna.

Precauciones

- Durante la compra, establezca la cantidad de nodos en el número de nodos que se van a proteger. La cuota CGS solo se puede utilizar en la región que seleccione.
- Después de comprar la cuota, vaya a la página **Containers & Quota** para **habilitar la protección**.

Procedimiento

Paso 1 **Inicie sesión en la consola de gestión.**

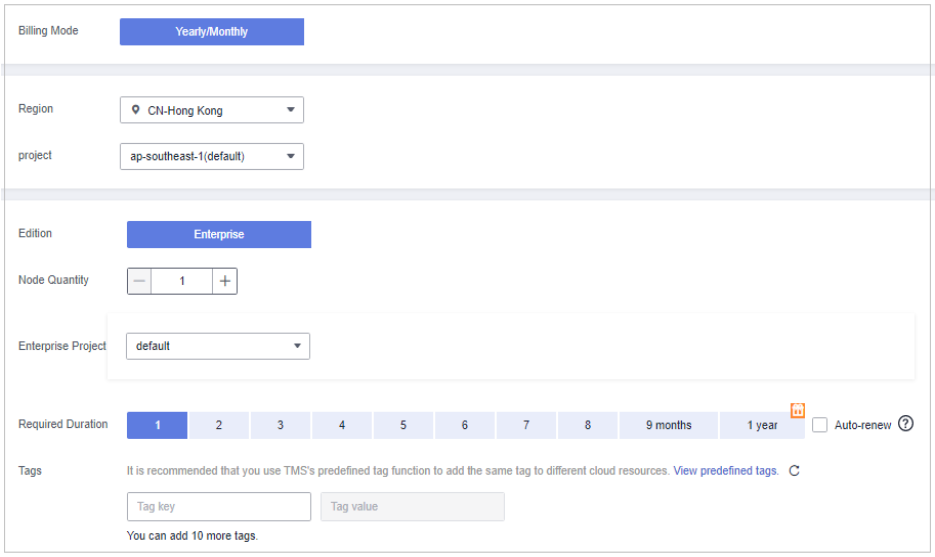
Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Load Management** > **Containers & Quota**.

Paso 4 Haga clic en **Buy CGS**.

Paso 5 Configurar las especificaciones CGS.

Figura 1-2 Compra de CGS



1. **Billing Mode**: Anual/Mensual
2. **Region**: Seleccione la región donde se despliegan los nodos. HSS no se puede utilizar en todas las regiones. Si compró una cuota en una región incorrecta, anule la suscripción y cómprela en tu región.
3. **Node Quantity**: número de nodos a proteger
4. **Required Duration**: El valor varía de 1 a 12 meses.

   Le recomendamos que seleccione **Auto-renew** para asegurarse de que sus servidores estén siempre protegidos.

   Si selecciona **Auto-renew**, el sistema renovará automáticamente tu suscripción siempre y cuando el saldo de tu cuenta sea suficiente. El período de renovación es el mismo que la duración requerida.

   Si no selecciona **Auto-renew**, renueve manualmente el servicio antes de que caduque.

Paso 6 En la esquina inferior derecha de la página, haz clic en **Next**.

Para obtener más información sobre los precios, consulte **Detalles de precios del producto**.

Paso 7 Verifique los detalles del pedido, lea el *Container Guard Service Disclaimer* y *Privacy Statement* y seleccione **I have read and agree to the Container Guard Service Disclaimer and Privacy Statement**.

Paso 8 En la página mostrada, haga clic en **Pay** y complete el pago.

----Fin

Procedimiento posterior

Unsubscription

Si compró la cuota en la edición o región incorrecta, primero puede darse de baja de ella y luego comprar la cuota correcta.

1.3 Instalación de un agente

1.3.1 Instalación de un agente en el sistema operativo Linux

Para habilitar la protección de cargas de trabajo para servidores en la nube, instale primero el agente.

En este tema se describe cómo instalar el agente en un servidor que ejecuta un sistema operativo Linux. Para obtener más información sobre cómo instalar un agente en el sistema operativo Windows, consulte **Instalación de un agente en el sistema operativo Windows**.

NOTA

- WTP, CGS y HSS comparten el mismo agente, por lo que solo necesita instalar el agente una vez en el mismo servidor.
- Las versiones de CentOS 6.x ya no se actualizan o mantienen en el sitio web oficial de Linux y, por lo tanto, ya no son compatibles con HSS. Si necesita estas versiones, puede **enviar una orden de trabajo** para obtener ayuda.

Limitaciones y Restricciones

HSS puede proteger tanto los servidores Huawei Cloud como los servidores que no son Huawei Cloud.

- Servidor de Huawei cloud
  - Puede gestionar servidores en la nube comprados en la consola de Huawei Cloud.
  - Solo se admiten servidores en la nube de 64 bits.
  - Asegúrese de haber adquirido HSS en la región del servidor y de haber utilizado el paquete de instalación o el comando de instalación en la región para instalar agentes HSS en los servidores.
- Servidor que no es de Huawei Cloud
  - Puede gestionar servidores comprados fuera de la consola de Huawei Cloud o los servidores de Huawei Cloud que no estén en su región.
  - Solo se admiten servidores en la nube de 64 bits.
  - Después de instalar el agente, puede buscar un servidor en la lista de servidores protegidos por el EIP del servidor.

AVISO

- Para una mejor compatibilidad y experiencia de servicio, se recomienda utilizar los servidores en la nube de Huawei.
- Cuando instale el agente, borre los procesos de aplicación y la información de configuración que puedan interferir con la instalación en los servidores para evitar errores de instalación.
- Hasta ahora, el agente solo se puede instalar en servidores que no sean de Huawei Cloud en la región **CN-Hong Kong**.

Ruta de instalación predeterminada

La ruta de instalación del agente en los servidores que ejecutan el sistema operativo Linux no se puede personalizar. La ruta predeterminada es:

/usr/local/hostguard/

Prerrequisitos

- Para instalar el agente en un servidor que no sea Huawei Cloud, asegúrese de que el servidor ejecute el sistema operativo Linux y pueda acceder a Internet.
- El firewall Linux mejorado de seguridad (SELinux) ha sido deshabilitado. El firewall afecta a la instalación del agente y debe permanecer deshabilitado hasta que se instale el agente.

Instalación de un agente mediante comandos

Este procedimiento implica iniciar sesión en el servidor y ejecutar comandos. La consola tarda de 3 a 5 minutos en actualizar el estado del agente después de la instalación del agente.

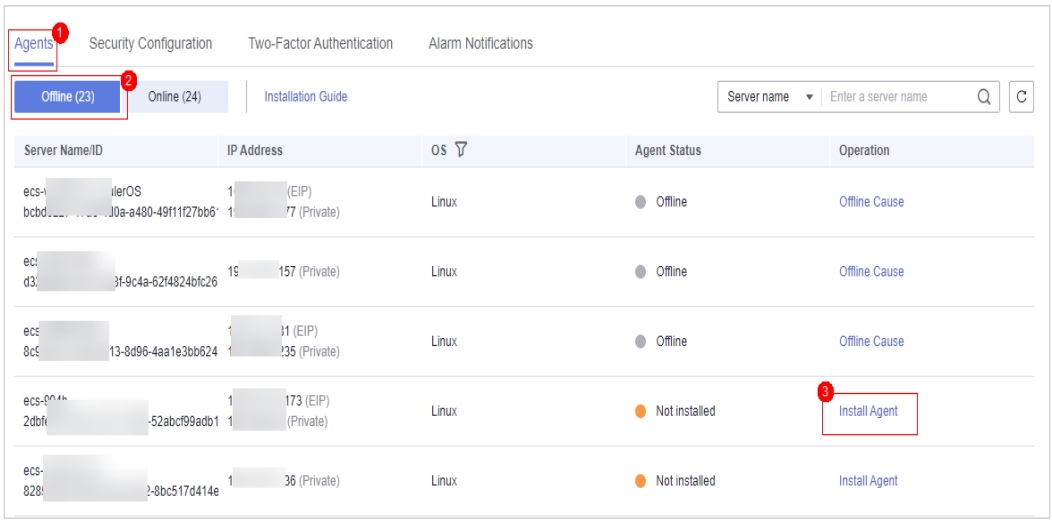
Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Installation & Configuration**.

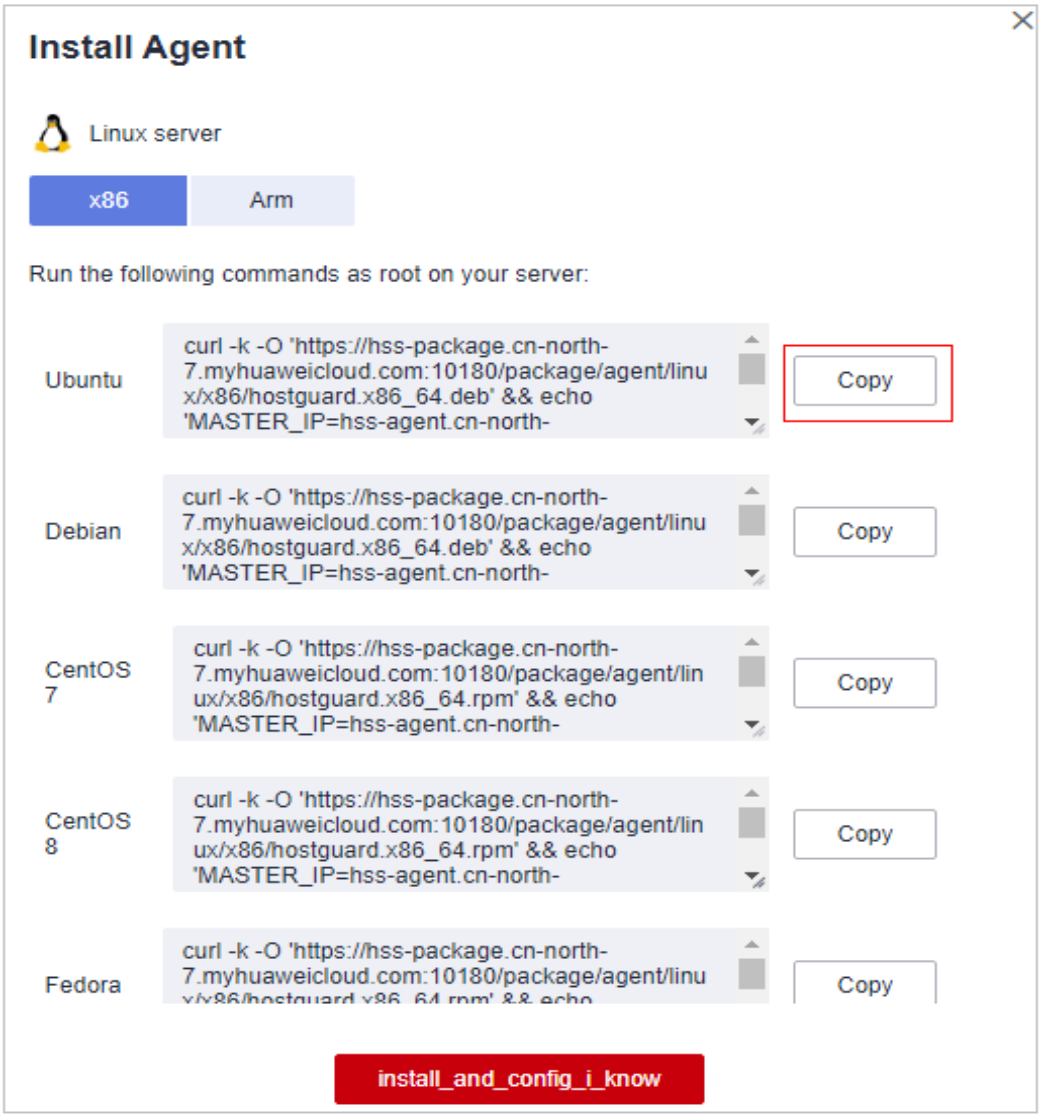
Paso 4 Haga clic en la pestaña **Agents**. Haga clic en **Offline**. En la columna **Operation** de un servidor, haga clic en **Install Agent**.

Figura 1-3 Selección de un servidor Linux



Paso 5 En el cuadro de diálogo que se muestra, copie el comando adecuado para la arquitectura del sistema y el sistema operativo.

Figura 1-4 Copiar el comando para instalar el agente



Paso 6 Inicie sesión de forma remota en el servidor donde se va a instalar el agente.

- Servidor de Huawei cloud
  - Inicie sesión en la consola de ECS, busque el servidor de destino y haga clic en **Remote Login** en la columna **Operation** para iniciar sesión en el servidor. Para obtener más información, consulte **Iniciar sesión usando VNC**.
  - Si su servidor tiene un EIP enlazado, también puede usar una herramienta de gestión remota, como PuTTY o Xshell, para iniciar sesión en el servidor e instalar el agente en el servidor como usuario **root**.
- Servidor que no es de Huawei Cloud

  Utilice una herramienta de gestión remota (como PuTTY o Xshell) para conectarse al EIP de su servidor e iniciar sesión de forma remota en su servidor.

Paso 7 Pegue el comando de instalación copiado y ejecútelo como usuario **root** para instalar el agente en el servidor.

NOTA

- Si no se puede descargar el paquete de instalación, compruebe que el DNS puede resolver el nombre de dominio en el comando de instalación.
- Para instalar el agente en un servidor que no sea Huawei Cloud, asegúrese de que existe el ID de organización en el comando. De lo contrario, el estado del agente puede mostrarse como **Not installed** aunque la instalación se haya realizado correctamente.

Si se muestra información similar a la siguiente, el agente se instala correctamente:

```
Preparing...                ########################### [100%]
1:hostguard                 ########################### [100%]
Hostguard is running.
Hostguard installed.
```

Paso 8 Ejecute el comando **service hostguard status** para comprobar el estado de ejecución del agente.

Si se muestra la siguiente información, el agente se está ejecutando correctamente:

```
Hostguard is running
```

----Fin

Procedimiento posterior

- Para obtener más información sobre el estado del agente y la solución de problemas, consulte **¿Qué debo hacer cuando el estado de ejecución del agente es anormal?**
- Para obtener más información sobre cómo manejar los errores de instalación del agente, consulte **¿Qué debo hacer si falló la instalación del agent?**
- Para obtener más información sobre la desinstalación del agente, consulte **¿Cómo desinstalo el agent?**

1.3.2 Instalación de un agente en el sistema operativo Windows

Para habilitar la protección de cargas de trabajo para servidores en la nube, instale primero el agente.

En este tema se describe cómo instalar el agente en un servidor que ejecuta un sistema operativo Windows. Para obtener más información sobre cómo instalar un agente en el sistema operativo Linux, consulte **Instalación de un agente en el sistema operativo Linux**.

NOTA

- WTP, CGS y HSS comparten el mismo agente, por lo que solo necesita instalar el agente una vez en el mismo servidor.
- Las versiones de CentOS 6.x ya no se actualizan o mantienen en el sitio web oficial de Linux y, por lo tanto, ya no son compatibles con HSS. Si necesita estas versiones, puede **enviar una orden de trabajo** para obtener ayuda.

Limitaciones y Restricciones

HSS puede proteger tanto los servidores Huawei Cloud como los servidores que no son Huawei Cloud.

- Servidor de Huawei cloud
  - Puede gestionar servidores en la nube comprados en la consola de Huawei Cloud.

  - Solo se admiten servidores en la nube de 64 bits.
  - Asegúrese de haber adquirido HSS en la región del servidor y de haber utilizado el paquete de instalación o el comando de instalación en la región para instalar agentes HSS en los servidores.
- Servidor que no es de Huawei Cloud
  - Puede gestionar servidores comprados fuera de la consola de Huawei Cloud o los servidores de Huawei Cloud que no estén en su región.
  - Solo se admiten servidores en la nube de 64 bits.
  - Después de instalar el agente, puede buscar un servidor en la lista de servidores protegidos por el EIP del servidor.

AVISO

- Para una mejor compatibilidad y experiencia de servicio, se recomienda utilizar los servidores en la nube de Huawei.
- Cuando instale el agente, borre los procesos de aplicación y la información de configuración que puedan interferir con la instalación en los servidores para evitar errores de instalación.
- Hasta ahora, el agente solo se puede instalar en servidores que no sean de Huawei Cloud en la región **CN-Hong Kong**.

Ruta de instalación predeterminada

No se puede personalizar la ruta de instalación del agente en los servidores que ejecutan el sistema operativo Windows. La ruta predeterminada es:

C:\Program Files (x86)\HostGuard

Prerrequisitos

- Para instalar el agente en un servidor que no sea Huawei Cloud, asegúrese de que el servidor ejecute el sistema operativo Windows y pueda acceder a Internet.
- Una herramienta de gestión remota, como mstsc y RDP, se ha instalado en su PC.

Procedimiento

Hay dos formas de instalar un agente. Esta sección describe la primera.

- Método 1: Descargue el paquete de instalación del agente, cárguelo en el servidor donde se va a instalar el agente y ejecute el comando de instalación en el servidor para instalar el agente.
- Método 2: Inicie sesión en un servidor, inicie sesión en la consola de gestión desde el servidor y descargue e instale el agente.

Paso 1 **Inicie sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Installation & Configuration**.

Paso 4 Haga clic en la pestaña **Agents**. Haga clic en **Offline**. En la columna **Operation** de un servidor, haga clic en **Install Agent**.

Paso 5 En el cuadro de diálogo que se muestra, copie el enlace de descarga del agente adecuado para la arquitectura del sistema y el sistema operativo.

Paso 6 Inicie sesión de forma remota en el servidor donde se va a instalar el agente.

- Servidor de Huawei cloud
  - Inicie sesión en la consola de ECS, busque el servidor de destino y haga clic en **Remote Login** en la columna **Operation** para iniciar sesión en el servidor. Para obtener más información, consulte **Iniciar sesión usando VNC**.
  - Si un EIP está enlazado al servidor, puede utilizar Conexión a Escritorio remoto de Windows o una herramienta de gestión remota de terceros, como mstsc o RDP, para iniciar sesión en el servidor e instalar el agente en el servidor como administrador.
- Servidor que no es de Huawei Cloud
  - Utilice una herramienta de gestión remota (como mstsc o RDP) para conectarse al EIP de su servidor e iniciar sesión de forma remota en su servidor.

Paso 7 Utilice Internet Explorer descargue el paquete de instalación del agent desde la dirección de descarga del agent copiado y descomprimalo.

NOTA

- Para instalar el agente en un servidor que no sea Huawei Cloud, asegúrese de que el ID de organización del comando sea correcto. De lo contrario, el estado del agente puede mostrarse como **Not installed** aunque la instalación se haya realizado correctamente.

Paso 8 Ejecute el programa de instalación del agente como administrador.

Seleccione un tipo de host en la página **Select host type**.

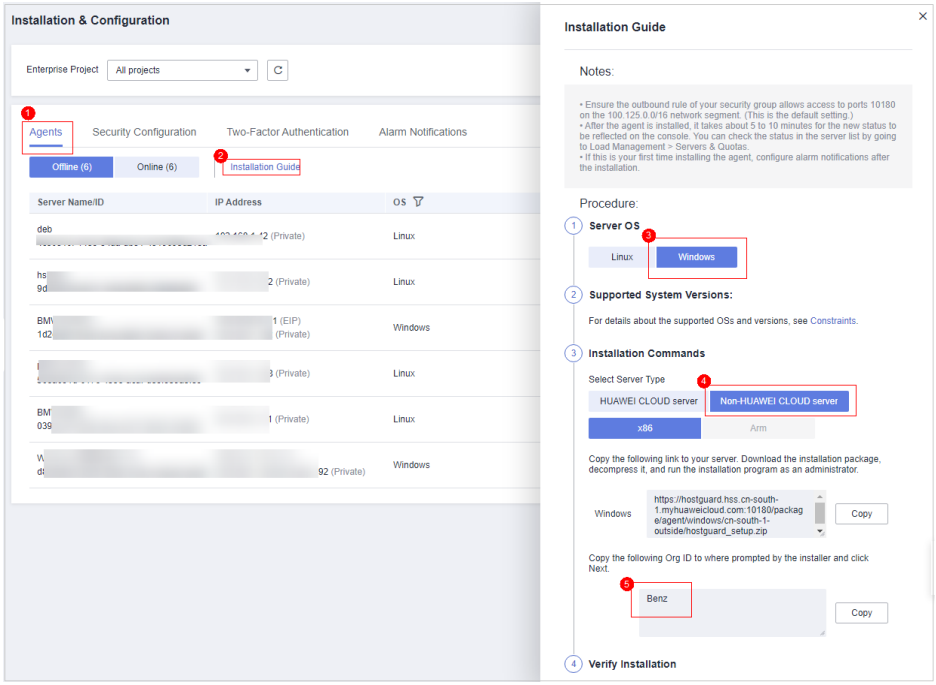
- Servidor Cloud de Huawei: Seleccione **Huawei Cloud Host**.
- Servidor Cloud que no es de Huawei: Seleccione **Other Cloud Host**.

  Copie el ID de organización en la página de instalación del agente, como se muestra en **Figura 1-5**. Ingrese el ID de organización e instale el agente como se le solicite.

AVISO

Asegúrese de que el ID de organización sea correcto. De lo contrario, el estado del agente puede mostrarse como **Not installed** aunque la instalación se haya realizado correctamente.

Figura 1-5 Obtención del ID de organización (para un servidor que no sea de Huawei Cloud)



Paso 9 Compruebe **HostGuard.exe** y **HostWatch.exe** en el Administrador de tareas de Windows.

Si los procesos no existen, la instalación del agent falla. En este caso, vuelva a instalar el agent.

La consola tarda de 3 a 5 minutos en actualizar el estado del agente después de la instalación del agente.

----Fin

Procedimiento posterior

- Para obtener más información sobre el estado del agente y la solución de problemas, consulte **¿Qué debo hacer cuando el estado de ejecución del agente es anormal?**
- Para obtener más información sobre cómo manejar los errores de instalación del agente, consulte **¿Qué debo hacer si falló la instalación del agent?**
- Para obtener más información sobre la desinstalación del agente, consulte **¿Cómo desinstalo el agent?**

1.4 Habilitación de HSS

1.4.1 Habilitación de la edición básica/empresarial/premium

Antes de habilitar la protección en servidores, debe asignar la cuota a un servidor especificado. Si la protección está deshabilitada o se elimina el servidor, la cuota se puede asignar a otros servidores.

Para la edición WTP, elija **Web Tamper Protection** > **Server Protection** y a continuación, habilítilo. Para más detalles, consulte **Habilitación de la edición WTP**.

NOTA

Para habilitar la edición WTP, elija **Prevention** > **Web Tamper Protection** y haga clic en la pestaña **Servers**. Todas las funciones de la edición premium están incluidas con la edición WTP.

Modo de verificación

El sistema HSS detecta todos los datos a las 00:00 todos los días.

Si habilita la protección del servidor antes del intervalo de detección, puede ver los resultados de la detección solo después de que se realice la detección a las 00:00 del día siguiente o realizar una detección manual inmediatamente.

Prerrequisitos

- El estado del agente del servidor que se va a proteger es **Online**. Para comprobar el estado, elija **Cloud Workload Protection Platform** > **Asset Management** > **Servers & Quota**.
- Ha adquirido cuotas de edición requeridas en su región.
- Para proteger mejor sus contenedores, se recomienda **establecer configuraciones de seguridad**.

Restricciones

- Linux OS

  En los servidores que ejecutan EulerOS con ARM, HSS no bloquea las direcciones IP sospechosas de ataques de fuerza bruta SSH, sino que solo genera alarmas.
- Windows OS
  - Autorice el firewall de Windows cuando habilite la protección para un servidor Windows. No deshabilite el firewall de Windows durante el período de servicio del HSS. Si el firewall de Windows está deshabilitado, HSS no puede bloquear direcciones IP de ataque de fuerza bruta.
  - Si el firewall de Windows está habilitado manualmente, es posible que HSS también no bloquee las direcciones IP de ataque de fuerza bruta.

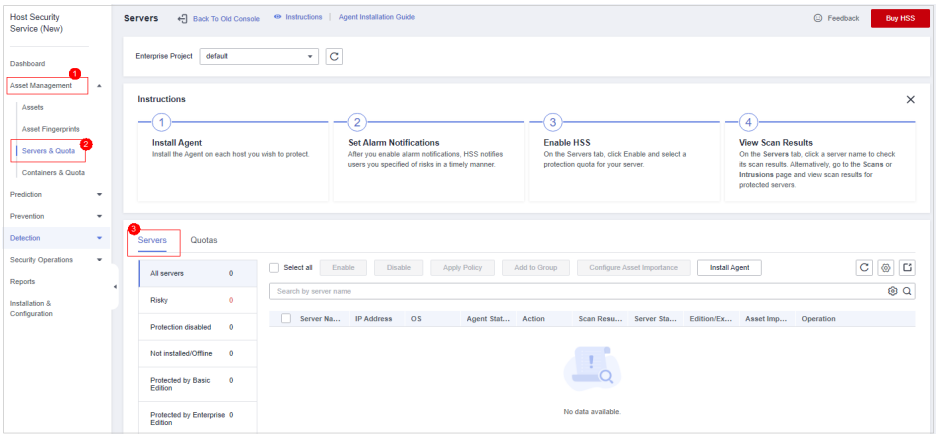
Habilitación de la protección

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 In the navigation pane, choose **Asset Management** > **Servers**. The server list is displayed.

Figura 1-6 Lista de servidores



NOTA

La lista de servidores muestra el estado de protección de solo los siguientes servidores:

- Servidores Huawei Cloud comprados en la región seleccionada
- Servidores que no son de Huawei Cloud agregados a la región seleccionada

Paso 4 Seleccione el servidor de destino y haga clic en **Enable**.

Puede comprar HSS en modo **On-demand** o **Yearly/Monthly**.

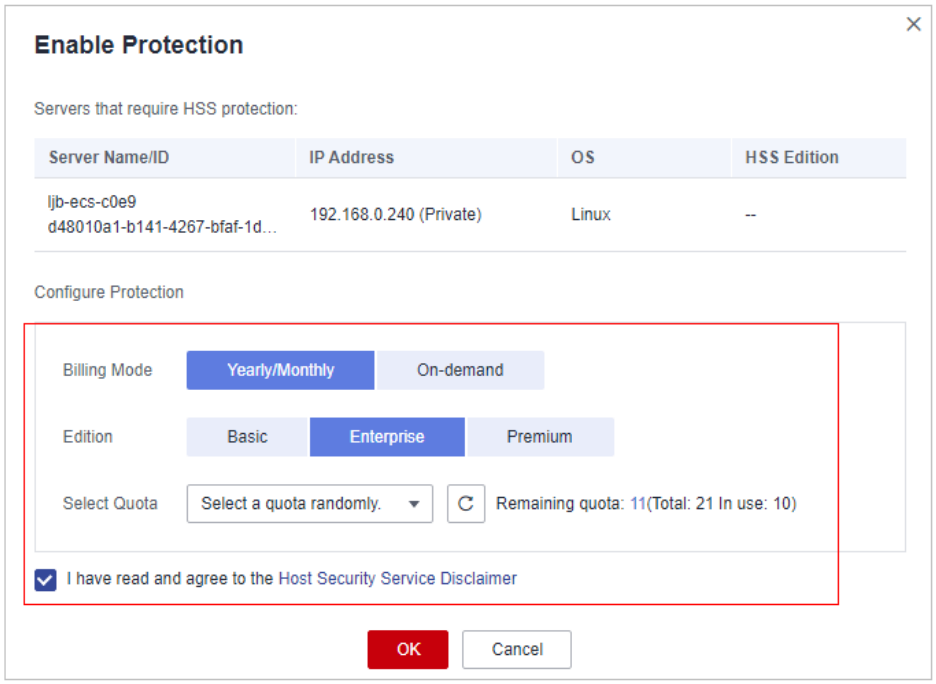
NOTA

On-demand: solo se admiten las ediciones empresariales y básicas. La edición básica se puede utilizar de forma gratuita durante 30 días. El modo anual/mensual de la edición básica solo se puede utilizar después de la compra. Para obtener más información, consulte **Comprar cuota de HSS**.

- Anual/Mensual

  En el cuadro de diálogo que se muestra, seleccione una edición, seleccione el modo **Yearly/Monthly**, asigne la cuota HSS y seleccione **I have read and agree to the Host Security Service Disclaimer**, como se muestra en **Figura 1-7**.

Figura 1-7 Habilitar HSS anual/mensual



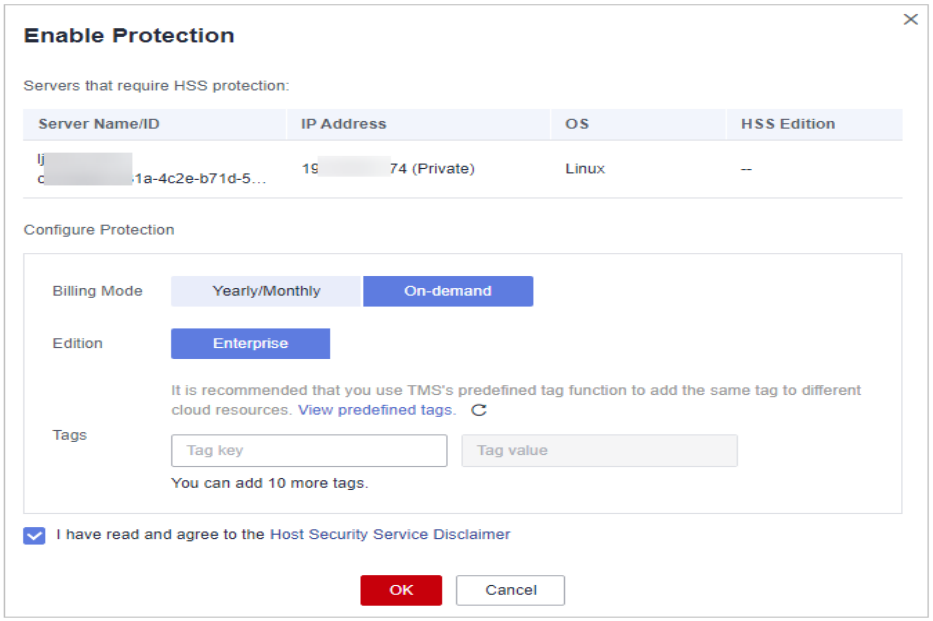
Las cuotas se pueden asignar de las siguientes maneras:

– Seleccione **Select a quota randomly.**. para permitir que el sistema asigne la cuota con la validez restante más larga al servidor.
– Seleccione un ID de cuota y asignelo a un servidor.
– Habilite la protección de servidores en lotes. El sistema asignará automáticamente la cuota a ellos.

- On-demand

  En el cuadro de diálogo que se muestra, seleccione el modo **On-demand**, seleccione la edición y seleccione **I have read and agree to the Host Security Service Disclaimer**, como se muestra en **Figura 1-8**.

Figura 1-8 Habilitación de on-demand HSS



NOTA

Si compra la edición básica en modo bajo demanda por primera vez, cada uno de sus servidores puede disfrutar de una prueba gratuita de HSS durante 30 días. Una vez finalizado el período de prueba, solo podrá utilizar HSS después de la compra.

Paso 5 Haga clic en **OK**. Vea el estado de protección del servidor en la lista de servidores.

Si el **Protection Status** del servidor de destino está **Enabled**, se ha habilitado la edición basic, , empresarial, o premium.

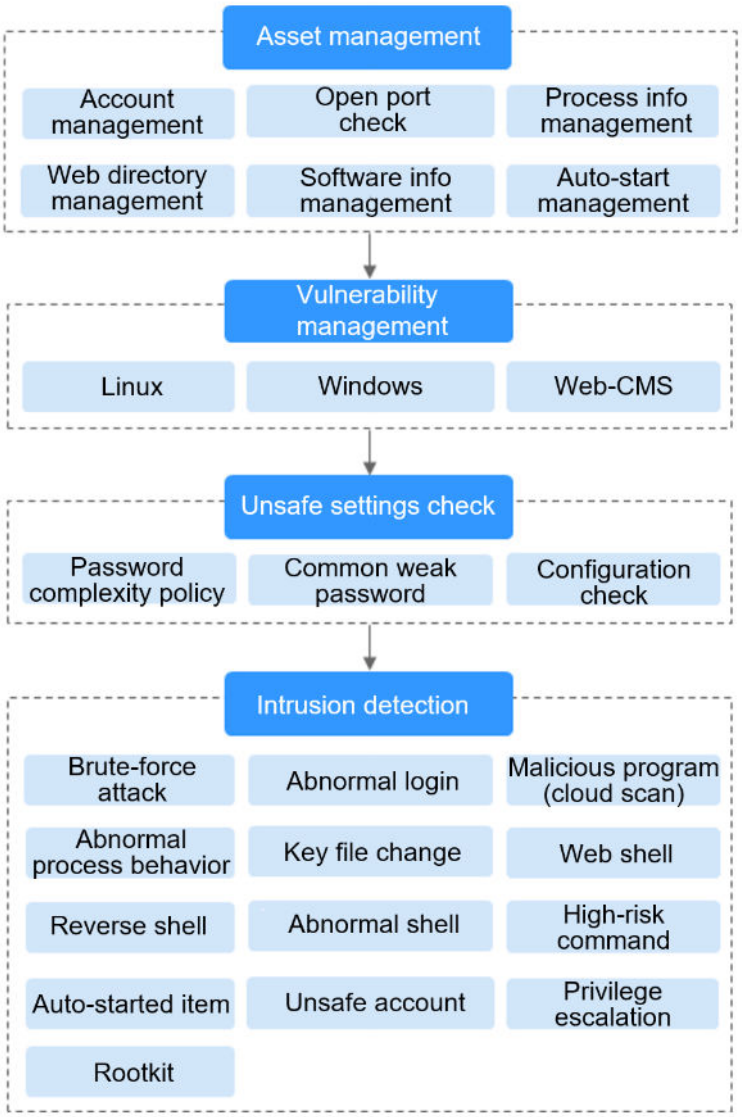
NOTA

- Como alternativa, en la pestaña **Quotas** de la página **Servers & Quota** , haga clic en **Bind Server** en la columna **Operation** para enlazar una cuota a un servidor. HSS habilitará automáticamente la protección para el servidor.
- Una cuota puede estar vinculada a un servidor para protegerla, a condición de que el agente en el servidor esté en línea.

Después de habilitar HSS, analizará sus servidores en busca de problemas de seguridad. Los elementos de verificación varían según la edición que haya habilitado. **Figura 1-9** ilustra más detalles.

Para obtener más información sobre las diferencias entre ediciones, consulte **Ediciones**.

Figura 1-9 Artículos de control de seguridad automático



----Fin

Consulta de detalles de detección

Una vez habilitada la protección del servidor, HSS realizará inmediatamente una detección completa en el servidor. La detección puede llevar mucho tiempo.

A la izquierda de la lista de protección, haga clic en **Risky**.

Haga clic en un nombre de servidor para ir a la página de detalles. En esta página, puede comprobar rápidamente la información detectada y los riesgos del servidor.

Operación de seguimiento

Puede configurar manualmente los elementos de comprobación, como se muestra en **Figura 1-10**. Los elementos configurables varían según la edición que haya habilitado.

Para obtener más información sobre las diferencias entre versiones, consulte **Ediciones**.

Figura 1-10 Elementos de comprobación manual

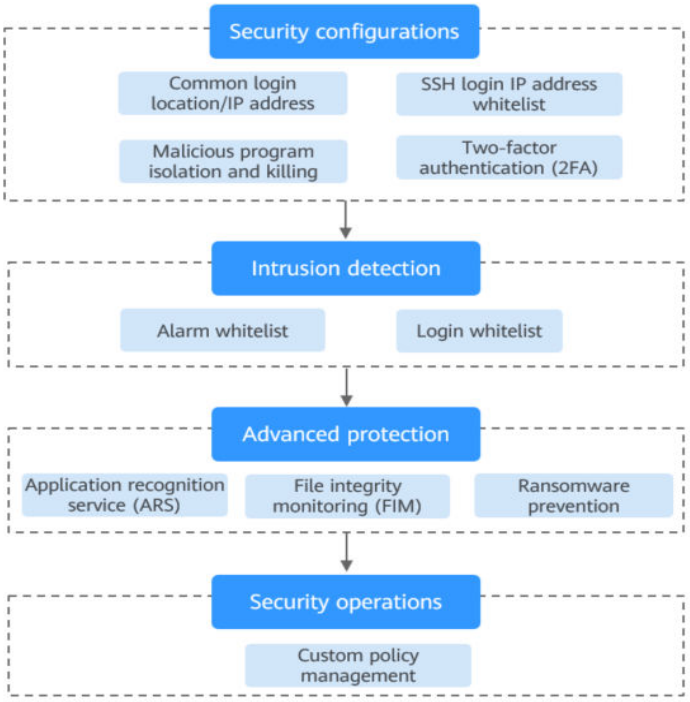


Tabla 1-3 Elementos de comprobación manual

Función	Elemento de comprobación	Referencia
Instalación y configuración	● Ubicación de inicio de sesión común/dirección IP ● Lista blanca de direcciones IP de inicio de sesión SSH ● Aislamiento y eliminación de programas maliciosos	**Configuración de seguridad**
Detección de intrusiones	● Lista blanca de alarmas ● Lista blanca de inicio de sesión	**Configuración de la lista blanca de inicio de sesión**
Protección proactiva	● Supervisión de la integridad de archivos (FIM) ● Prevención de ransomware	**Detección de intrusiones**
Operaciones de seguridad	● Gestión de políticas	**Operaciones de seguridad**
Informe de seguridad	● Denunciar contenido	**Gestión de un informe de seguridad**

Procedimiento posterior

Deshabilitación de HSS

En la pestaña **Server** de la página **Servers & Quotas**, haga clic en **Disable** en la columna **Operation** de un servidor.

Si HSS está deshabilitado, el estado de la cuota de HSS cambiará de ocupado a inactivo. Puede asignar las cuotas inactivas a otros servidores o cancelar la suscripción de las cuotas innecesarias para evitar el desperdicio de cuotas.

AVISO

- Antes de desactivar la protección, realice una detección completa en el servidor, maneje los riesgos conocidos y registre la información de operación para evitar errores y ataques de O&M en el servidor.
- Después de deshabilitar la protección, borre datos importantes en el servidor, detenga aplicaciones importantes en el servidor y desconecte el servidor de la red externa para evitar pérdidas innecesarias causadas por ataques.

Desvinculación de cuota

Elija **Asset Management** > **Servers & Quota**, y haga clic en la pestaña **Quotas**. Haga clic en **Unbind** en la columna **Operation**. El estado de uso de la cuota independiente cambiará de **In use** a **Idle**. HSS deshabilitará automáticamente la protección para el servidor independiente de la cuota.

Puede asignar las cuotas inactivas a otros servidores o cancelar la suscripción de las cuotas innecesarias para evitar el desperdicio de cuotas.

1.4.2 Habilitación de la edición WTP

Antes de habilitar WTP, debe asignar una cuota a un servidor especificado. Si el servicio está deshabilitado o se elimina el servidor, la cuota se puede asignar a otros servidores.

La edición premium se activará cuando se habilita WTP.

Cómo WTP previene la manipulación de páginas web

Tabla 1-4 Mecanismos de protección

Tipo	Mecanismo
Static web page protection	1. Bloqueo de directorio local WTP bloquea los archivos en un directorio de archivos web en una unidad para evitar que los atacantes los modifiquen. Los administradores del sitio web pueden actualizar el contenido del sitio web mediante procesos privilegiados. 2. Copia de respaldo y restauración activas Si WTP detecta que un archivo en un directorio protegido está manipulado, inmediatamente utiliza el archivo de copia de respaldo en el host local para restaurar el archivo. 3. Copia de respaldo y restauración remotas Si un directorio de archivos o un directorio de copia de respaldo del host local no es válido, puede utilizar el servicio de copia de respaldo remota para restaurar la página Web manipulada.
Dynamic web page protection	1. Filtrado de comportamiento malicioso basado en RASP La autoprotección de aplicaciones en tiempo de ejecución (RASP) única de Huawei- detecta los comportamientos de los programas de aplicación, evitando que los atacantes alteren las páginas web a través de programas de aplicación. 2. Control de acceso a archivos de disco de red WTP implementa una gestión detallada para controlar los permisos para agregar, modificar y consultar contenido de archivos en discos de red, evitando la manipulación sin afectar la publicación de contenido del sitio web.

Prerrequisitos

- Elija **Prevention** > **Web Tamper Protection**. Haga clic en la pestaña **Servers**. El **Protection Status** del servidor está **Disabled**.
- Elija **Asset Management** > **Servers & Quota**. El **Agent Status** de un servidor está **Online** y el **Protection Status** está **Disabled**.

Configuración de directorios protegidos

Puede configurar:

- Directorios

  Puede agregar un máximo de 50 directorios protegidos a un host. Para obtener más información, consulte **Adición de un directorio protegido**.

  Para registrar el estado de ejecución del servidor en tiempo real, excluya los archivos de registro del directorio protegido. Puede conceder permisos de lectura y escritura altos para los archivos de registro para evitar que los atacantes vean o manipulen los archivos de registro.

Habilitación de WTP

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Prevention** > **Web Tamper Protection**. En la página **Web Tamper Protection**, haga clic en **Add Server**.

Paso 4 En la página **Add Server**, seleccione el servidor que desea proteger y haga clic en **Add and Enable Protection**.

Paso 5 Vea el estado del servidor en la página **Web Tamper Protection**.

La edición premium se activará cuando se habilita WTP.

- Elija **Prevention** > **Web Tamper Protection**. Si el **Protection Status** del servidor está **Protected**, se ha habilitado WTP.
- Elija **Asset Management** > **Servers & Quota** y haga clic en la pestaña **Servers**. Si el estado de protección del servidor de destino está **Enabled** y la **Edition/Expiration Date** del mismo es **Premium (included with WTP)**, la edición premium proporcionada por la edición WTP se habilita de forma gratuita.

----Fin

AVISO

- Para habilitar la protección WTP para un servidor, también puede elegir Asset Management > **Servers & Quota**, haga clic en la pestaña **Quotas** y haga clic en **Bind Server**.
- Una cuota puede estar vinculada a un servidor para protegerla, a condición de que el agente en el servidor esté en línea.
- Deshabilite WTP antes de actualizar un sitio web y habilítelo una vez completada la actualización. De lo contrario, el sitio web no se actualizará.
- Su sitio web no está protegido mientras WTP está deshabilitado. Habilitar inmediatamente después de actualizar su sitio web.

Procedimiento posterior

Deshabilitación de WTP

Elija **Prevention** > **Web Tamper Protection** y haga clic en la pestaña **Servers**. Haga clic en **Disable Protection** en la columna **Operation** de un servidor.

Si WTP está deshabilitado, su estado de cuota cambiará de ocupado a inactivo. Puede asignar las cuotas inactivas a otros servidores o cancelar la suscripción de las cuotas innecesarias para evitar el desperdicio de cuotas.

AVISO

- Antes de desactivar WTP, realice una detección completa en el servidor, maneje los riesgos conocidos y registre la información de operación para evitar errores y ataques de O&M en el servidor.
- Si WTP está deshabilitado, es más probable que las aplicaciones web sean manipuladas. Por lo tanto, debe eliminar datos importantes en el servidor, detener servicios importantes en el servidor y desconectar el servidor de la red externa de manera oportuna para evitar pérdidas innecesarias causadas por ataques en el servidor.
- Después de desactivar WTP, los archivos del directorio protegido ya no están protegidos. Se recomienda procesar los archivos en el directorio protegido antes de realizar estas operaciones.
- Si encuentra que faltan algunos archivos después de deshabilitar WTP, búsquelos en la ruta de copia de respaldo local o remota.
- La edición premium se desactivará cuando se deshabilite WTP.

Desvinculación de cuota

Elija **Load Management** > **Servers & Quota** y haga clic en la pestaña **Quotas**. Haga clic en **Unbind** en la columna **Operation**. El estado de uso de la cuota independiente cambiará de **In use** a **Idle**. HSS deshabilita automáticamente WTP para los servidores asociados con la cuota.

Puede asignar las cuotas inactivas a otros servidores o cancelar la suscripción de las cuotas innecesarias para evitar el desperdicio de cuotas.

1.5 Habilitación de la protección de nodos de contenedores

Antes de habilitar la protección para un nodo contenedor, debe asignar una cuota a un nodo especificado. Si la protección está deshabilitada o el nodo se elimina, la cuota se puede asignar a otros nodos.

Frecuencia de comprobación

HSS realiza un control completo en la mañana temprano todos los días.

Si habilita la protección del servidor antes del intervalo de comprobación, puede ver los resultados de la comprobación solo después de que se complete la comprobación a las 00:00 del día siguiente.

Prerrequisitos

- El **Agent Status** de un servidor es **Online**. Para comprobar el estado, elija **Host Security Service** > **Asset Management** > **Containers & Quota**.
- Ha creado nodos en CCE.
- El **Protection Status** del nodo es **Unprotected**.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Asset Management** > **Containers & Quota**. Se muestra la página de descripción general del contenedor.

Paso 4 En la columna **Operation** de la lista de nodos, haga clic en **Enable Protection**.

Paso 5 Puede comprar la cuota en modo de pago por uso o anual/mensual.

- Anual/Mensual

  En el cuadro de diálogo que se muestra, seleccione **Yearly/Monthly**, lea el *Container Guard Service Disclaimer* y seleccione **I have read and agreed to Container Guard Service Disclaimer**.

- Pago por uso

  En el cuadro de diálogo que se muestra, seleccione **pay-per-use**, lea *Container Guard Service Disclaimer* y seleccione **I have read and agreed to Container Guard Service Disclaimer**.

Paso 6 Haga clic en **OK** para habilitar la protección para el nodo. Si el **Protection Status** del nodo está **Enabled**, se ha habilitado la protección para el nodo.

NOTA

- Durante la compra, establezca **Node Quantity** en el número de nodos que desea proteger.

----Fin

Procedimiento posterior

Desactivación de la protección para un nodo

Elija **Asset Management** > **Containers & Quota**, haga clic en la pestaña **Container Nodes** y haga clic en **Nodes**. En la columna **Operation**, haga clic en **Disable Protection**.

Si la protección está deshabilitada, el estado de la cuota cambiará de ocupado a inactivo. Puede asignar la cuota inactiva a otro nodo o cancelar la suscripción a la cuota innecesaria para evitar el desperdicio de cuota.

AVISO

- Antes de desactivar la protección, realice una detección completa en el contenedor, maneje los riesgos detectados y registre la información de operación para evitar errores de operación y ataques en el contenedor.
- Después de deshabilitar la protección, borre datos importantes en el contenedor, detenga aplicaciones importantes en el contenedor y desconecte el contenedor de la red externa para evitar pérdidas innecesarias causadas por ataques.

1.6 (Opcional) Cambio de la edición HSS

Puede cambiar la edición HSS a la edición básica (pago por uso o anual/mensual), la edición empresarial (pago por uso o anual/mensual) o la edición premium.

NOTA

- Las ediciones HSS no se pueden cambiar por lotes.
- Al comprar un ECS, puede habilitar la protección en la edición básica o empresarial. HSS instalará su agente en el ECS y habilitará la edición seleccionada, facturada en modo de pago por uso. Puede cambiar al modo de facturación anual/mensual cambiando la edición.

Precauciones

- De pago por uso a anual/mensual

  Se generará un pedido de paquete anual/mensual para usted. La cuota anual/mensual estará disponible inmediatamente cuando complete el pago. Para habilitar la cuota anual/mensual, elija **Servers & Quota** y haga clic en la pestaña **Servers**. En la columna **Operation** del servidor requerido, haga clic en **Enable** y seleccione la cuota anual/mensual.
- De anual/mensual a pago por uso

  Elija **Servers & Quota** y haga clic en la pestaña **Servers**. En la columna **Operation** del servidor requerido, haga clic en **Enable** y seleccione la cuota de pago por uso.
- Si se cambia HSS de una edición superior a una edición inferior, los servidores protegidos serán más vulnerables a los ataques.
- Puede cambiar de otras ediciones a la edición básica, empresarial o premium. Para utilizar la edición WTP o CGS, debe comprarla y habilitarla por separado.

Preparación para el conmutador de edición

- Elija **Host Security Service** > **Asset Management** > **Servers & Quota** y haga clic en la pestaña **Servers**. Compruebe que el **Agent Status** del servidor requerido está **Online** y que la protección se ha habilitado para el servidor.
- Compre cuotas anuales/mensuales requeridas.
- Antes de cambiar a una edición inferior, compruebe el servidor, gestione los riesgos conocidos y registre la información de operación para evitar errores y ataques de O&M.

Ediciones de conmutación

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Asset Management** > **Servers**.

NOTA

Probablemente estás en la región equivocada. Solo se muestran los siguientes servidores en la consola:

- Servidores Huawei Cloud comprados en la región seleccionada
- Servidores que no son de Huawei Cloud agregados a la región seleccionada

Paso 4 En la columna **Operation** de un servidor, haga clic en **Switch Edition**.

NOTA

- Para cambiar entre los modos de facturación en la edición básica o empresarial, deshabilite la protección y, a continuación, elija el modo de facturación deseado cuando vuelva a activar la protección.

Puede cambiar a una edición HSS en modo de pago por uso o anual/mensual.

- Anual/Mensual

  En el cuadro de diálogo que se muestra, seleccione una edición, seleccione el modo anual/mensual, asigne la cuota HSS y seleccione **I have read and agree to the Host Security Service Disclaimer**.

- Pago por uso

  En el cuadro de diálogo que se muestra, seleccione **Pay-per-use**, seleccione una edición y seleccione **I have read and agree to the Host Security Service Disclaimer**.

Paso 5 Haga clic en **OK**. La información de la edición en la columna **Edition** se actualizará.

Si se actualiza la información de **Edition** en la columna Edición, el modificador de edición se realiza correctamente.

----Fin

Procedimiento posterior

- Después de cambiar a una edición inferior, borre datos importantes en el servidor, detenga aplicaciones importantes en el servidor y desconecte el servidor de la red externa para evitar pérdidas innecesarias causadas por ataques.
- Después de cambiar a una edición superior, realice una detección de seguridad en el servidor, maneje los riesgos de seguridad en el servidor y configure las funciones necesarias de manera oportuna.
- Después de cambiar la edición, puede asignar las cuotas inactivas a otros servidores o cancelar la suscripción de las cuotas innecesarias para evitar el desperdicio de cuotas.

1.7 Habilitación de notificaciones de alarma

Después de activar la notificación de alarma, puede recibir notificaciones de alarma enviadas por HSS para obtener información sobre los riesgos de seguridad que enfrentan sus servidores y páginas web. Sin esta función, debe iniciar sesión en la consola de gestión para ver las alarmas.

- La configuración de notificación de alarma solo es efectiva para la región actual. Para recibir notificaciones de otra región, cambie a esa región y configure la notificación de alarma.
- Las notificaciones de alarma pueden estar bloqueadas por error. Si ha habilitado las notificaciones pero no ha recibido ninguna, compruebe si se han bloqueado como espasmos.
- El servicio Simple Message Notification (SMN) es un servicio de pago. Para obtener más información sobre el precio, consulte **Detalles de precios del producto**.

Prerrequisitos

Antes de configurar la notificación de alarma,

- Si configura **Alarm Receiving Settings** en **Use Message Center settings**, para configurar los destinatarios, vaya al Centro de mensajes y elija **Message Receiving Management** > **SMS & Email Settings**. En el área **Security**, haga clic en **Modify** en la fila donde reside **Security event**.

- Si configura **Alarm Receiving Settings** en **Use SMN topic settings**, se recomienda crear un tema de mensaje en el servicio SMN como administrador. Para obtener más información, consulte **Publicación de un mensaje**.

Habilitación de notificaciones de alarma

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Installation & Configuration** y haga clic en **Alarm Notifications**. **Tabla 1-5** describe los parámetros.

Tabla 1-5 configuraciones de alarma

Tipo	Descripción	Sugerencia
Notificación diaria de alarma	HSS escanea las cuentas, directorios web, vulnerabilidades, programas maliciosos y configuraciones clave en el sistema servidor a las 00:00 todos los días, y envía los resultados de detección resumidos a los destinatarios que ha establecido en el Centro de mensajes o SMN, dependiendo de cuál haya elegido. Para ver los elementos de notificación, haga clic en **View Default Daily Notification Events**.	• Se recomienda que reciba y revise periódicamente todo el contenido de la notificación diaria de alarma para eliminar los riesgos de manera oportuna. • Las notificaciones de alarma diarias contienen una gran cantidad de elementos de verificación. Si desea enviar las notificaciones a los destinatarios establecidos en un tema SMN, le recomendamos que establezca el protocolo del tema en **Email**.
Notificación de alarma en tiempo real	Cuando un atacante intruye un servidor, las alarmas se envían a los destinatarios que ha establecido en el Centro de mensajes o SMN, dependiendo de cuál haya elegido. Para ver los elementos de notificación, haga clic en **View Default Real-time Notification Events**.	• Se recomienda que reciba todo el contenido en la notificación de alarma en tiempo real y verlos a tiempo. El sistema HSS monitoriza la seguridad de los servidores en tiempo real, detecta la intrusión del atacante y envía notificaciones de alarma en tiempo real para que pueda manejar rápidamente el problema. • Las notificaciones de alarma en tiempo real se refieren a problemas urgentes. Si desea enviar las notificaciones a los destinatarios establecidos en un tema SMN, le recomendamos que establezca el protocolo de tema en **SMS**.

Tipo	Descripción	Sugerencia
Severidad	Seleccione las gravedades de las alarmas de las que desea que se le notifique.	Todos
Eventos enmascarados	Seleccione los eventos de los que no desea que se le notifique. Seleccione los eventos que se van a enmascarar en el cuadro de lista desplegable.	-

Paso 4 Seleccione el modo de notificación de alarma.

- Usar la configuración del Centro de mensajes

  De forma predeterminada, las notificaciones de alarma se envían a los destinatarios especificados en el centro de mensajes. Puede iniciar sesión en su cuenta para comprobar la configuración de su destinatario

  Para configurar los destinatarios, haga clic en **Message Receive Management** para ir al Centro de mensajes. Elija **Message Receiving Management** > **SMS & Email Settings**. En la categoría **Security**, haga clic en **Modify** en la fila donde reside **Security event**.

- Usar la configuración del tema SMN

  Seleccione un tema disponible en la lista desplegable o haga clic en **View Topics** y crear un tema.

  Para crear un tema, es decir, para configurar un número de teléfono móvil o una dirección de correo electrónico para recibir notificaciones de alarma, realice los siguientes pasos:

  a. Crear un tema. Para obtener más información, consulte **Creación de un tema**.

  b. Configure el número de teléfono móvil o la dirección de correo electrónico para recibir notificaciones de alarma, es decir, agregue una o más suscripciones para el tema creado. Para obtener más información, consulte **Adición de una suscripción**.

  c. Confirme la suscripción. Después de agregar la suscripción, confirme la suscripción según lo indique el mensaje SMS o correo electrónico recibido.

     El mensaje de confirmación sobre la suscripción a un tema puede ser considerado como spam. Si no recibe el mensaje, compruebe si se intercepta como spam.

  Puede crear varios temas de notificación basados en el plan O&M y el tipo de notificación de alarma para recibir diferentes tipos de notificaciones de alarma. Para obtener más información acerca de los temas y suscripciones, consulte la *Guía del usuario de Simple Message Notification*.

Paso 5 Haga clic en **Apply**. Se mostrará un mensaje indicando que la notificación de alarma se ha configurado correctamente.

----Fin

Notificaciones de alarmas

Tipo	Artículo	Descripción
Daily Alarm Notifications El servicio comprueba los riesgos en sus servidores a primera hora de la mañana todos los días, resume y recopila los resultados de la detección, y envía los resultados a su teléfono móvil o buzón de correo electrónico a las 10:00 todos los días.		
Activos	Puerto peligroso	Compruebe si hay puertos abiertos de alto riesgo y puertos innecesarios.
Vulnerabilidades	Vulnerabilidades críticas	Detectar vulnerabilidades críticas y corregirlas de manera oportuna.
Configuración insegura	Configuraciones inseguras	Detecte configuraciones inseguras de aplicaciones clave que probablemente serán explotadas por hackers informáticos para entrometerse en los servidores.
	Contraseñas débiles comunes	Detecte contraseñas débiles en MySQL, FTP y cuentas del sistema.
Intrusiones	Malware	Comprobar y manejar programas maliciosos detectados en un solo lugar, incluyendo web shells, caballos de Troya, software de minería, gusanos y virus.
	Webshell	Puede comprobar si los archivos (a menudo archivos PHP y JSP) en sus directorios web son shells web. ● La información del shell web incluye la ruta del archivo troyano, el estado, la primera hora de descubrimiento y la última hora de descubrimiento. Puede optar por ignorar la advertencia en los archivos de confianza. ● Puede utilizar la función de detección manual para detectar web shells en los servidores.
	Reverse shell	Supervise los comportamientos de los procesos del usuario en tiempo real para detectar shells inversos causados por conexiones no válidas. Se pueden detectar shells inversos para protocolos como TCP, UDP e ICMP.
	Escalada de privilegios de archivo	Compruebe las escalaciones de privilegios de archivo en su sistema.
	Escalada de privilegios de proceso	Se pueden detectar las siguientes operaciones de escalada de privilegios de proceso: ● Escalada de privilegios de root mediante la explotación de las vulnerabilidades del programa SUID ● Escalada de privilegios de root mediante la explotación de vulnerabilidades del kernel

Tipo	Artículo	Descripción
	Cambio de archivo crítico	Reciba alarmas cuando se modifiquen archivos críticos del sistema.
	Cambios de archivo/ directorio	Se supervisan los archivos y directorios del sistema. Cuando se modifica un archivo o directorio, se genera una alarma que indica que el archivo o directorio puede ser manipulado.
	Detección de comportamiento de proceso anormal	Compruebe los procesos en los servidores, incluidos sus identificadores, líneas de comandos, rutas de proceso y comportamiento. Envíe alarmas sobre operaciones e intrusiones de procesos no autorizados. Se puede detectar el siguiente comportamiento anormal del proceso: ● Uso anormal de la CPU ● Procesos que acceden a direcciones IP maliciosas ● Aumento anormal de las conexiones de proceso simultáneo
	Ejecución de comandos de alto riesgo	Compruebe los comandos ejecutados en tiempo real y genere alarmas si se detectan comandos de alto riesgo.
	Abnormal shell	Detecte acciones en shells anormales, como mover, copiar y eliminar archivos de shell, y modificar los permisos de acceso y los enlaces duros de los archivos.
	Ataque de fuerza bruta	Compruebe si hay intentos de ataque de fuerza bruta y ataques de fuerza bruta exitosos. ● Sus cuentas están protegidas de ataques de fuerza bruta. HSS bloqueará los hosts atacantes cuando detecte tales ataques. ● Activar una alarma si un usuario inicia sesión mediante un ataque de fuerza bruta.
	Inicio de sesión anormal	Compruebe y maneje los inicios de sesión remotos. Si la ubicación de inicio de sesión de un usuario no es una ubicación de inicio de sesión común que establezca, se activará una alarma.
	Cuentas no válidas	Escanee las cuentas de los servidores y enumere las cuentas sospechosas de manera oportuna.
	Escapes de vulnerabilidad	El servicio informa de una alarma si detecta un comportamiento de proceso de contenedor que coincide con el comportamiento de vulnerabilidades conocidas (como el Dirty COW, brute-force attack, runC, y shocker).

Tipo	Artículo	Descripción
	Escapes de archivos	El servicio informa de una alarma si detecta que un proceso contenedor accede a un directorio de archivos clave (por ejemplo, **/etc/shadow** o **/etc/crontab**). Los directorios que cumplen con las reglas de asignación de directorios de contenedores también pueden activar tales alarmas.
	Procesos de contenedores anormales	Los servicios de contenedores suelen ser simples. Si está seguro de que sólo se ejecutan procesos específicos en un contenedor, puede agregar los procesos a la lista blanca de una política y asociarla con el contenedor. El servicio informa de una alarma si detecta que un proceso que no está en la lista blanca se está ejecutando en el contenedor.
	Inicios anormales de contenedores	Compruebe si hay configuraciones de parámetros inseguras utilizadas durante el inicio del contenedor. Algunos parámetros de inicio especifican permisos de contenedor. Si su configuración es inapropiada, los atacantes pueden aprovecharlos para entrometerse en contenedores.
	Llamadas al sistema de alto riesgo	Los usuarios pueden ejecutar tareas en núcleos mediante llamadas al sistema Linux. El servicio informa de una alarma si detecta una llamada de alto riesgo, como **open_by_handle_at**, **ptrace**, **setns**, y **reboot**.
	Acceso a archivos confidenciales	Detectar comportamientos de acceso sospechosos (como la escalada de privilegios y la persistencia) en archivos importantes.
	Minería	Detecte intrusiones, como software incluido, ataques de fuerza bruta y bypass de autenticación.
Notificaciones de alarma en tiempo real Cuando se produce un evento, se envía inmediatamente una notificación de alarma.		
Intrusiones	Programas maliciosos	Comprobar y manejar programas maliciosos detectados en un solo lugar, incluyendo web shells, troyanos, software de minería, gusanos y virus.
	Webshell	Puede comprobar si los archivos (a menudo archivos PHP y JSP) en sus directorios web son shells web. ● La información del shell web incluye la ruta del archivo troyano, el estado, la primera hora de descubrimiento y la última hora de descubrimiento. Puede optar por ignorar la advertencia en los archivos de confianza. ● Puede utilizar la función de detección manual para detectar web shells en los servidores.

Tipo	Artículo	Descripción
	Reverse shell	Supervise los comportamientos de los procesos del usuario en tiempo real para detectar shells inversos causados por conexiones no válidas. Se pueden detectar shells inversos para protocolos como TCP, UDP e ICMP.
	Escalada de privilegios de archivo	Compruebe las escalaciones de privilegios de archivo en su sistema.
	Escalada de privilegios de proceso	Se pueden detectar las siguientes operaciones de escalada de privilegios de proceso: ● Escalada de privilegios de root mediante la explotación de las vulnerabilidades del programa SUID ● Escalada de privilegios de root mediante la explotación de vulnerabilidades del kernel
	Cambio de archivo crítico	Reciba alarmas cuando se modifiquen archivos críticos del sistema.
	Cambios de archivo/ directorio	Se supervisan los archivos y directorios del sistema. Cuando se modifica un archivo o directorio, se genera una alarma que indica que el archivo o directorio puede ser manipulado.
	Detección de comportamiento de proceso anormal	Compruebe los procesos en los servidores, incluidos sus identificadores, líneas de comandos, rutas de proceso y comportamiento. Envíe alarmas sobre operaciones e intrusiones de procesos no autorizados. Se puede detectar el siguiente comportamiento anormal del proceso: ● Uso anormal de la CPU ● Procesos que acceden a direcciones IP maliciosas ● Aumento anormal de las conexiones de proceso simultáneo
	Detección de ejecución de comandos de alto riesgo	Compruebe los comandos ejecutados en tiempo real y genere alarmas si se detectan comandos de alto riesgo.
	Detección de shell anormales	Detecte acciones en shells anormales, como mover, copiar y eliminar archivos de shell, y modificar los permisos de acceso y los enlaces duros de los archivos.

Tipo	Artículo	Descripción
	Estadística de excepción	Compruebe y maneje los inicios de sesión remotos. Si la ubicación de inicio de sesión de un usuario no es una ubicación de inicio de sesión común que establezca, se activará una alarma.
	Cuentas no válidas	Escanee las cuentas de los servidores y enumere las cuentas sospechosas de manera oportuna.
	Escapes de vulnerabilidad	El servicio informa de una alarma si detecta un comportamiento de proceso de contenedor que coincide con el comportamiento de vulnerabilidades conocidas (como el Dirty COW, brute-force attack, runC, y shocker).
	Escapes de archivos	El servicio informa de una alarma si detecta que un proceso contenedor accede a un directorio de archivos clave (por ejemplo, **/etc/shadow** o **/etc/crontab**). Los directorios que cumplen con las reglas de asignación de directorios de contenedores también pueden activar tales alarmas.
	Procesos de contenedores anormales	Los servicios de contenedores suelen ser simples. Si está seguro de que sólo se ejecutan procesos específicos en un contenedor, puede agregar los procesos a la lista blanca de una política y asociarla con el contenedor. El servicio informa de una alarma si detecta que un proceso que no está en la lista blanca se está ejecutando en el contenedor.
	Inicios anormales de contenedores	Compruebe si hay configuraciones de parámetros inseguras utilizadas durante el inicio del contenedor. Algunos parámetros de inicio especifican permisos de contenedor. Si su configuración es inapropiada, los atacantes pueden aprovecharlos para entrometerse en contenedores.
	Llamadas al sistema de alto riesgo	Los usuarios pueden ejecutar tareas en núcleos mediante llamadas al sistema Linux. El servicio informa de una alarma si detecta una llamada de alto riesgo, como **open_by_handle_at**, **ptrace**, **setns**, y **reboot**.
	Acceso a archivos confidenciales	Detectar comportamientos de acceso sospechosos (como la escalada de privilegios y la persistencia) en archivos importantes.
	Minería	Detecta intrusiones, como software incluido, ataques de fuerza bruta y bypass de autenticación.

1.8 Configuración de seguridad

Después de habilitar la protección, puede configurar las ubicaciones de inicio de sesión comunes, las direcciones IP de inicio de sesión comunes y la lista blanca de direcciones IP de inicio de sesión SSH. También puede habilitar el aislamiento automático y la eliminación de programas maliciosos.

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

----Fin

Configuración de ubicaciones de inicio de sesión comunes

Después de configurar ubicaciones de inicio de sesión comunes, HSS generará alarmas en los inicios de sesión desde otras ubicaciones de inicio de sesión. Se puede agregar un servidor a múltiples ubicaciones de inicio de sesión.

Paso 1 En la pestaña **Common Login Locations**, haga clic en **Add Common Login Location**.

Paso 2 En el cuadro de diálogo que se muestra, configure la ubicación y los servidores.

----Fin

Configuración de direcciones IP de inicio de sesión comunes

Después de configurar direcciones IP comunes, HSS generará alarmas en los inicios de sesión desde otras direcciones IP.

Paso 1 En la pestaña **Common Login IP Addresses**, haga clic en **Add Common Login IP Address**.

Paso 2 En el cuadro de diálogo que se muestra, configure la dirección IP de inicio de sesión y los servidores.

NOTA

Una dirección IP de inicio de sesión común debe ser una dirección IP pública o un segmento de dirección IP. De lo contrario, no puede iniciar sesión remotamente en el servidor en modo SSH.

----Fin

Configuración de una lista blanca de direcciones IP de inicio de sesión SSH

La lista blanca de inicio de sesión SSH controla el acceso SSH a los servidores, evitando efectivamente el agrietamiento de la cuenta.

Después de configurar una lista blanca de direcciones IP de inicio de sesión SSH, los inicios de sesión SSH solo se permitirán desde direcciones IP de la lista blanca.

- Antes de habilitar esta función, asegúrese de que todas las direcciones IP que necesitan iniciar los inicios de sesión SSH se agreguen a la lista blanca. De lo contrario, no puede iniciar sesión remotamente en su servidor usando SSH.

Si su servicio necesita acceder a un servidor, pero no necesariamente a través de SSH, no necesita agregar su dirección IP a la lista blanca.

- Tenga cuidado al agregar una dirección IP a la lista blanca. Esto hará que HSS ya no restrinja el acceso desde esta dirección IP a sus servidores.

NOTA

La lista blanca de direcciones IP SSH no tiene efecto para los servidores que ejecutan Kunpeng EulerOS (EulerOS with ARM).

Paso 1 En la pestaña **SSH IP Whitelist**, haga clic en **Add IP Address**.

Paso 2 En el cuadro de diálogo **Add IP Address**, introduzca una dirección IP y seleccione servidores.

NOTA

Una dirección IP de la lista blanca debe ser una dirección IP pública o un segmento de dirección IP (las direcciones IPv4 e IPv6 son compatibles). De lo contrario, no puede iniciar sesión remotamente en el servidor en modo SSH.

----Fin

Aislamiento y eliminación de programas maliciosos

HSS aísla y elimina automáticamente los programas maliciosos identificados, como shells web, troyanos y gusanos, eliminando los riesgos de seguridad.

En la pestaña **Isolation and Killing of Malicious Programs**, haga clic en  .

El aislamiento automático y la matanza pueden causar falsos positivos. Puede elegir **Intrusions** > **Events** para ver programas maliciosos aislados. Puede cancelar el aislamiento o ignorar los programas maliciosos mal informados. Para más detalles, consulte **Comprobación y manejo de alarmas de servidor**.

AVISO

- Cuando un programa se aísla y finaliza, el proceso del programa finaliza inmediatamente. Para evitar el impacto en los servicios, verifique el resultado de la detección y cancele el aislamiento de los programas maliciosos (si los hay).
- Si **Isolate and Kill Malicious Programs** se establece en **Disable** en la pestaña **Isolation and Killing of Malicious Programs**, HSS generará una alarma cuando detecte un programa malicioso.

  Para aislar y eliminar los programas maliciosos que desencadenaron alarmas, elija **Intrusions** > **Events** y haga clic en **Malicious program**.

Habilitación de 2FA

- 2FA requiere que los usuarios proporcionen códigos de verificación antes de iniciar sesión. Los códigos se enviarán a sus teléfonos móviles o casillas de correo electrónico.
- Tiene que elegir un tema SMN para los servidores donde 2FA está habilitado. El tema especifica los destinatarios de los códigos de verificación de inicio de sesión, y HSS autenticará a los usuarios de inicio de sesión en consecuencia.

Prerrequisitos:

- Ha creado un tema de mensaje cuyo protocolo es SMS o correo electrónico.
- Se ha habilitado la protección del servidor.
- Los servidores Linux requieren contraseñas de usuario para iniciar sesión.
- Para habilitar la autenticación de dos factores, debe deshabilitar el firewall SELinux.
- En un servidor Windows, 2FA puede entrar en conflicto con G01 y 360 Guard (edición de servidor). Se aconseja que los detengas.

Restricciones y limitaciones

- Si 2FA está habilitado, no puede iniciar sesión en los servidores que ejecutan un sistema operativo Linux GUI.
- Si ha habilitado 2FA en un servidor Linux, no puede iniciar sesión a través de CBH.
- Si ha habilitado 2FA en un servidor, no puede iniciar sesión en el servidor a través de CloudShell.
- 2FA solo se admite cuando la versión OpenSSH de Linux es anterior a 8.

Procedimiento

Paso 1 En la pestaña **Two-Factor Authentication**, seleccione un servidor y haga clic en **Enable 2FA**.

Paso 2 En el cuadro de diálogo **Enable 2FA** que se muestra, seleccione un modo de autenticación.

- **SMS/Email**

  Debe seleccionar un tema SMN para la verificación de SMS y correo electrónico.

  – La lista desplegable muestra solo los temas de notificación que se han confirmado.

  – Si no hay ningún tema, haga clic en **View** para crear uno. Para obtener más información, consulte **Creación de un tema**.

  – Durante la autenticación, todos los números de teléfono móvil y direcciones de correo electrónico especificadas en el tema recibirán un SMS o correo electrónico de verificación. Puede eliminar números de teléfono móvil y direcciones de correo electrónico que no necesitan recibir mensajes de verificación.

- **Código de verificación**

  Utilice el código de verificación que recibe en tiempo real para la verificación.

Paso 3 Haga clic en **OK**. Después de que 2FA está habilitado, la configuración toma aproximadamente 5 minutos para que surta efecto.

AVISO

Cuando inicia sesión en un servidor Windows remoto desde otro servidor Windows donde 2FA está habilitado, debe agregar manualmente credenciales en este último. De lo contrario, el inicio de sesión fallará.

Para agregar credenciales, elija **Start** > **Control Panel**, y haga clic en **User Accounts**. Haga clic en **Manage your credentials** y, a continuación, haga clic en **Add a Windows credential**. Agregue el nombre de usuario y la contraseña del servidor remoto al que desea acceder.

----Fin

2 Descripción General de Riesgos

En la página del panel de control de la consola HSS, puede conocer el estado de seguridad y los riesgos de todos sus servidores y contenedores en tiempo real, incluido el índice de riesgo, la tendencia de riesgo, los 5 tipos de eventos principales y la cuota de servicio.

NOTA

Si ha habilitado la función de proyecto de empresa, puede seleccionar su proyecto de empresa en la lista desplegable **Enterprise project** para comprobar la visión general de riesgo del servidor del proyecto. Si selecciona **All projects**, se muestra la visión general de riesgos de los servidores en todos los proyectos de esta región.

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Dashboard**.

----Fin

Índice de riesgo de activos (últimas 24 horas)

Puede comprobar los riesgos en servidores y contenedores protegidos en las últimas 24 horas.

Para manejar los riesgos, haga clic en **Handle Now**. El panel **Risks** se mostrará a la derecha. Puede manejar los riesgos consultando la guía correspondiente. Puede manejar los siguientes tipos de riesgos:

- Intrusiones
- Vulnerabilidades
- Configuración insegura
- Riesgos de contenedores

Para comprobar la seguridad de los activos, haga clic en **Scan**.

Estado de protección (últimas 24 horas)

Puede comprobar el número de servidores y nodos protegidos y desprotegidos.

Para habilitar la protección de un servidor, haga clic en **Enable Protection**.

Riesgos (últimas 24 horas)

Puede comprobar el número de riesgos de activos de servidor, vulnerabilidades de servidor, líneas de base de servidor y riesgos de contenedores, y su comparación con el día anterior.

Estadísticas de Riesgos

Puedes comprobar la tendencia de riesgo en las últimas 24 horas, los últimos 3 días, los últimos 7 días y los últimos 30 días.

Tabla 2-1 Estadísticas de riesgos

Categoría	Carrera
Riesgos de activos	● Cuentas ● Puertos abiertos ● Gestor de procesos ● Directorios web ● Software instalado ● Inicio automático
Vulnerabilidades	● Vulnerabilidades Linux ● Vulnerabilidades de Windows ● Vulnerabilidades de CMS web
Riesgos de referencia	● Comprobación de políticas de complejidad de contraseñas ● Comprobación de contraseña débil común ● Comprobación de configuración
Riesgos de contenedores	● Vulnerabilidad de imagen local ● Vulnerabilidades de imagen privada ● Archivos maliciosos en imágenes ● Línea base de la imagen

Intrusiones (últimas 24 horas)

Puede comprobar el número total de intrusiones detectadas en servidores y contenedores, y las gravedades de las intrusiones.

Estas estadísticas de intrusión se actualizan a las 00:00 todos los días.

Los 5 mejores eventos

Para servidores protegidos por la edición básica, empresarial, premium o CGS, puede consultar los 5 principales tipos de eventos de intrusión detectados en las últimas 24 horas, los últimos 3 días, los últimos 7 días o los últimos 30 días; y el número de cada tipo de eventos.

A las 00:00 de cada mañana, se recopilan las estadísticas sobre los riesgos del servidor detectados en los últimos 30 días, los 5 eventos principales y el número de cada tipo de eventos.

Si no se muestran datos debido a problemas de conexión, corrija la red y haga clic en  para recuperar datos de nuevo.

Alarmas en tiempo real

Puede comprobar las alarmas en tiempo real.

Compruebe los últimos cinco eventos de intrusión no controlados en las últimas 24 horas, incluyendo sus gravedades, nombres de alarmas, tiempo de ocurrencia y estados.

- Para comprobar los detalles de la alarma, haga clic en un nombre de alarma.
- Para controlar una alarma, haga clic en **Handle** en su co lumna **Operation**. Después de que se maneje la alarma, se eliminará de la lista. La lista se actualiza y muestra los últimos cinco eventos de intrusión que no se han manejado en las últimas 24 horas.
- Para comprobar más eventos de alarma, haga clic en **View More**.

3 Gestión de activos

3.1 Gestión de activos

Puede contar todos sus activos y comprobar sus estadísticas, incluido el estado del agente, el estado de protección, la cuota, la cuenta, el puerto, el proceso, el software y los elementos iniciados automáticamente.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Seleccione **Asset Management** > **Assets**. Consulta sus activos y sus estadísticas.

----Fin

3.2 Gestión de servidores

3.2.1 Gestión de listas de protección de host

La lista de servidores de la página **Servers & Quota** muestra el estado de protección de sólo los siguientes servidores:

- Servidores de Huawei Cloud comprado en la región seleccionada
- Servidores que no son de Huawei Cloud agregados a la región seleccionada

NOTA

- Cambie a la región correcta antes de buscar sus servidores.
- Si ha habilitado la función de proyecto de empresa, puede seleccionar su proyecto de empresa en la lista desplegable Proyecto **Enterprise** para comprobar la visión general de riesgo del servidor del proyecto.

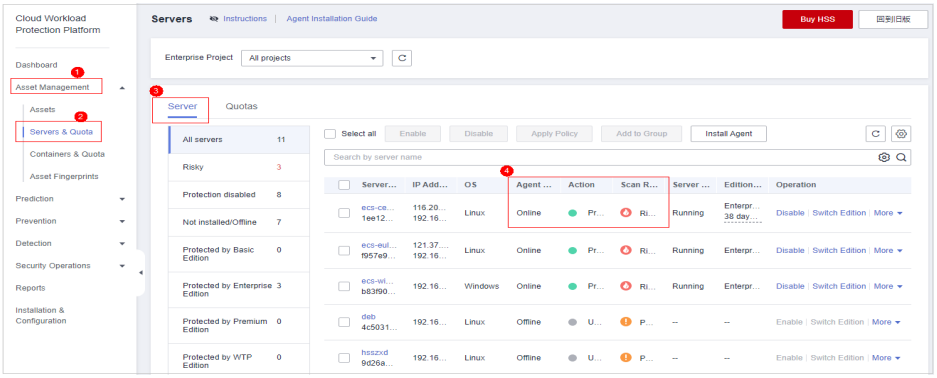
Consulta de la lista de servidores

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Seleccione **Asset Management** > **Servers & Quota**. En la página **Server**, vea el estado de protección de los servidores.

Figura 3-1 Lista de servidores



NOTA

- Puede expandir el área de búsqueda avanzada y buscar un servidor por su nombre, ID, dirección IP, sistema operativo, estado del agente, estado de protección, resultado de detección, grupo de políticas, grupo de servidores, edición o estado del servidor.

Tabla 3-1 Statuses

Parámetro	Descripción
Agent Status	● **Not installed**: El agente no se ha instalado ni se ha iniciado correctamente. Haga clic en **Install Agent** e instale el agente como se le solicite. Para obtener más información, consulte **Instalación de un agente**. ● **Online**: El agente se está ejecutando correctamente. ● **Offline**: La comunicación entre el agente y el servidor HSS es anormal y HSS no puede proteger sus servidores. Puede hacer clic en **Offline** y ver los servidores de Huawei Cloud cuyos agentes están sin conexión y las razones sin conexión en la parte inferior de la página que se muestra.
Action	● **Enabled**: El servidor está completamente protegido por HSS. ● **Disabled**: el servidor no está protegido. Si un servidor no necesita protección, puede deshabilitar HSS para reducir su consumo de recursos.
Scan Results	● **Risky**: El host tiene riesgos. ● **Safe**: No se encuentran riesgos. ● **Pending risk detection**: HSS no está habilitado para el servidor.

----Fin

Consulta de la lista WTP

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Elija **Prevention > Web Tamper Protection** para ver el estado de protección de los servidores.

Tabla 3-2 Statuses

Parámetro	Descripción
Protection Status	**Protected**: HSS proporciona protección estática de manipulación web (WTP) para el servidor.
Dynamic WTP	Estado de WTP dinámico, que puede ser: ● : Habilitación de WTP dinámico ● : Deshabilitación de WTP dinámico (Después de habilitar WTP dinámico, reinicie Tomcat para que esta configuración tenga efecto.)
Static Tampering Attacks	Número de veces que los archivos de páginas web estáticas son atacados y manipulados.
Dynamic Tampering Attacks	Número de vulnerabilidades de aplicaciones web y ataques de inyección.

----Fin

Exportación de la lista de hosts

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Seleccione **Asset Management** > **Servers & Quota**. Se muestra la página de pestaña **Server**.

Paso 4 Haga clic en la esquina superior derecha de la página de pestaña **Server** para exportar los detalles de la lista de servidores.

NOTA

Se puede exportar un máximo de 1000 registros de detalles del servidor a la vez.

----Fin

3.2.2 Habilitación de la protección

3.2.2.1 Edición Básica/Profesional/Premium

Las ediciones básica, empresarial y premium ofrecen diferentes niveles de protección para sus servidores. Puede comprarlos y habilitarlos según sea necesario.

Precauciones

Las ediciones básicas y empresariales se pueden pagar después del uso. Para habilitar otras ediciones, primero compre sus cuotas. Para obtener más información, consulte **Comprar Cuota de HSS** y **Comprar Cuota de CGS**.

Frecuencia de comprobación

HSS realiza una exploración completa en la mañana temprano todos los días.

Después de habilitar la protección del servidor, puede ver los resultados del análisis después del análisis automático a primera hora de la mañana siguiente o realizar un análisis manual inmediatamente.

Prerrequisitos

El agente se ha instalado en los servidores que se van a proteger, el estado del agente es **Online**y el estado de protección es **Unprotected**.

Restricciones

- Linux OS

  En los servidores que ejecutan EulerOS con ARM, HSS no bloquea las direcciones IP sospechosas de ataques de fuerza bruta SSH, sino que solo genera alarmas.
- Windows OS
  - Autorice el firewall de Windows cuando habilite la protección para un servidor Windows. No deshabilite el firewall de Windows durante el período de servicio del HSS. Si el firewall de Windows está deshabilitado, HSS no puede bloquear direcciones IP de ataque de fuerza bruta.
  - Si el firewall de Windows está habilitado manualmente, es posible que HSS también no bloquee las direcciones IP de ataque de fuerza bruta.

Procedimiento

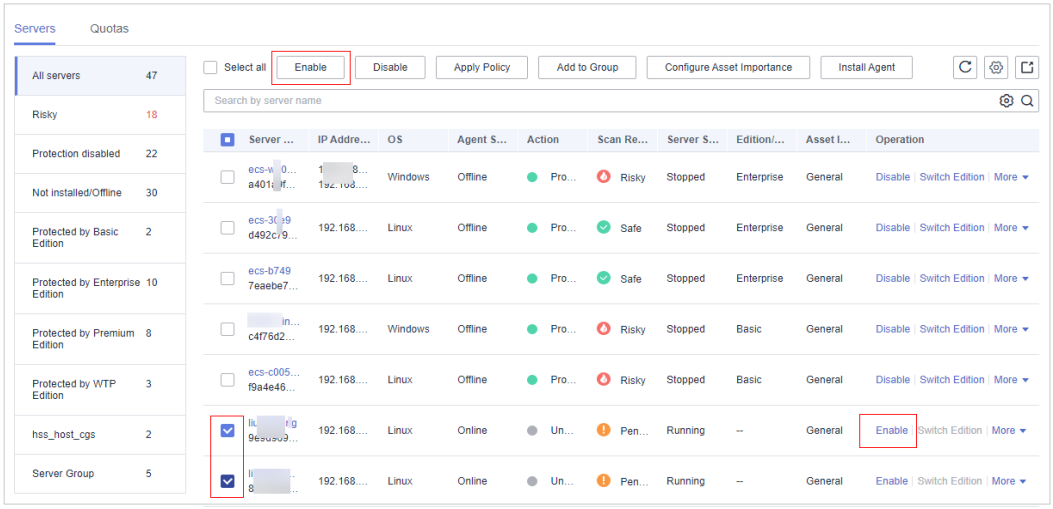
Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Asset Management** > **Servers & Quota**. Haga clic en la pestaña **Server**.

Paso 4 Habilite la protección para uno o varios servidores.

Figura 3-2 Habilitación de la protección



- **Habilitación de la protección de un servidor**

  a. Haga clic en **Enable** en la columna **Operation** de un servidor. En el cuadro de diálogo que se muestra, confirme la información del servidor y seleccione el modo de facturación, la edición y la cuota.

  Figura 3-3 Confirmación de la información de protección de un servidor

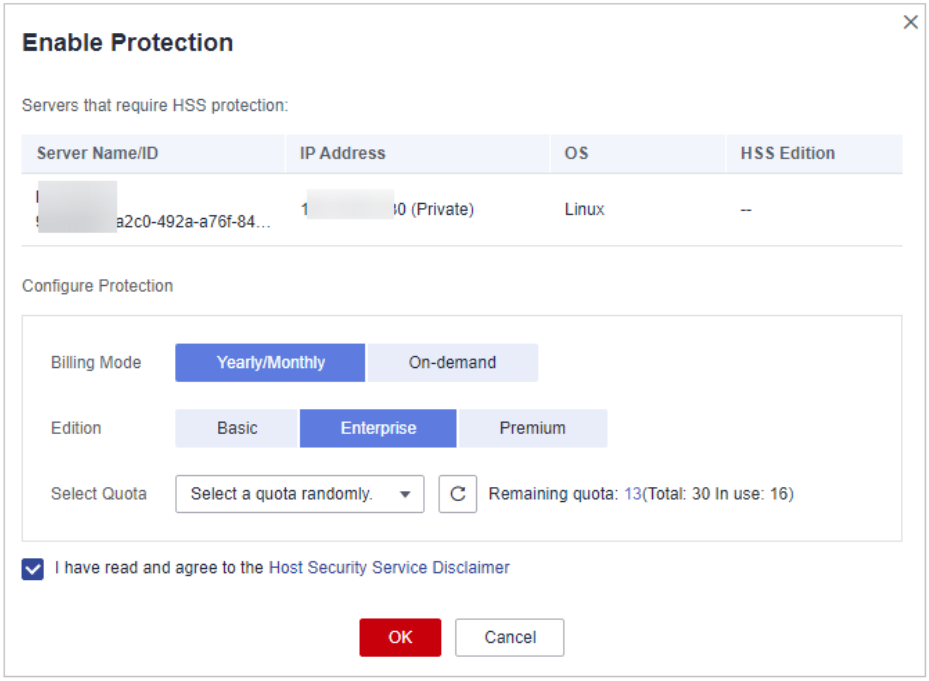


Tabla 3-3 Parámetros de protección

Parámetro	Descripción	Valor de ejemplo
Billing Mode	■ Anual/Mensual ○ Seleccione la edición básica, empresarial o premium. ○ No hay prueba gratuita disponible aquí. Se le facturará por la duración requerida que seleccionó. ○ Un paquete anual/mensual ofrece un descuento más alto que el modo de pago por uso, y se recomienda para usuarios a largo plazo. ■ On-demand ○ Seleccione la edición básica o de empresa. ○ Usted paga por la duración de uso de los recursos. Los precios se calculan por hora y no se requiere una tarifa mínima. ○ La edición básica en modo de pago por uso es gratuita en un plazo de 30 días naturales si se ha habilitado por primera vez. Cada servidor puede disfrutar de una prueba gratuita.	Yearly/ Monthly
Edition	Seleccione la edición básica, empresarial o premium. ■ Edición básica: Protege servidores de prueba o servidores de usuarios individuales. Puede proteger cualquier número de servidores, pero solo una parte de las capacidades de análisis de seguridad están disponibles. Esta edición no proporciona capacidades de protección, ni proporciona soporte para la certificación DJCP Multi-level Protection Scheme (MLPS). La edición básica en modo de pago por uso es gratuita durante 30 días si se ha habilitado por primera vez. ■ Edición Enterprise: Proporciona soporte para la certificación DJCP MLPS L2. Las características principales incluyen la gestión de huellas dactilares de activos, la gestión de vulnerabilidades, la detección de programas maliciosos, la detección de shells web y la detección de comportamientos de procesos anormales. Para obtener más información, consulte **Ediciones y Características**. ■ Edición Premium: Le ayuda con la certificación DJCP MLPS L3 y proporciona características avanzadas, que incluyen protección de aplicaciones, prevención de ransomware, detección de comandos de alto riesgo, detección de escalamiento de privilegios y detección de shell anormal. Para obtener más información, consulte **Ediciones y Características**.	Enterprise

Parámetro	Descripción	Valor de ejemplo
Select Quota	Seleccione una cuota para el servidor. ■ Si no desea especificar una cuota, seleccione **Select a quota randomly**. ■ También puede seleccionar una cuota. Si está habilitando la protección para varios servidores, solo uno de ellos estará vinculado a la cuota seleccionada y el resto de los servidores estará vinculado a cuotas asignadas aleatoriamente. **NOTA** Si el sistema muestra un mensaje que indica que no hay cuotas disponibles, primero debe comprar las cuotas.	Select a quota randomly

b. Confirme la información y haga clic en **OK**. Si el **Protection Status** del servidor es **Protected**, indica que se ha habilitado la protección.

- **Habilitación de la protección en lotes**

a. Seleccione varios servidores y haga clic en **Enable** encima de la lista de servidores. En el cuadro de diálogo que se muestra, confirme la información del servidor y seleccione el modo de facturación, la edición y la cuota.

Figura 3-4 Confirmar información sobre varios servidores

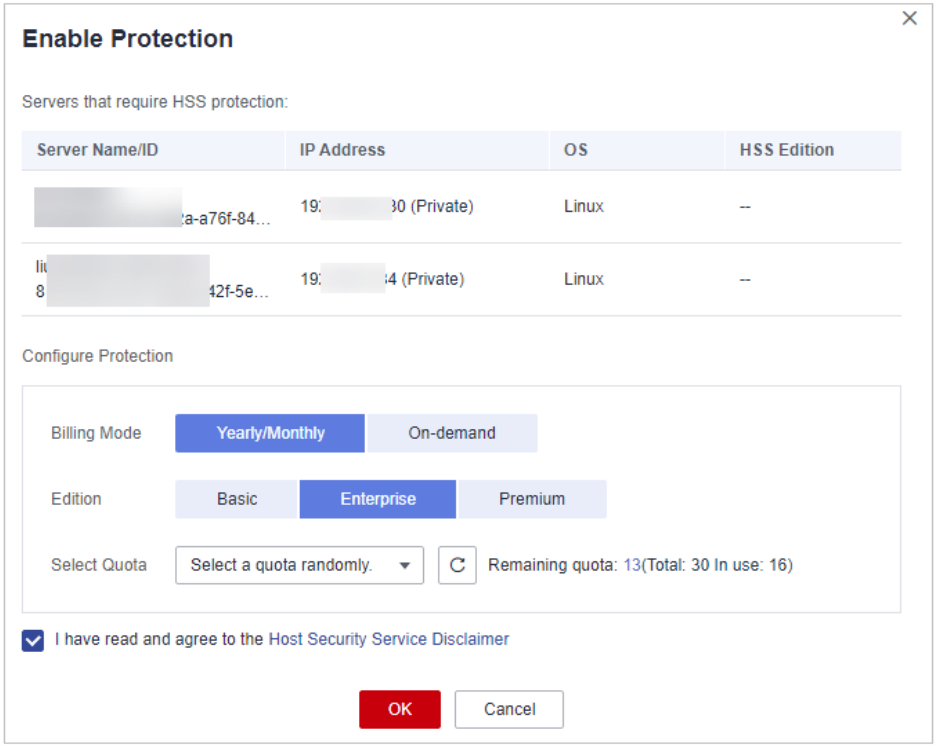


Tabla 3-4 Parámetros de protección

Parámetro	Descripción	Valor de ejemplo
Billing Mode	■ Anual/Mensual ○ Seleccione la edición básica, empresarial o premium. ○ No hay prueba gratuita disponible aquí. Se le facturará por la duración requerida que seleccionó. ○ Un paquete anual/mensual ofrece un descuento más alto que el modo de pago por uso, y se recomienda para usuarios a largo plazo. ■ On-demand ○ Seleccione la edición básica o de empresa. ○ Usted paga por la duración de uso de los recursos. Los precios se calculan por hora y no se requiere una tarifa mínima. ○ La edición básica en modo de pago por uso es gratuita en un plazo de 30 días naturales si se ha habilitado por primera vez. Cada servidor puede disfrutar de una prueba gratuita.	Yearly/ Monthly
Edition	Seleccione la edición básica, empresarial o premium. ■ Edición básica: Protege servidores de prueba o servidores de usuarios individuales. Puede proteger cualquier número de servidores, pero solo una parte de las capacidades de análisis de seguridad están disponibles. Esta edición no proporciona capacidades de protección, ni proporciona soporte para la certificación DJCP Multi-level Protection Scheme (MLPS). La edición básica en modo de pago por uso es gratuita durante 30 días si se ha habilitado por primera vez. ■ Edición Enterprise: Proporciona soporte para la certificación DJCP MLPS L2. Las características principales incluyen la gestión de huellas dactilares de activos, la gestión de vulnerabilidades, la detección de programas maliciosos, la detección de shells web y la detección de comportamientos de procesos anormales. Para obtener más información, consulte **Ediciones y Características**. ■ Edición Premium: Le ayuda con la certificación DJCP MLPS L3 y proporciona características avanzadas, que incluyen protección de aplicaciones, prevención de ransomware, detección de comandos de alto riesgo, detección de escalamiento de privilegios y detección de shell anormal. Para obtener más información, consulte **Ediciones y Características**.	Enterprise

Parámetro	Descripción	Valor de ejemplo
Select Quota	Seleccione una cuota para el servidor. ■ Si no desea especificar una cuota, seleccione **Select a quota randomly**. ■ También puede seleccionar una cuota. Si está habilitando la protección para varios servidores, solo uno de ellos estará vinculado a la cuota seleccionada y el resto de los servidores estará vinculado a cuotas asignadas aleatoriamente. **NOTA** Si el sistema muestra un mensaje que indica que no hay cuotas disponibles, primero debe comprar las cuotas.	Select a quota randomly

b. Confirme la información y haga clic en **OK**. Si el **Protection Status** del servidor es **Protected**, indica que se ha habilitado la protección.

----Fin

3.2.2.2 Edición WTP

La edición WTP proporciona capacidades de protección contra manipulaciones web para sus servidores.

Cómo WTP previene la manipulación de páginas web

Tabla 3-5 Cómo funciona WTP

Tipo	Mecanismo
Static web page protection	1. Bloqueo de directorio local WTP bloquea los archivos en un directorio de archivos web en una unidad para evitar que los atacantes los modifiquen. Los administradores del sitio web pueden actualizar el contenido del sitio web mediante procesos privilegiados. 2. Copia de respaldo y restauración proactivas Si WTP detecta que un archivo en un directorio protegido está manipulado, inmediatamente utiliza el archivo de copia de respaldo en el servidor local para restaurar el archivo. 3. Copia de respaldo y restauración remotas Si un directorio de archivos o un directorio de copia de respaldo del servidor local no es válido, puede utilizar el servicio de copia de respaldo remota para restaurar la página Web manipulada.

Tipo	Mecanismo
Dynamic web page protection	1. Filtrado de comportamiento malicioso basado en RASP La autoprotección de aplicaciones en tiempo de ejecución (RASP) única de Huawei- detecta los comportamientos de los programas de aplicación, evitando que los atacantes alteren las páginas web a través de programas de aplicación. 2. Control de acceso a archivos de disco de red WTP implementa una gestión detallada para controlar los permisos para agregar, modificar y consultar contenido de archivos en discos de red, evitando la manipulación sin afectar la publicación de contenido del sitio web.

Prerrequisitos

- El agente se ha instalado en los servidores que se van a proteger, el estado del agente es **Online**y el estado de protección es **Unprotected**.

Configuración de directorios protegidos

Puede agregar hasta 50 directorios para ser protegidos. Para obtener más información, consulte **Adición de un directorio protegido**.

Para registrar el estado de ejecución del servidor en tiempo real, excluya los archivos de registro del directorio protegido. Puede conceder permisos de lectura y escritura altos para los archivos de registro para evitar que los atacantes vean o manipulen los archivos de registro.

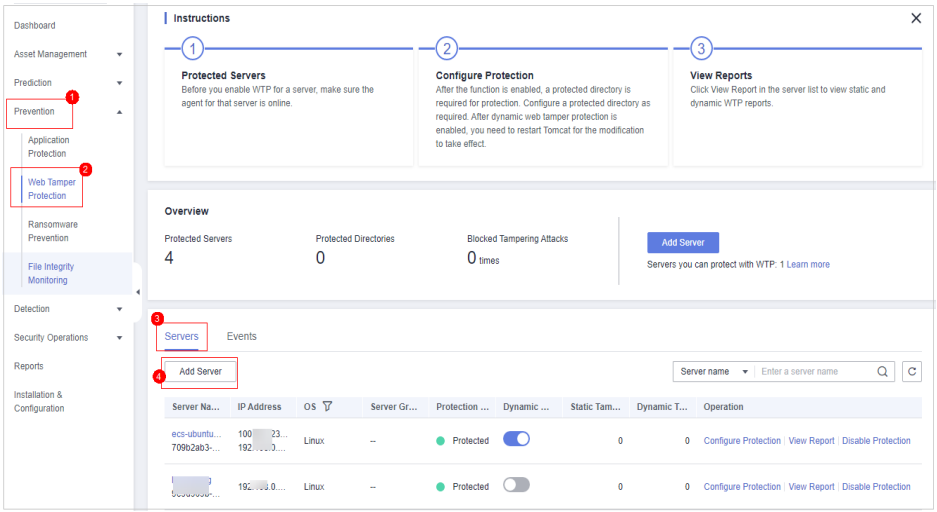
Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, seleccione **Protection** > **Web Tamper Protection**. En la página **Web Tamper Protection**, haga clic en la pestaña **Servers**.

Figura 3-5 Introducir la página para la configuración de directorios protegidos

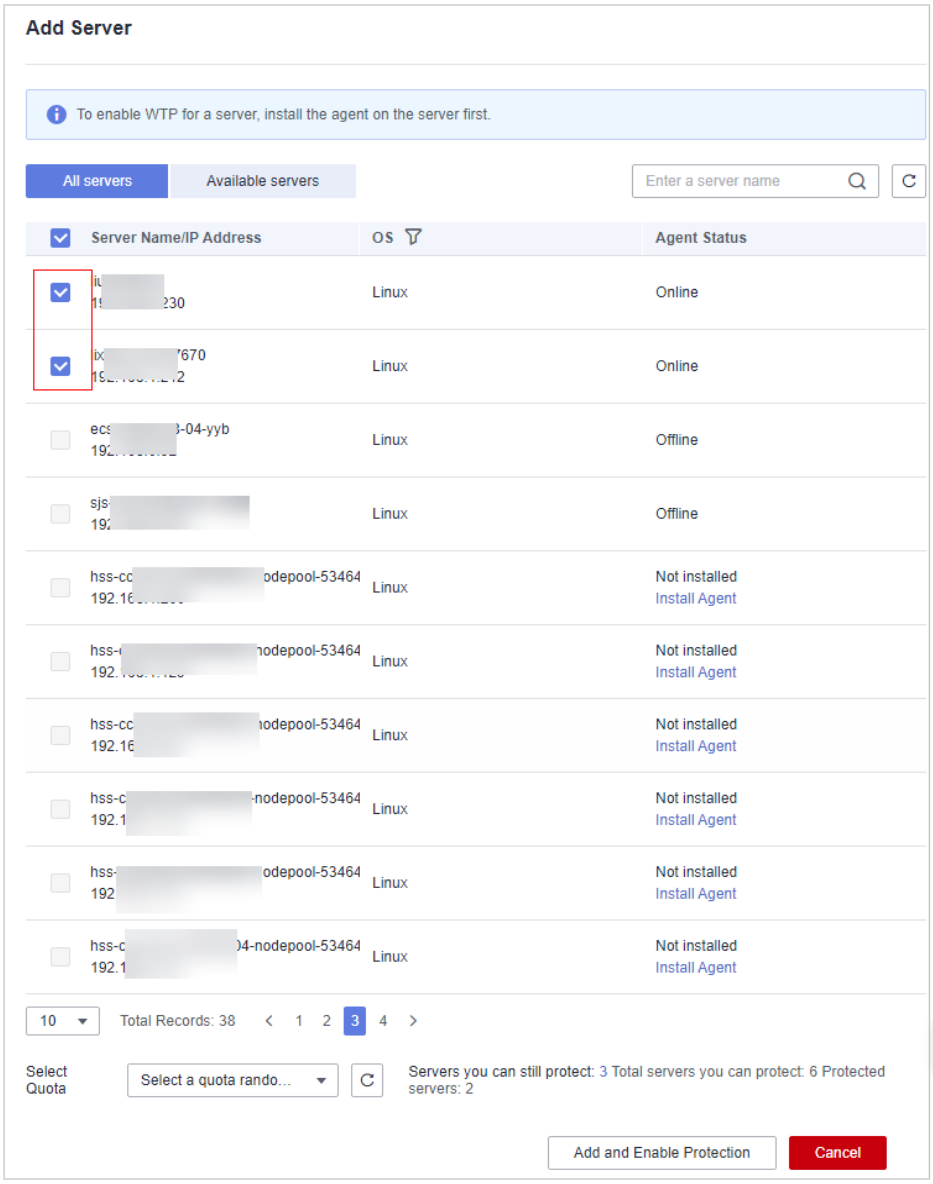


Paso 4 Haga clic en **Add Server**. En el cuadro de diálogo mostrado, seleccione servidores. En la lista desplegable **Select Quota**, seleccione **Select a quota randomly**.

NOTA

Asegúrese de tener suficientes cuotas. Para obtener más información, consulte **Adquisición de cuotas WTP**.

Figura 3-6 Adición de servidores protegidos



Paso 5 Haga clic en **Add and Enable Protection** y compruebe el estado de protección. Seleccione **Protection** > **Web Tamper Protection**. En la página **Web Tamper Protection**, haga clic en la pestaña **Servers**. Si el **Protection Status** del servidor está **Protected**, se ha habilitado WTP.

AVISO

- Después de que WTP esté habilitado, configure los directorios protegidos para que WTP tenga efecto. Para más detalles, consulte **Adición de un directorio protegido**.
- El WTP dinámico solo se puede habilitar para servidores Linux, y solo se puede usar después de reiniciar Tomcat.
- Puede comprobar el estado de protección del servidor en la página **Web Tamper Protection**.

  La edición premium se activará cuando se habilita WTP. Puede realizar las siguientes operaciones para comprobar el estado de protección:

  – Elija **Prevention** > **Web Tamper Protection**. Si el **Protection Status** del servidor está **Protected**, se ha habilitado WTP.

  – Elija **Asset Management** > **Servers & Quota** y haga clic en la pestaña **Servers**. Si el estado de protección del servidor de destino está **Enabled** y la **Edition/Expiration Date** del mismo es **Premium (included with WTP)**, la edición premium proporcionada por la edición WTP se habilita de forma gratuita.

----Fin

3.2.2.3 Edición CGS

La edición CGS protege sus contenedores.

Para habilitar la protección de un nodo contenedor, debe asignar una cuota al nodo. Si la protección está deshabilitada o el nodo se elimina, la cuota se puede asignar a otro nodo.

Frecuencia de comprobación

HSS realiza una exploración completa en la mañana temprano todos los días.

Después de habilitar la protección del servidor, puede ver los resultados del análisis después del análisis automático a primera hora de la mañana siguiente.

Prerrequisitos

- El **Agent Status** de un servidor es **Online**. Para comprobar el estado, elija **Host Security Service** > **Asset Management** > **Containers & Quota**.
- Ha creado un nodo en CCE.
- El **Protection Status** del nodo es **Unprotected**.

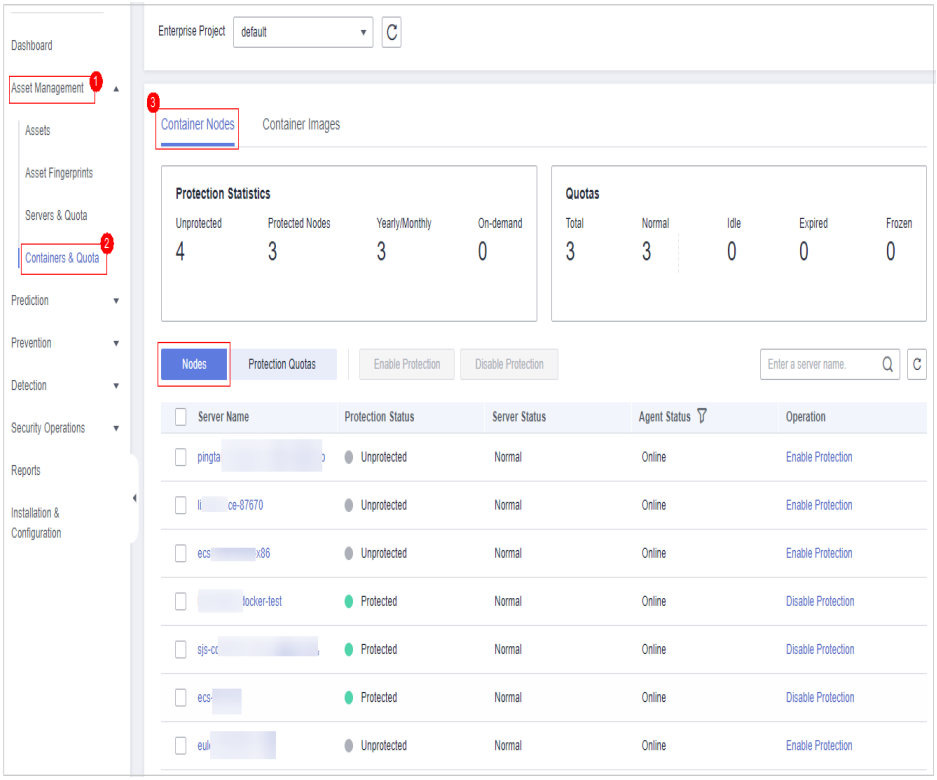
Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Asset Management** > **Containers & Quota**.

Figura 3-7 Acceder a la página de gestión del nodo contenedor

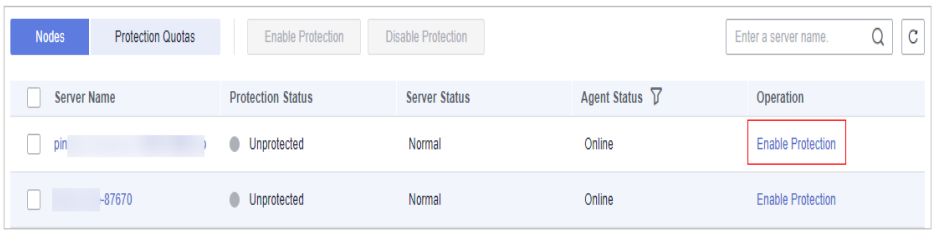


Paso 4 Habilite la protección para uno o varios servidores.

- **Habilitación de la protección de un servidor**

  a. En la columna **Operation** de un servidor, haga clic en **Enable Protection**.

  Figura 3-8 Habilitación de la protección del contenedor

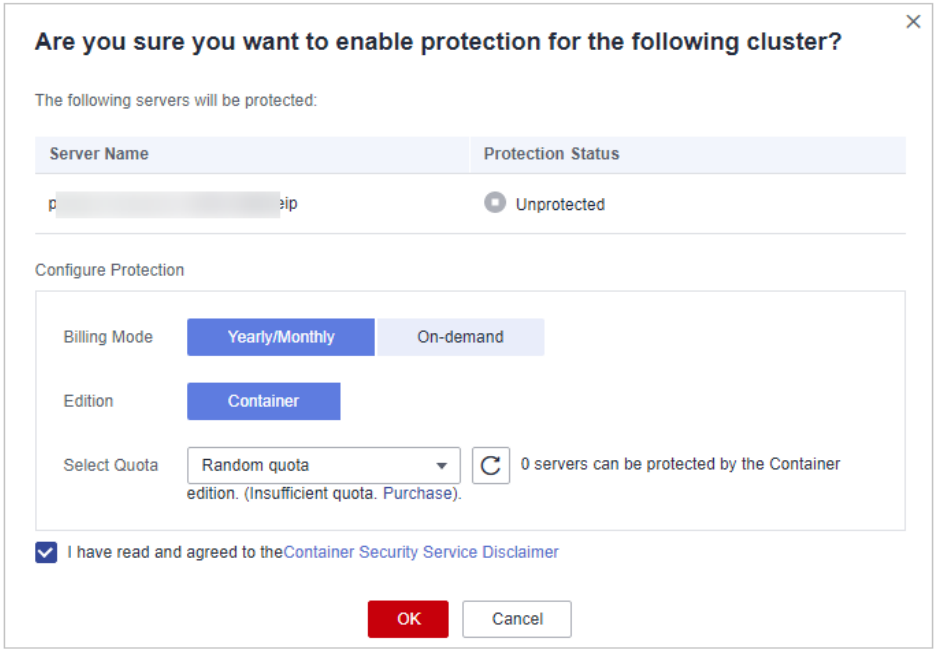
  

  b. En el cuadro de diálogo que se muestra, confirme la información y seleccione un modo de facturación.

  NOTA

  - Para habilitar la protección en el modo de facturación anual/mensual, asegúrese de haber adquirido suficientes cuotas. Para obtener más información, consulte **Compra de una cuota CGS**. También puede habilitar la protección en modo de pago por uso sin utilizar cuotas.
  - Una cuota CGS protege un nodo de clúster.

Figura 3-9 Confirmación de la información de CGS

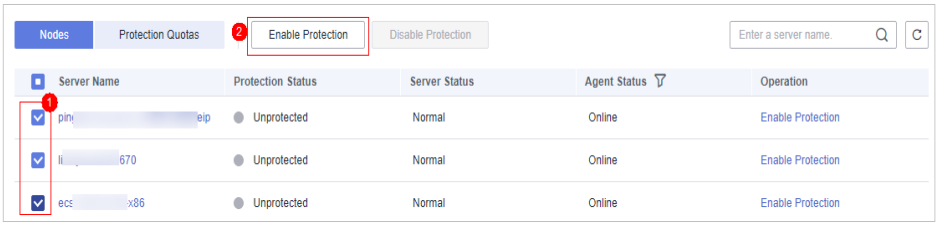


c. Confirme la información, lea el Descargo de responsabilidad del servicio de Container Guard, seleccione **I have read and agreed to the Container Guard Service Disclaimer** y haga clic en **OK**. Si el **Protection Status** de la lista de contenedores cambia a **Protected**, indica que se ha habilitado la protección.

- **Habilitación de la protección en lotes**

  a. En la lista de nodos, seleccione servidores y haga clic en **Enable Protection** encima de la lista.

  Figura 3-10 Selección de servidores

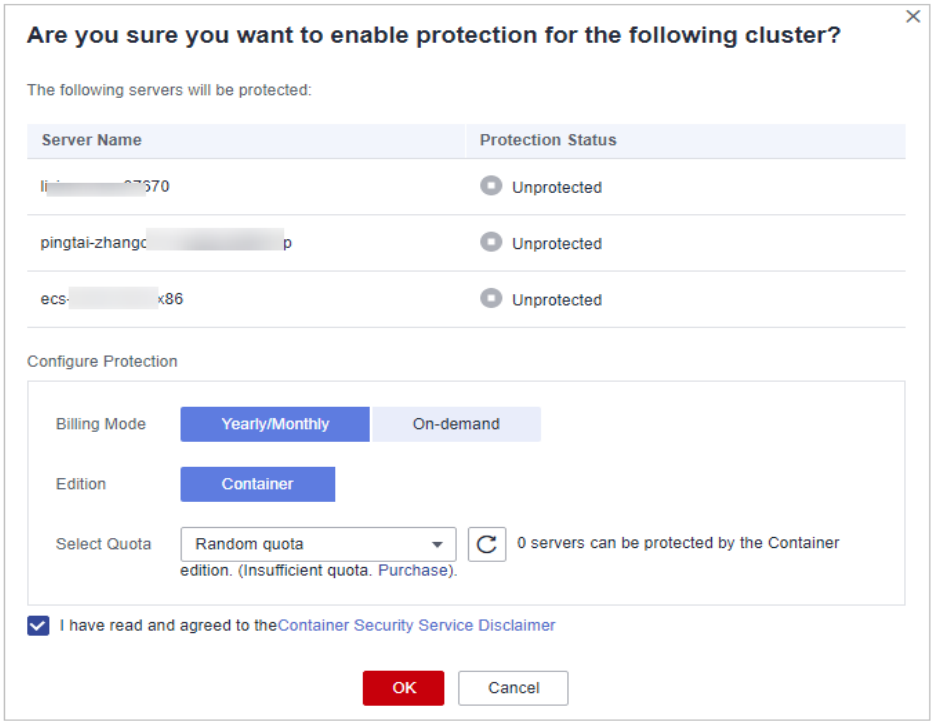


  b. En el cuadro de diálogo que se muestra, confirme la información y seleccione un modo de facturación.

  NOTA

  - Para habilitar la protección en el modo de facturación anual/mensual, asegúrese de haber adquirido suficientes cuotas. Para obtener más información, consulte **Compra de una cuota CGS**. También puede habilitar la protección en modo de pago por uso sin utilizar cuotas.
  - Una cuota CGS protege un nodo de clúster.

Figura 3-11 Confirmación de la información CGS sobre varios servidores



c. Confirme la información, lea el Descargo de responsabilidad del servicio de Container Guard, seleccione **I have read and agreed to the Container Guard Service Disclaimer** y haga clic en **OK**. Si el **Protection Status** de la lista de contenedores cambia a **Protected**, indica que se ha habilitado la protección.

----Fin

3.2.3 Deshabilitación de protección

3.2.3.1 Edición Básica/Profesional/Premium

Puede desactivar la protección para un servidor. Una cuota que no se ha enlazado de un servidor puede estar enlazada a otra.

Precauciones

La deshabilitación de la protección no afecta a los servicios, pero aumentará los riesgos de seguridad. Le aconsejamos que mantenga sus servidores protegidos.

Habilitación de la protección

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

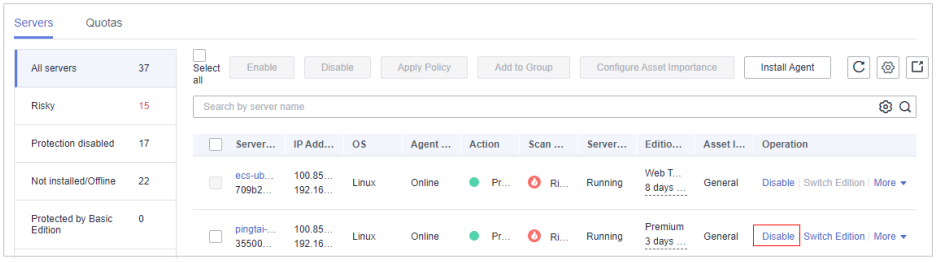
Paso 3 En el panel de navegación, elija **Asset Management** > **Servers & Quota**. Haga clic en la pestaña **Servers**.

Paso 4 Deshabilitar la protección para uno o varios servidores.

- **Deshabilitación de la protección de un servidor**

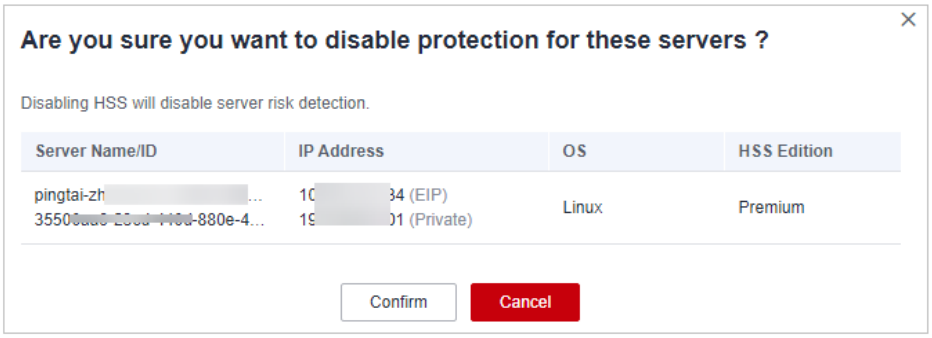
  a. Haga clic en **Disable** en la columna **Operation** de un servidor.

  Figura 3-12 Deshabilitación de la protección de un servidor



  b. En el cuadro de diálogo que se muestra, confirme la información y haga clic en **OK**.

  Figura 3-13 Confirmar la información sobre un servidor



  c. Compruebe el estado de protección en la lista de servidores. Si está **Unprotected**, se ha deshabilitado la protección.

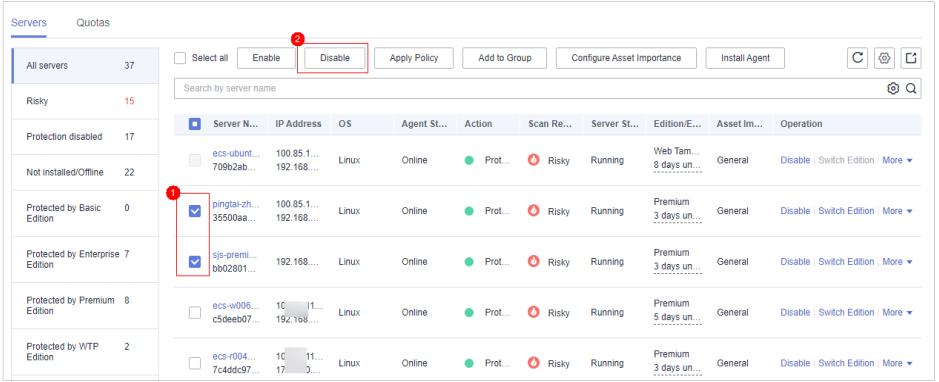
ATENCIÓN

La deshabilitación de la protección no afecta a los servicios, pero aumentará los riesgos de seguridad. Le aconsejamos que mantenga sus servidores protegidos.

- **Habilitación de la protección en lotes**

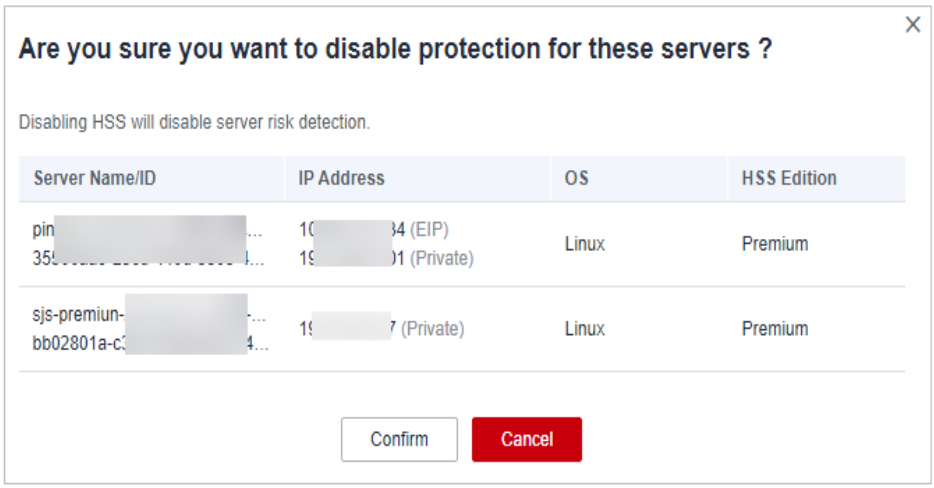
  a. Seleccione varios servidores y haga clic en **Disable** encima de la lista de servidores.

  Figura 3-14 Deshabilitación de la protección en lotes



b. En el cuadro de diálogo que se muestra, confirme la información y haga clic en **OK**.

Figura 3-15 Confirmar información sobre varios servidores



c. Compruebe el estado de protección en la lista de servidores. Si está **Unprotected**, se ha deshabilitado la protección.

ATENCIÓN

La deshabilitación de la protección no afecta a los servicios, pero aumentará los riesgos de seguridad. Le aconsejamos que mantenga sus servidores protegidos.

----Fin

3.2.3.2 Edición WTP

Puede desactivar la edición WTP para un servidor. Una cuota que no se ha enlazado de un servidor puede estar enlazada a otra.

Precauciones

La deshabilitación de la protección no afecta a los servicios, pero aumentará los riesgos de seguridad. Le aconsejamos que mantenga sus servidores protegidos.

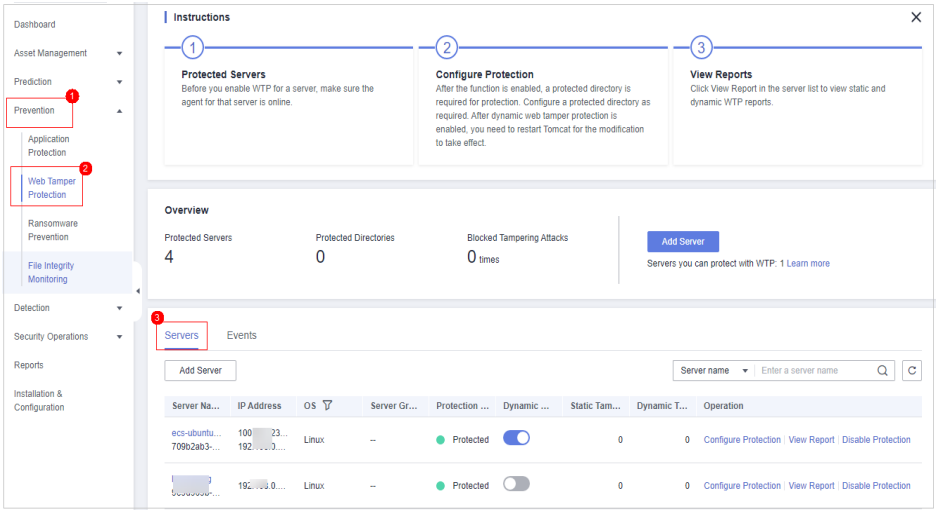
Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, seleccione **Protection** > **Web Tamper Protection**. En la página **Web Tamper Protection**, haga clic en la pestaña **Servers**.

Figura 3-16 Introducir la página para la configuración de directorios protegidos

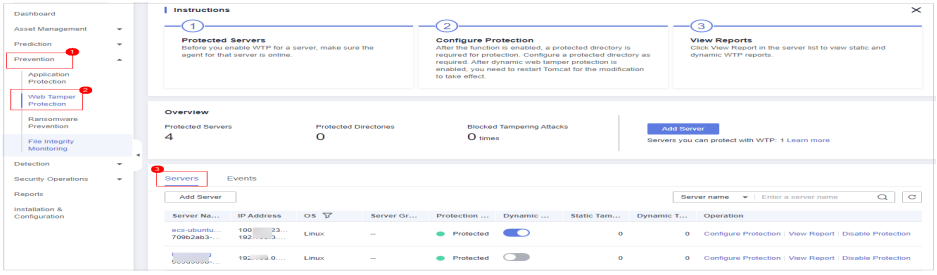


Paso 4 Haga clic en **Disable** en la columna **Operation**.

NOTA

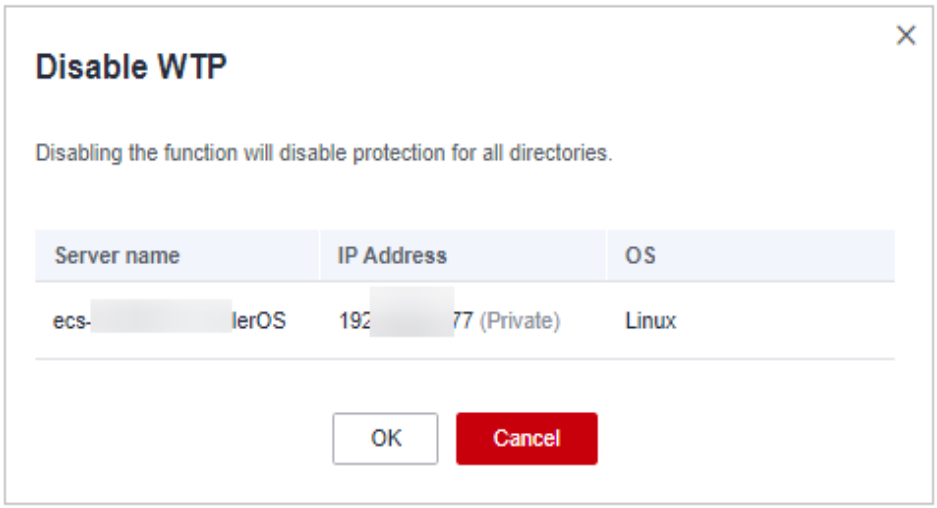
La edición WTP no se puede deshabilitar para servidores en lotes.

Figura 3-17 Deshabilitación de WTP



Paso 5 En el cuadro de diálogo que se muestra, confirme la información y haga clic en **OK**.

Figura 3-18 Confirmación de información sobre la desactivación de WTP



Paso 6 Elija **Asset Management** > **Servers & Quota** y haga clic en la pestaña **Servers**. Compruebe el estado de protección en la lista de servidores. Si está **Unprotected**, se ha deshabilitado la protección.

> ⚠ ATENCIÓN
>
> La deshabilitación de la protección no afecta a los servicios, pero aumentará los riesgos de seguridad. Le aconsejamos que mantenga sus servidores protegidos.

----Fin

3.2.3.3 Edición CGS

Puede desactivar la edición CGS para un servidor. Una cuota que no se ha enlazado de un servidor puede estar enlazada a otra.

Antes de empezar

La deshabilitación de la protección no afecta a los servicios, pero aumentará los riesgos de seguridad. Le aconsejamos que mantenga sus servidores protegidos.

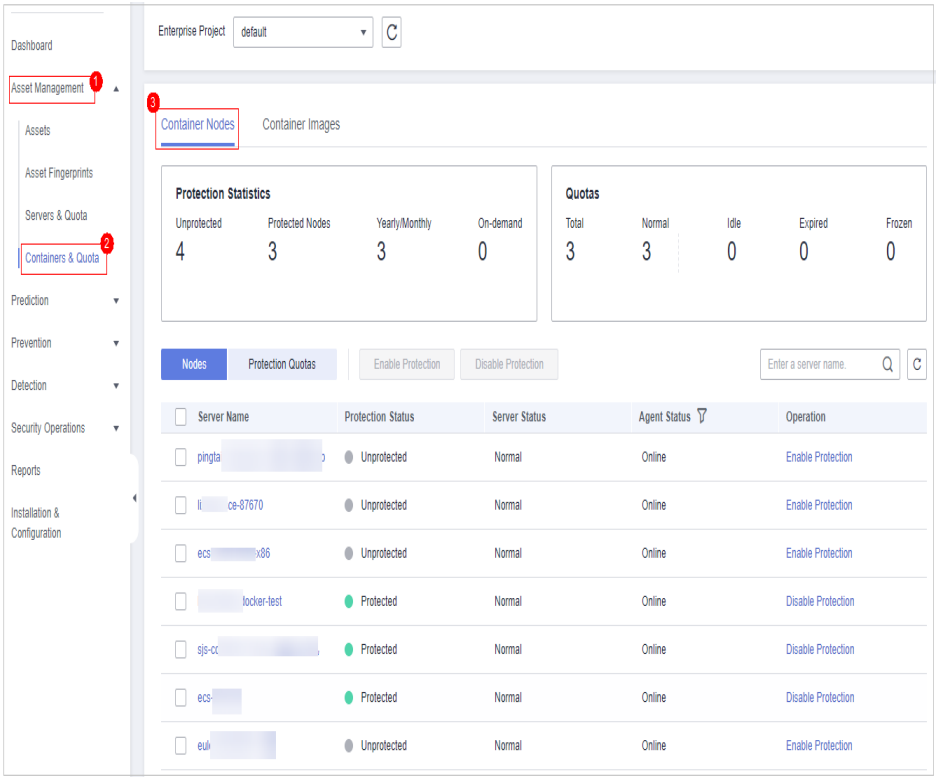
Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Asset Management** > **Containers & Quota**.

Figura 3-19 Acceder a la página de gestión del nodo contenedor

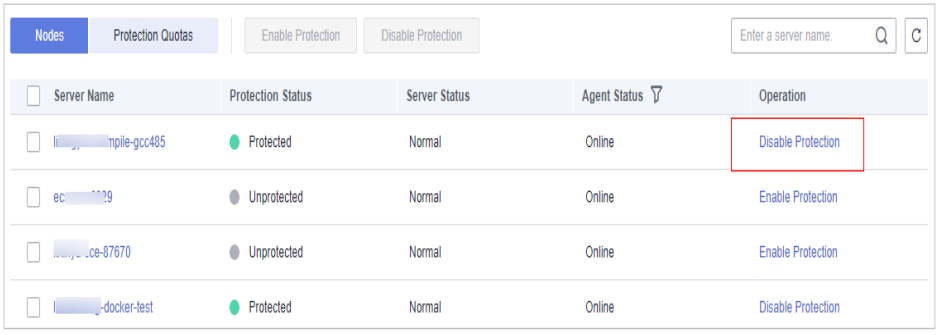


Paso 4 Deshabilitar la protección para uno o varios servidores.

- **Deshabilitación de la protección de un servidor**

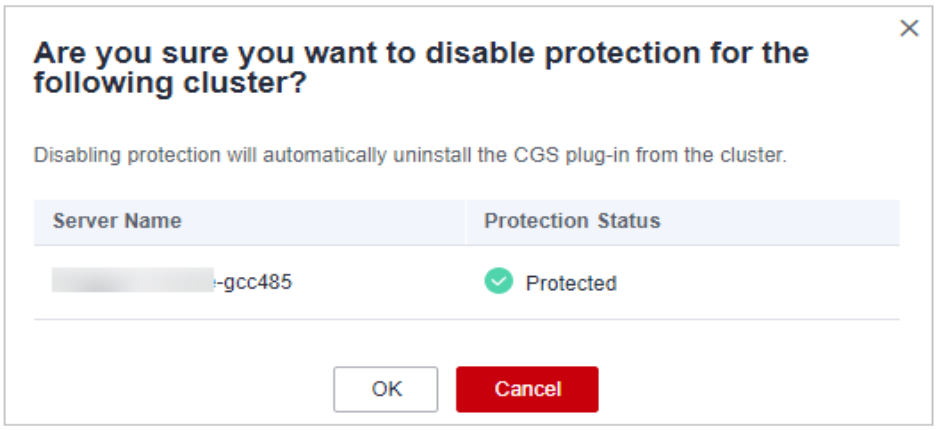
  a. En la lista de nodos, haga clic en **Disable Protection** en la columna **Operation** de un servidor.

  Figura 3-20 Deshabilitar la protección del contenedor



  b. En el cuadro de diálogo que se muestra, confirme la información y haga clic en **OK**.

Figura 3-21 Confirmación de información sobre la desactivación de CGS



c. Elija **Asset Management** > **Containers & Quota** y haga clic en la pestaña **Container Nodes**. Compruebe el estado de protección en la lista de servidores. Si está **Unprotected**, se ha deshabilitado la protección.

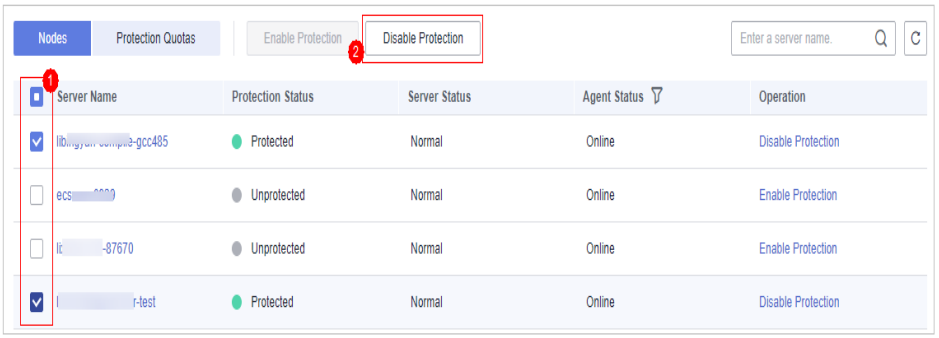
ATENCIÓN

La deshabilitación de la protección no afecta a los servicios, pero aumentará los riesgos de seguridad. Le aconsejamos que mantenga sus servidores protegidos.

- **Deshabilitación de la protección en lotes**

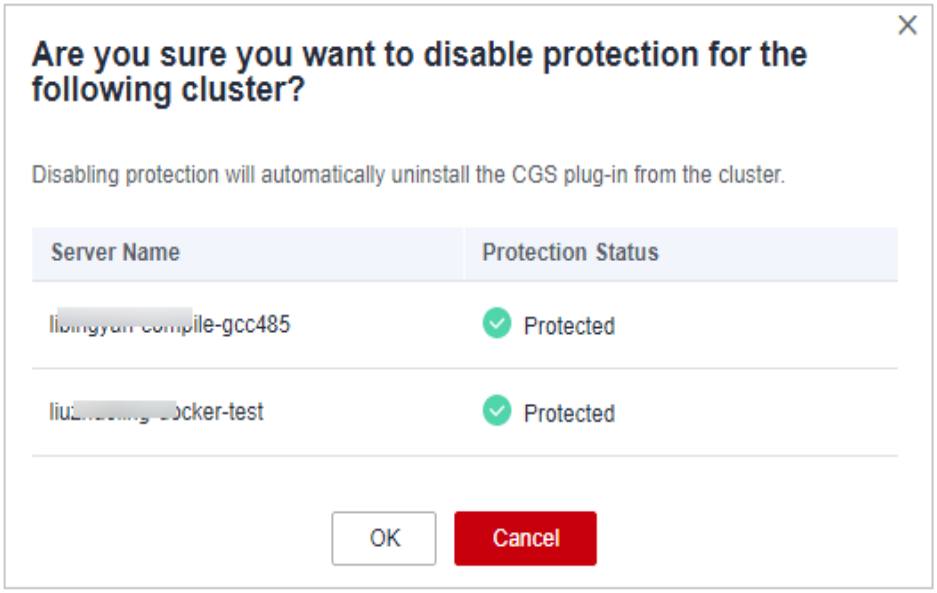
a. En la lista de nodos, seleccione servidores y haga clic en **Disable Protection** encima de la lista.

Figura 3-22 Selección de servidores



b. En el cuadro de diálogo que se muestra, confirme la información y haga clic en **OK**.

Figura 3-23 Confirmación de información sobre la desactivación de CGS en lotes



c. Elija **Asset Management** > **Containers & Quota** y haga clic en la pestaña **Container Nodes**. Compruebe el estado de protección en la lista de servidores. Si está **Unprotected**, se ha deshabilitado la protección.

> ⚠ ATENCIÓN
>
> La deshabilitación de la protección no afecta a los servicios, pero aumentará los riesgos de seguridad. Le aconsejamos que mantenga sus servidores protegidos.

d. Confirme la información, lea el Descargo de responsabilidad del servicio de Container Guard, seleccione **I have read and agreed to the Container Guard Service Disclaimer** y haga clic en **OK**. Si el **Protection Status** de la lista de contenedores cambia a **Protected**, indica que se ha habilitado la protección.

----Fin

3.2.4 Aplicación de una política

Puede configurar e iniciar rápidamente análisis de servidores mediante grupos de políticas. Simplemente cree un grupo, agregue directivas y aplique este grupo a los servidores. Los agentes implementados en sus servidores analizarán todo lo especificado en las directivas.

Precauciones

- Cuando habilita la edición empresarial, el grupo de políticas de esta edición (incluidas las políticas de detección de shell de sitios web y contraseñas débiles) entra en vigor para todos los servidores de forma predeterminada.
- Al habilitar la edición premium que compró por separado o que se incluyó con la edición WTP, el grupo de políticas de esta edición entra en vigor por defecto.

  Para crear su propio grupo de políticas, puede copiar el grupo de políticas de la edición premium y agregar o quitar políticas en la copia.

Creación de un grupo de política

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el árbol de navegación de la izquierda, elija **Security Operations** > **Policies**

Paso 4 Copiar un grupo de políticas.

- Seleccione el grupo de políticas **tenant_linux_premium_default_policy_group**. Busque la fila en la que reside este grupo de políticas, haga clic en **Copy** en la columna **Operation**, como se muestra en **Figura 3-24**.

  Figura 3-24 Copia de un grupo de políticas de Linux

- Seleccione el grupo de políticas **tenant_windows_premium_default_policy_group**. Busque la fila en la que reside este grupo de políticas, haga clic en **Copy** en la columna **Operation**, como se muestra en **Figura 3-25**.

  Figura 3-25 Copia de un grupo de políticas de Windows

Paso 5 En el cuadro de diálogo que se muestra, escriba el nombre y la descripción de un grupo de políticas y haga clic en **OK**.

NOTA

- El nombre de un grupo de políticas debe ser único o no se creará el grupo.
- El nombre del grupo de políticas y su descripción pueden contener sólo letras, dígitos, guiones bajos (_), guiones (-) y espacios, y no pueden comenzar o terminar con un espacio.

Paso 6 Haga clic en **OK**.

Paso 7 Haga clic en el nombre del grupo de políticas que acaba de crear. Se mostrarán las políticas del grupo.

Paso 8 Haga clic en un nombre de política y modifique su configuración según sea necesario. Para más detalles, consulte **Modificación de una política**.

Paso 9 Habilite o deshabilite la política haciendo clic en el botón correspondiente en la columna **Operation**. Puede hacer clic para actualizar la página.

----Fin

Aplicación de un grupo de política

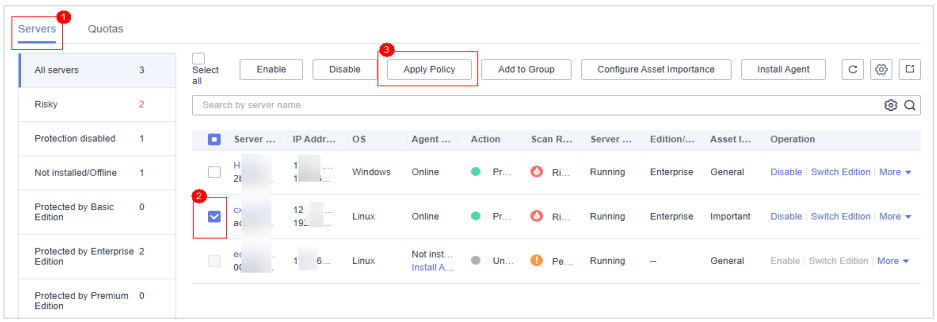
Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Asset Management** > **Servers & Quota** y haga clic en **Server**.

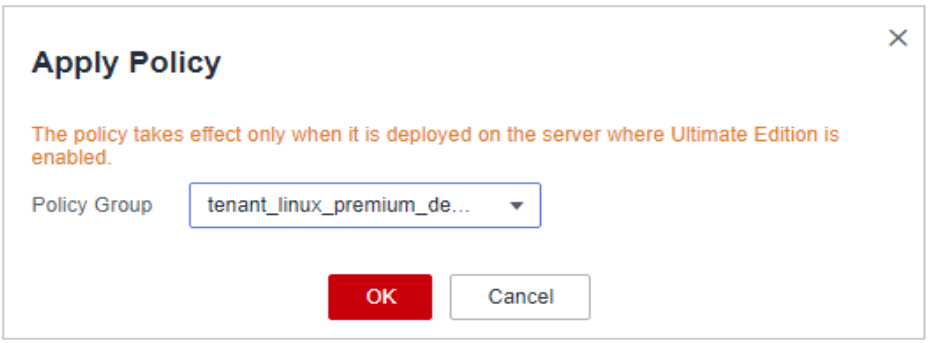
Paso 4 Seleccione uno o más servidores y haga clic en **Apply Policy**, como se muestra en **Figura 3-26**.

Figura 3-26 Aplicación de una política



Paso 5 En el cuadro de diálogo que aparece, seleccione un grupo de políticas y haga clic en **OK**.

Figura 3-27 Selección de un grupo de políticas



NOTA

- Las políticas antiguas aplicadas a un servidor no serán válidas si se aplican nuevas directivas al servidor.
- Las políticas se aplican a los servidores en un minuto.
- Laspmàñs aplicadas a los servidores sin conexión no surtirán efecto hasta que los servidores estén en línea.
- En un grupo de políticas implementado, puede habilitar, deshabilitar o modificar políticas.
- No se puede eliminar un grupo de políticas implementado.

----Fin

3.2.5 Gestión de grupos de servidores

Para gestionar servidores por grupo, puede crear un grupo de servidores y agregarle servidores.

Puede comprobar el número de servidores, servidores inseguros y servidores desprotegidos en un grupo.

Creación de un grupo de servidores

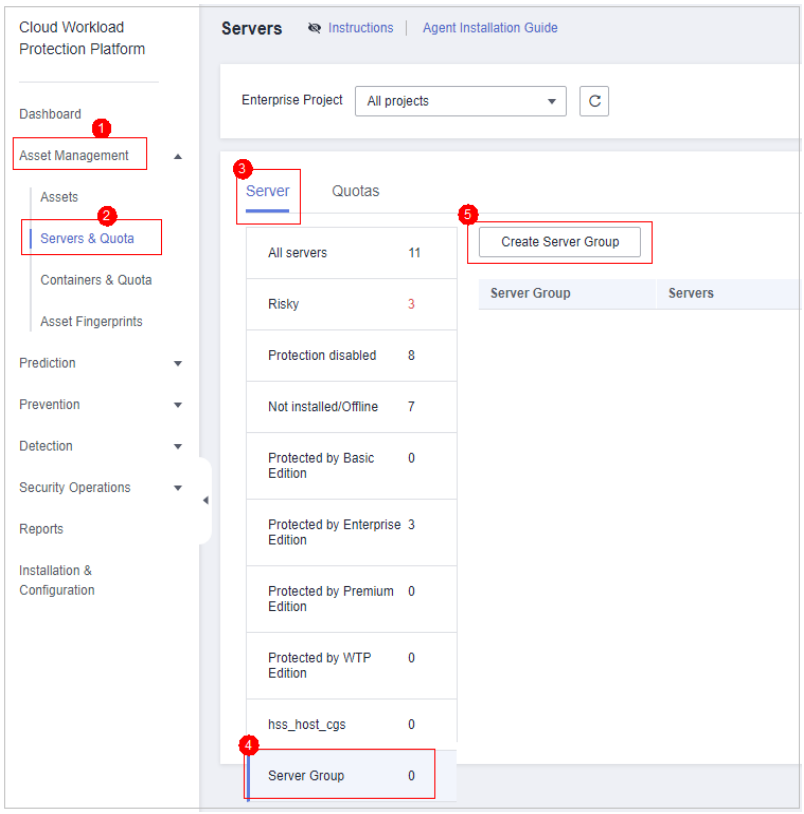
Después de crear un grupo de servidores, puede asignar servidores al grupo para la gestión unificada.

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, elija **Asset Management** > **Servers & Quota**, haga clic en **Server Group** en la lista **Server** y haga clic en **Create Server Group**, como se muestra en **Figura 3-28**.

Figura 3-28 Acceso a la página de grupos de servidores

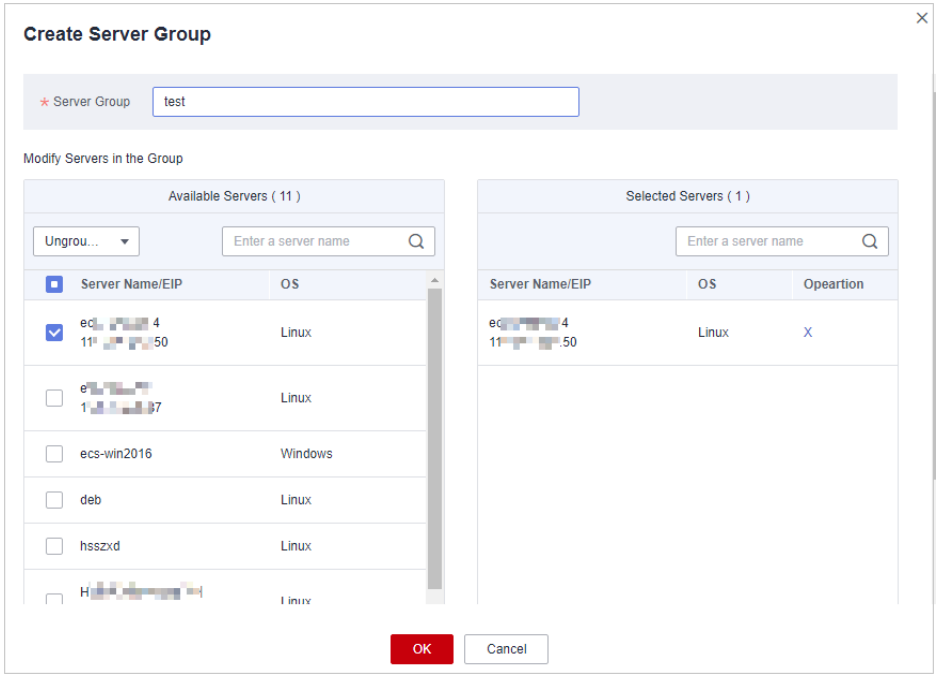


Paso 4 En el cuadro de diálogo **Create Server Group**, escriba un nombre de grupo de servidores y seleccione los servidores que se agregarán al grupo, como se muestra en **Figura 3-29**.

NOTA

- Un nombre de grupo de servidor debe ser único o no se creará el grupo.
- Un nombre no puede contener espacios. Contiene solo letras, dígitos, guiones bajos (_), guiones (-), puntos (.), asteriscos (*), y signos más (+). La longitud no puede exceder los 64 caracteres.

Figura 3-29 Creación de un grupo de servidores



Paso 5 Haga clic en **OK**.

----Fin

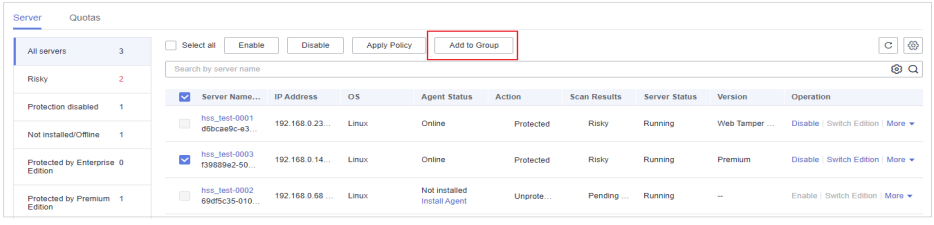
Adición de servidores a grupos

Puede agregar servidores a un grupo de servidores existente.

Paso 1 Haga clic en la pestaña **Server**.

Paso 2 Seleccione uno o más servidores y haga clic en **Add to Group**, como se muestra en **Figura 3-30**.

Figura 3-30 Adición de servidores a un grupo



NOTA

Para agregar un servidor a un grupo, también puede localizar la fila donde reside el servidor, haga clic en **More** en la columna **Operation** y elija **Add to Group**.

Paso 3 En el cuadro de diálogo mostrado, seleccione un grupo de servidores y haga clic en **OK**.

NOTA

Un servidor solo se puede agregar a un grupo de servidores.

----Fin

Procedimiento posterior

Edición de un grupo de servidores

Paso 1 Haga clic en **Servers & Quota** y haga clic en **Server Group** en la lista **Server**.

Paso 2 Busque la fila donde reside un grupo de servidores y haga clic en **Edit** en la columna **Operation**.

Paso 3 En el cuadro de diálogo que se muestra, agregue o elimine servidores del grupo.

Paso 4 Haga clic en **OK**.

----Fin

Eliminación de un grupo de servidores

Paso 1 Haga clic en **Servers & Quota** y haga clic en **Server Group** en la lista **Server**.

Paso 2 Busque la fila donde reside un grupo de servidores y haga clic en **Delete** en la columna **Operation**.

NOTA

Después de eliminar el grupo de servidores, la columna **Server Group** de los servidores que estaban en el grupo estará en blanco.

----Fin

3.2.6 Configuración de Importancia de Activos

Puede configurar la importancia de activos de un servidor y gestionar servidores por nivel de importancia de activos.

La importancia del activo de un servidor puede modificarse.

Prerrequisitos

El agente se ha instalado en los servidores.

Comprobación de Importancia de Activos

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Asset Management** > **Servers & Quota**. Haga clic en la pestaña **Server**.

Paso 4 En la parte inferior de la página de pestañas, compruebe la importancia del activo. Puede hacer clic en **Important**, **General**, o **Test** para ver los servidores por nivel de importancia.

- La importancia de los activos puede ser:
  - **Important**. Especifique este nivel para los servidores que ejecutan servicios importantes o almacenan datos importantes.
  - **General**. Especifique este nivel para los servidores que ejecutan servicios generales o almacenan datos generales.
  - **Test**. Especifique este nivel para los servidores que ejecutan servicios de prueba o almacenan datos de prueba.

----Fin

Especificación de Importancia de Activos

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Asset Management** > **Servers & Quota**. Haga clic en la pestaña **Server**.

Paso 4 Configurar la importancia de los activos.

AVISO

Si el estado del agente de un servidor es **Not installed**, no puede especificar la importancia del activo para el servidor.

- Configuración de un servidor
  - Método 1: Seleccione un servidor y configure su importancia de activo.
    i. Seleccione un servidor y haga clic en **Configure Asset Importance**.
    ii. En el cuadro de diálogo que se muestra, seleccione un nivel de importancia de activo.

    NOTA

    La importancia de los activos puede ser:
    - **Important**. Especifique este nivel para los servidores que ejecutan servicios importantes o almacenan datos importantes.
    - **General**. Especifique este nivel para los servidores que ejecutan servicios generales o almacenan datos generales.
    - **Test**. Especifique este nivel para los servidores que ejecutan servicios de prueba o almacenan datos de prueba.

    iii. Confirme la información y haga clic en **OK**.
  - Método 2: Haga clic en el botón de configuración en la columna **Operation**.
    i. En la columna **Operation** de un servidor, elija **More** > **Configure Asset Importance**.
    ii. En el cuadro de diálogo que se muestra, seleccione un nivel de importancia de activo.

NOTA

La importancia de los activos puede ser:

- **Important**. Especifique este nivel para los servidores que ejecutan servicios importantes o almacenan datos importantes.
- **General**. Especifique este nivel para los servidores que ejecutan servicios generales o almacenan datos generales.
- **Test**. Especifique este nivel para los servidores que ejecutan servicios de prueba o almacenan datos de prueba.

iii. Confirme la información y haga clic en **OK**.

- Configuración de servidores en lotes
  a. Seleccione varios servidores y haga clic en **Configure Asset Importance**.
  b. En el cuadro de diálogo que se muestra, seleccione un nivel de importancia de activo.

NOTA

Todos los servidores seleccionados tendrán la importancia del activo seleccionado.

La importancia de los activos puede ser:

- **Important**. Especifique este nivel para los servidores que ejecutan servicios importantes o almacenan datos importantes.
- **General**. Especifique este nivel para los servidores que ejecutan servicios generales o almacenan datos generales.
- **Test**. Especifique este nivel para los servidores que ejecutan servicios de prueba o almacenan datos de prueba.

  c. Confirme la información y haga clic en **OK**.

----Fin

Modificación de la importancia de los activos

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Asset Management** > **Servers & Quota**. Haga clic en la pestaña **Server**.

Paso 4 Modifique la importancia del activo.

- Modificación de un servidor
  – Método 1: Seleccione un servidor y modifique su importancia de activo.
    i. Seleccione un servidor y haga clic en **Configure Asset Importance**.
    ii. En el cuadro de diálogo que se muestra, seleccione un nivel de importancia de activo.

NOTA

La importancia de los activos puede ser:

- **Important**. Especifique este nivel para los servidores que ejecutan servicios importantes o almacenan datos importantes.
- **General**. Especifique este nivel para los servidores que ejecutan servicios generales o almacenan datos generales.
- **Test**. Especifique este nivel para los servidores que ejecutan servicios de prueba o almacenan datos de prueba.

iii. Confirme la información y haga clic en **OK**.

– Método 2: Haga clic en el botón de configuración en la columna **Operation**.

i. En la columna **Operation** de un servidor, elija **More** > **Configure Asset Importance**.

ii. En el cuadro de diálogo que se muestra, seleccione un nivel de importancia de activo.

NOTA

La importancia de los activos puede ser:

- **Important**. Especifique este nivel para los servidores que ejecutan servicios importantes o almacenan datos importantes.
- **General**. Especifique este nivel para los servidores que ejecutan servicios generales o almacenan datos generales.
- **Test**. Especifique este nivel para los servidores que ejecutan servicios de prueba o almacenan datos de prueba.

iii. Confirme la información y haga clic en **OK**.

- Configuración de servidores en lotes

a. Seleccione varios servidores y haga clic en **Configure Asset Importance**.

b. En el cuadro de diálogo que se muestra, seleccione un nivel de importancia de activo.

NOTA

Todos los servidores seleccionados tendrán la importancia del activo seleccionado.

La importancia de los activos puede ser:

- **Important**. Especifique este nivel para los servidores que ejecutan servicios importantes o almacenan datos importantes.
- **General**. Especifique este nivel para los servidores que ejecutan servicios generales o almacenan datos generales.
- **Test**. Especifique este nivel para los servidores que ejecutan servicios de prueba o almacenan datos de prueba.

c. Confirme la información y haga clic en **OK**.

----Fin

3.2.7 Agentes de instalación por lotes

Después de crear una tarea de instalación del agente por lotes, el sistema instalará los agentes automáticamente. Puede habilitar la protección para los servidores de destino una vez que los agentes se hayan instalado correctamente.

Prerrequisitos

- Ha comprado al menos un servidor y no ha instalado el agente en él.
- Todos los servidores de destino deben admitir el inicio de sesión SSH.
- Se han obtenido las cuentas de inicio de sesión, los números de puerto y las contraseñas correctas de todos los servidores.
- Todos los servidores de destino deben estar en estado **Running**.

Restricciones

- Actualmente, solo los servidores Linux pueden instalar agentes en lotes.
- En la VPC donde se ubican los servidores de destino, al menos un servidor ha instalado el agente.
- Los agentes se pueden instalar en hasta 50 servidores a la vez.

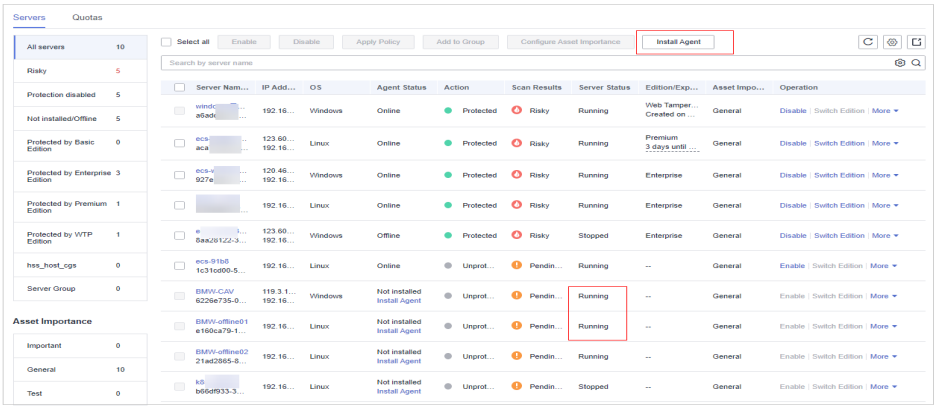
Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Asset Management** > **Servers & Quota**. Haga clic en la pestaña **Servers**.

Figura 3-31 Lista de servidores

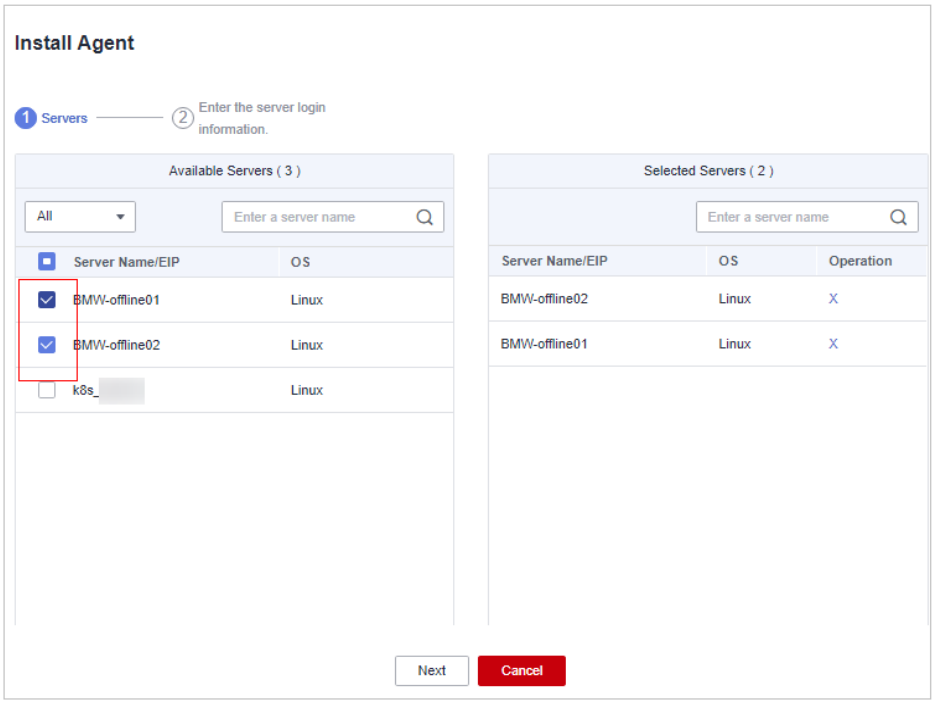


Paso 4 Haga clic en **Install Agent** en la parte superior de la página y seleccione servidores de destino en la página de diálogo mostrada.

AVISO

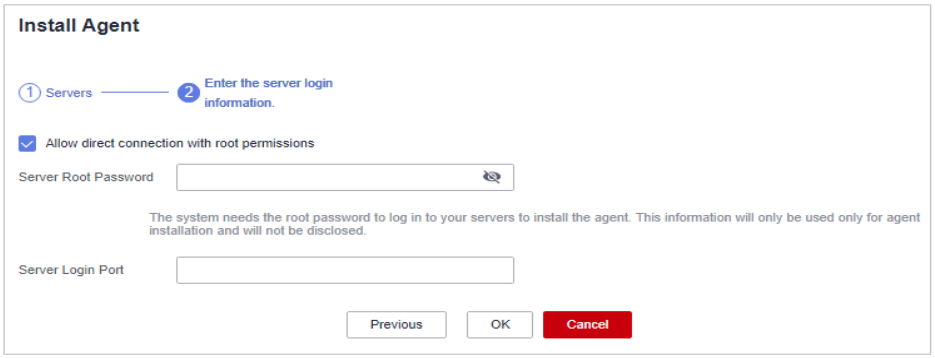
- Todos los servidores de destino deben estar en estado **Running**.
- En la VPC donde se ubican los servidores de destino, al menos un servidor ha instalado el agente. De lo contrario, la instalación por lotes fallará.
- Los servidores seleccionados deben usar la misma contraseña de root y el mismo número de puerto. De lo contrario, la instalación por lotes fallará.
- Los agentes se pueden instalar en hasta 50 servidores a la vez.

Figura 3-32 Selección de servidores



Paso 5 Haga clic en **Next**. Introduzca la contraseña de root del servidor y el puerto de inicio de sesión del servidor.

Figura 3-33 Introducir información del servidor



Paso 6 Haga clic en **OK**. Los agentes se instalarán automáticamente en los servidores que haya seleccionado.

NOTA

Los agentes se instalarán automáticamente en los servidores que seleccionó en secuencia. Puede elegir **Asset Management** > **Servers & Quota** > **Servers** para ver el estado del agente. Si el **Agent Status** de un servidor de destino cambia a **Online**, puede habilitar la protección para el servidor.

----Fin

3.3 Gestión de contenedores

3.3.1 Consulta de los clústeres y las cuotas de protección

La página **Container Nodes** muestra el estado de protección, nodo y escudo de clústeres en Cloud Container Engine (CCE), lo que le ayuda a obtener información sobre el estado de seguridad de los clústeres en tiempo real.

Consulta de los clústeres

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, elija **Asset Management** > **Containers & Quota**. Haga clic en **Container Nodes**.

Paso 4 Vea el estado de protección de nodos en la página **Nodes**. Puede obtener los detalles en **Tabla 3-6**.

Tabla 3-6 Descripción del parámetro

Parámetro	Descripción
Protection Status	Estado de protección de un nodo. Las opciones son las siguientes: ● Unprotected ● Protected
Server Status	● Running ● Unavailable ● Normal
Agent Status	● Online ● Offline ● Not installed

----Fin

Consulta de cuotas de protección

En la página **Container Nodes**, haga clic en **Protection Quotas** para ver los detalles de la cuota.

Tabla 3-7 Descripción del parámetro

Parámetro	Descripción
Quota Version	Versión de la cuota comprada.
Quota ID	ID de la cuota comprada.
Quota Status	Estado de la cuota objetivo actual. ● Borrar la lista blanca de una cuota normal ● Borrar la lista blanca de una cuota vencida ● Borrar la lista blanca de una cuota congelada
Usage Status	Estado de uso actual de la cuota de destino. ● Normal ● In use
Expires	Tiempo antes de que expire una cuota de Container Guard Service (CGS)

- Haga clic en las áreas correspondientes de la columna **Operation** para renovar o renovar automáticamente las cuotas. Para obtener más información, consulte **¿Cómo renuevo mis cuotas de CGS?**
- Haga clic en **Unsubscribe** para cancelar la suscripción de la cuota CGS. Para obtener más información, consulte **¿Cómo cancelo la suscripción de una cuota de CGS?**

3.3.2 Imágenes de contenedores

3.3.2.1 Imágenes Locales

Esta sección describe cómo comprobar las vulnerabilidades en la imagen local y determinar si ignorar las vulnerabilidades.

Método de comprobación

Después de habilitar la protección de nodos, los clústeres se analizarán automáticamente.

Prerrequisitos

Se ha habilitado la función de protección de nodos.

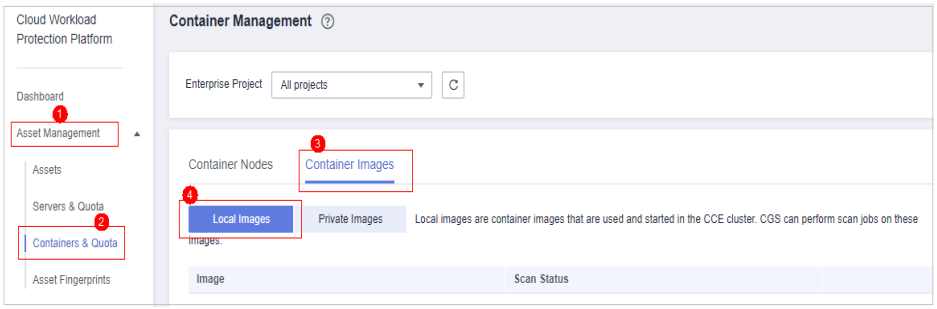
Consulta de los resultados del análisis de imágenes locales

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Seleccione una imagen local y vea los resultados del escaneo de imagen, como se muestra en **Figura 3-34**.

Figura 3-34 Consulta de los resultados del escaneo de imágenes



----Fin

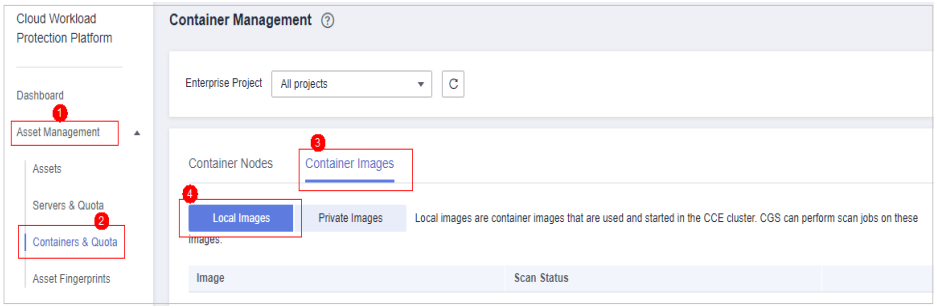
Consulta de la información básica y los informes de vulnerabilidades

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Seleccione una imagen local y vea los resultados del escaneo de imagen, como se muestra en **Figura 3-35**.

Figura 3-35 Consulta de los resultados del escaneo de imágenes



Paso 4 Haga clic en el nombre de la imagen para ver su información básica y los informes de vulnerabilidad.

----Fin

3.3.2.2 Imágenes privadas

Las imágenes en el repositorio de imágenes privadas son de SWR. CGS puede escanear estas imágenes y proporcionar informes y soluciones de vulnerabilidad. También puede comprobar la información de archivo malicioso, información de software, información de archivo y configuración de línea base.

Consulta de la lista de imágenes privadas

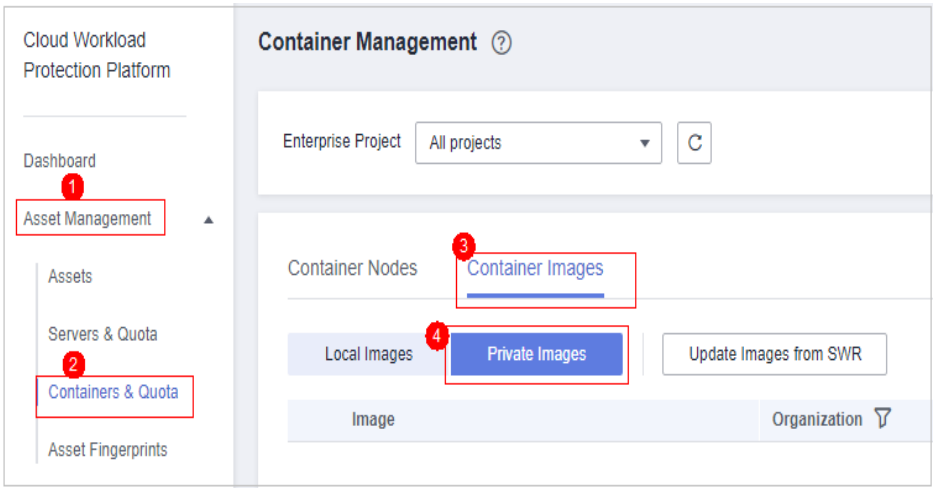
Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, elija **Asset Management** > **Containers & Quota**. En la página mostrada, elija **Container Images** > **Private Images**.

Paso 4 Vaya a la lista de imágenes privadas, como se muestra en **Figura 3-36**.

Figura 3-36 Acceder a la lista de imágenes privadas



Paso 5 Puede hacer clic en **Update Images from SWR** para actualizar las imágenes propias de SWR. Para obtener más información, consulte **Tabla 3-8**.

Tabla 3-8 Descripción del parámetro

Parámetro	Descripción	Operación
Image	Nombre de la imagen	Haga clic antes del nombre de una imagen para ver las versiones de la imagen.
Organization	Nombre de la organización a la que pertenece la imagen. La organización de la imagen es administrada por Software Repository for Container (SWR).	-
Image Versions	Número de versiones de imagen.	-

----Fin

Escaneo de una imagen privada

HSS escanea automáticamente todas las imágenes de contenedores privados a primera hora de la mañana todos los días. También puede elegir una imagen para escanear.

La duración de un análisis de seguridad depende del tamaño de la imagen escaneada. Generalmente, una imagen se puede escanear completamente en 3 minutos.

Una vez finalizado el análisis, haga clic en **View Report** para comprobar el informe de vulnerabilidad.

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Asset Management** > **Containers & Quota**.

Paso 4 Elija **Container Images** > **Private Images**, expanda los detalles del nombre de la imagen, y haga clic en **Security Scan** en la columna **Operation** de la fila que contiene la versión deseada para escanear una sola imagen.

Paso 5 En el cuadro de diálogo que se muestra, haga clic en **OK** para iniciar el trabajo de análisis.

Paso 6 **Scanned** en la columna **Scan Status** indica que se ha completado el escaneo de la imagen de destino.

----Fin

Consulta de Vulnerabilidades de Versión de Imagen Privada

Una vez completado el análisis, puede ver los informes de vulnerabilidades.

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Asset Management** > **Containers & Quota**.

Paso 4 Elija **Container Images** > **Private Images**, expanda los detalles del nombre de la imagen y haga clic en **View Report** en la columna **Operation** para ver los detalles de vulnerabilidad de la versión de imagen.

----Fin

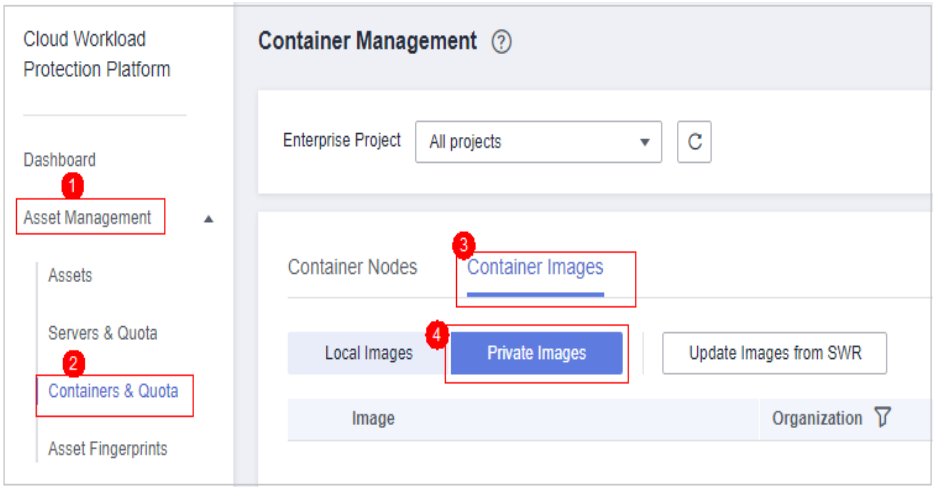
Consulta de información básica sobre una versión de imagen privada

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Vaya a la lista de imágenes privadas, como se muestra en **Figura 3-37**.

Figura 3-37 Acceder a la lista de imágenes privadas



Paso 4 Haga clic ⌄ antes del nombre de una imagen para ver las versiones de la imagen.

Paso 5 Haga clic en una versión para ver su información básica.

----Fin

Consulta de archivos maliciosos de una versión de imagen privada

Después de escanear las imágenes, puede ver archivos maliciosos en ellos. Esta sección describe cómo ver archivos maliciosos en una versión de imagen.

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Asset Management** > **Containers & Quota**.

Paso 4 Elija **Container Images** > **Private Images**, expanda los detalles del nombre de la imagen y haga clic en el nombre de la versión de la imagen para ir a la página de información básica de la versión de la imagen.

Paso 5 Haga clic en **Malicious Files** para ver los archivos maliciosos en la imagen.

----Fin

Consulta de información de software sobre una imagen privada

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Asset Management** > **Containers & Quota**.

Paso 4 Elija **Container Images** > **Private Images**, expanda los detalles del nombre de la imagen y haga clic en el nombre de la versión de la imagen para ir a la página de información básica de la versión de la imagen.

Paso 5 Haga clic en **Software Information** para ver el software contenido en la versión de la imagen, el tipo de software y el número de vulnerabilidades del software.

Paso 6 Haga clic junto al nombre de un software para ver el nombre de la vulnerabilidad del software, la urgencia de reparación y la solución.

----Fin

Consulta de información de archivo sobre una imagen privada

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Asset Management** > **Containers & Quota**.

Paso 4 Elija **Container Images** > **Private Images**, expanda los detalles del nombre de la imagen y haga clic en el nombre de la versión de la imagen para ir a la página de información básica de la versión de la imagen.

Paso 5 Haga clic en **File Information** para ver la información de archivo sobre la imagen.

Se muestran las cantidades y tamaños de paquetes de software y archivos no atribuibles, y los 50 principales archivos no atribuibles.

----Fin

Consulta de la configuración insegura de una imagen privada

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Asset Management** > **Containers & Quota**.

Paso 4 Elija **Container Images** > **Private Images**, expanda los detalles del nombre de la imagen y haga clic en el nombre de la versión de la imagen para ir a la página de información básica de la versión de la imagen.

Paso 5 Haga clic en **Unsafe Settings** para ver la configuración insegura y modificar las configuraciones según las sugerencias proporcionadas.

----Fin

3.4 Gestión de huellas dactilares de activos

3.4.1 Comprobación de detalles de activos

HSS comprueba de forma proactiva los puertos abiertos, los procesos, los directorios web, y las entradas de inicio automático en sus servidores Asset Management le brinda una mejor perspectiva sobre la información de activos del host y le permite identificar activos de

servidor riesgosos de manera oportuna. Para obtener más información sobre la gestión de activos, consulte **Gestión de activos**.

HSS no toca sus activos. Es necesario eliminar manualmente los riesgos.

Frecuencia de comprobación

La información de la cuenta y los puertos abiertos se comprueban en tiempo real. El resultado de la detección de puerto abierto se actualiza cada seis horas.

Los procesos, los directorios web, el software y las entradas de inicio automático se comprueban a primera hora de la mañana todos los días.

Consulta de información de activos

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Elija **Asset Management** > **Asset Fingerprints**, y haga clic en la pestaña correspondiente de la página mostrada para ver todos los activos detectados por HSS.

----Fin

Tabla 3-9 Huellas dactilares de activos

Artículo	Descripción	Frecuencia de comprobación
Account information management	Compruebe y administre todas las cuentas de sus servidores para mantenerlas seguras. Puede comprobar en tiempo real e información histórica de la cuenta para encontrar cuentas sospechosas. ● La información de la cuenta en tiempo real incluye el nombre de la cuenta, el número de servidores, el nombre del servidor/dirección IP, el permiso de inicio de sesión, el permiso de raíz, el grupo de usuarios, el directorio de usuarios, el shell iniciado por el usuario y la última hora de análisis. ● Los registros históricos de cambio de cuenta incluyen el nombre del servidor/dirección IP, el estado de cambio, el permiso de inicio de sesión, el permiso de raíz, el grupo de usuarios, el directorio de usuarios, el shell iniciado por el usuario y la última hora de análisis.	Comprobación en tiempo real

Artículo	Descripción	Frecuencia de comprobación
Open port check	Compruebe los puertos abiertos en sus servidores, incluidos los puertos riesgosos y desconocidos. Puede encontrar fácilmente puertos de alto riesgo comprobando puertos locales, tipos de protocolo, nombres de servidor, direcciones IP, estados, PID y archivos de programa. ● Desactivación manual de puertos de alto riesgo Si HSS detecta puertos abiertos de alto riesgo o puertos no utilizados, compruebe si sus servicios realmente los utilizan. Para puertos de alto riesgo, compruebe los archivos de programa. Si hay riesgos, elimine o aísle los archivos de origen. Se recomienda que maneje los puertos en el nivel de riesgo **Dangerous** con prontitud y que maneje los puertos en el nivel **Unknown** según las condiciones de servicio reales. ● Ignorar riesgos: Si un puerto de alto riesgo detectado es en realidad un puerto normal utilizado para los servicios, puede ignorarlo. El puerto ya no se considerará riesgoso ni generará alarmas.	Comprobación en tiempo real
Process check	Compruebe los procesos en sus servidores y encuentre procesos anormales. Puede identificar fácilmente rutas de proceso basadas en procesos anormales, nombres de servidor, direcciones IP, parámetros de inicio, tiempo de inicio, usuarios que ejecutan los procesos, permisos de archivo, PID y hashes de archivo. Si no se ha detectado un proceso sospechoso en los últimos 30 días, su información se eliminará automáticamente de la lista de procesos.	Comprobación en tiempo real
Software information management	Compruebe y gestione todo el software instalado en sus servidores e identifique las versiones inseguras. Puede comprobar la información histórica y en tiempo real del software para determinar si el software es arriesgado. ● La información del software en tiempo real incluye el nombre del software, el número de servidores, los nombres del servidor, las direcciones IP, las versiones del software, el tiempo de actualización del software y el tiempo de última exploración. ● Los registros históricos de cambios de software incluyen los nombres de servidor, direcciones IP, estados de cambios, versiones de software, tiempo de actualización de software y el último tiempo de análisis.	● Comprobación automática en la mañana temprano todos los días

Artículo	Descripción	Frecuencia de comprobación
Auto-started items	Compruebe si hay elementos de inicio automático y localizar rápidamente troyanos. ● La información en tiempo real sobre los elementos iniciados automáticamente incluye sus nombres, tipos (servicio de inicio automático, carpeta de inicio, biblioteca dinámica precargada, Ejecutar clave del Registro o tarea programada), número de servidores, nombres de servidor, direcciones IP, rutas de acceso, hashes de archivos, usuarios y la última hora de análisis. ● Los registros de cambios históricos de los elementos iniciados automáticamente incluyen nombres de servidor, direcciones IP, estados de cambios, rutas de acceso, hashes de archivo, usuarios y la última hora de análisis.	Comprobación en tiempo real
Website	Puede consultar estadísticas sobre directorios web y sitios a los que se puede acceder desde Internet. Puede ver los directorios y permisos, las rutas de acceso, los puertos externos, y los procesos clave de los sitios web.	Una vez a la semana (05:00 a.m. todos los lunes)
Web framework	Puede consultar estadísticas sobre marcos utilizados para la presentación de contenido web, incluidas sus versiones, rutas y procesos asociados.	Una vez a la semana (05:00 a.m. todos los lunes)
Middleware	Puede comprobar la información sobre servidores, versiones, rutas y procesos asociados con middleware.	Una vez a la semana (05:00 a.m. todos los lunes)
Kernel module	Compruebe la información acerca de todos los archivos de módulo de programa que se ejecutan en los núcleos, incluidos los servidores asociados, los números de versión, las descripciones de los módulos, las rutas de los archivos del controlador, los permisos de archivos y los hashes de archivos.	Una vez a la semana (05:00 a.m. todos los lunes)

3.4.2 Comprobación del historial de operaciones

HSS registra proactivamente los cambios en la información de la cuenta, la información de software y los elementos iniciados automáticamente. Puede comprobar los detalles de cambio según diferentes dimensiones y rangos de tiempo.

Comprobación de registros de cambio

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Elija **Asset Management** > **Asset Fingerprints**. Haga clic en la pestaña **Operation History**. Seleccione un intervalo de tiempo y compruebe el historial de cambios de la cuenta, el software y el elemento de inicio automático.

----Fin

Gestión de la información de la cuenta

Las operaciones realizadas a las cuentas se registran.

- La columna **Action** registra las operaciones. Su valor puede ser **Create** (recientemente encontrado en la última comprobación), **Delete** (encontrado en cheques anteriores pero falta en el último cheque) y **Modify**, (se detectan cambios en la información de la cuenta, como nombres de cuenta, derechos de administrador y grupos de usuarios).
- La última hora de análisis indica la hora del último análisis realizado para los servidores en un período.

Puede consultar la información y los cambios en todas las cuentas aquí. Si encuentra cuentas innecesarias o superprivilegiadas (como **root**) que no son obligatorias para los servicios, elimínelas o modifique sus permisos para evitar ataques.

Gestión de software

Las operaciones realizadas a las cuentas se registran.

- **Action**: **Create** y **Delete**.
- El último tiempo de escaneo registra la hora en que se obtuvieron los cambios, no la hora en que se realizaron.

Puede comprobar la información y los cambios en todo el software, actualizar el software y eliminar el software que es innecesario, sospechoso o en la versión anterior.

Elementos iniciados automáticamente

Los troyanos suelen entrometerse en los servidores mediante la creación de servicios de inicio automático, tareas programadas, bibliotecas dinámicas precargadas, claves de registro de ejecución o carpetas de inicio. La función de comprobación de inicio automático recopila información sobre todos los elementos iniciados automáticamente, incluidos sus nombres, tipos y número de servidores afectados, lo que facilita la localización de elementos iniciados automáticamente sospechosos.

Puede comprobar los servidores, las direcciones IP, los cambios, las rutas, los hashes de archivos, los usuarios y la última hora de análisis de los elementos de inicio automático.

3.5 Gestión de cuotas de protección

3.5.1 Visualización de cuotas

Puede comprobar, renovar y cancelar la suscripción de su cuota en la lista de servidores.

Solo se muestra la cuota comprada en la región seleccionada. Si no se encuentra su cuota, asegúrese de haber cambiado a la región correcta y vuelva a buscar.

Cuota HSS

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En la página **Servers & Quota**, haga clic en **Quotas**.

Paso 4 Compruebe las cuotas y los servidores vinculados a ellas.

- Puede hacer clic en **All**, **Enterprise**, **Premium**, o **Web Tamper Protection (WTP)** en el área **Edition** para comprobar las cuotas de versión y los servidores enlazados a ellas.
- Puede hacer clic en **All**, **In use**, o **Idle** en el área **Usage Status** para comprobar el uso de la cuota.

Tabla 3-10 Descripción del parámetro

Parámetro	Descripción
Edition	Edición de cuota
Quota ID	ID de cuota
Quota Status	● **Available**: la cuota no ha caducado y se puede utilizar correctamente. ● **Expired**: la cuota ha caducado. Durante este período, todavía puede usar la cuota. ● **Frozen**: la cuota ya no protege sus servidores. Cuando expire el período congelado, la cuota se eliminará de forma permanente.
Usage Status	● **In use**: La cuota se está utilizando para un servidor. El nombre del servidor se muestra debajo del estado. ● **Idle**: la cuota no está en uso.

NOTA

- Vinculación de cuota a un servidor

  Como alternativa, en la pestaña **Quotas** de la página **Servers & Quota**, haga clic en **Bind Server** en la columna **Operation** para enlazar una cuota a un host. HSS habilitará automáticamente la protección para el servidor.

  Una cuota puede estar vinculada a un servidor para protegerla, a condición de que el agente en el servidor esté en línea.

- Desvincular

  En la pestaña **Quotas** de la página **Servers & Quota**, haga clic en **Unbind** en la columna **Operation** de una cuota. HSS deshabilitará automáticamente la protección para el servidor correspondiente y el estado de la cuota cambiará a **Idle**.

----Fin

Cuota del contenedor

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, elija **Asset Management** > **Containers & Quota**. En la página mostrada, haga clic en la pestaña **Protection Quotas**.

Paso 4 Compruebe las cuotas y los nodos vinculados a ellas.

Tabla 3-11 Descripción del parámetro

Parámetro	Descripción
Quota Version	Versión de cuota.
Quota ID	ID de cuota
Quota Status	● **In use**: se está utilizando la cuota. ● **Idle**: la cuota no se ha utilizado. ● **Frozen**: la cuota ya no protege sus servidores. Cuando expire el período congelado, la cuota se eliminará de forma permanente.
Usage Status	● **In use**: La cuota se está utilizando para un servidor. El nombre del servidor se muestra debajo del estado. ● **Idle**: la cuota no está en uso.

NOTA

- Renovación

  Puede hacer clic en **Renew** en la columna **Operation** de la cuota para renovarla. Para obtener más información, consulte **¿Cómo puedo renovar HSS?**
- Cancelación de suscripción

  Puede hacer clic en **Unsubscribe** en la columna **Operation** de la cuota para cancelar su suscripción. Para obtener más información, consulte **¿Cómo solicito una cancelación de suscripción y reembolso?**

----Fin

3.5.2 Vinculación de una cuota a un servidor

Una cuota puede estar vinculada a un servidor para protegerla, a condición de que el agente en el servidor esté en línea.

Prerrequisitos

- Se han obtenido las credenciales de inicio de sesión.
- El agente se ha instalado en el servidor que desea proteger.

- La cuota está en estado **Available** y su **Usage Status** es **Idle**.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En la página **Servers & Quota**, haga clic en **Quotas**.

Paso 4 En la página Detalles de la cuota, haga clic en **Bind Server** en la fila de la cuota.

NOTA

Para habilitar la protección WTP para un servidor, elija **Prevention** > **Web Tamper Protection**, busque la fila que contiene el servidor en la nube de destino y haga clic en el área correspondiente en la columna **Operation** para habilitar la protección.

Paso 5 Seleccione un servidor.

Paso 6 Haga clic en **OK**. HSS habilitará automáticamente la protección para el servidor.

----Fin

3.5.3 Desvincular una cuota de un servidor

Puede desvincular cuotas de servidores que ya no necesitan estar protegidos. Tenga cuidado al realizar esta operación, ya que los servidores desprotegidos están expuestos a riesgos de seguridad.

Después de desvincular una cuota, puede vincularla a otro servidor o cancelar su suscripción para reducir costos.

Prerrequisitos

- Ha obtenido un nombre de usuario y su contraseña para iniciar sesión en la consola de gestión.
- Los contingentes que deben no consolidarse están en uso.

Desvincular una cuota de un servidor

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En la página **Servers & Quota**, haga clic en **Quotas**.

Paso 4 En la lista de cuotas, haga clic en **Unbind**.

NOTA

Para desvincular varias cuotas a la vez, selecciónelas y desvincularlas en lotes. Tenga cuidado al realizar esta operación, ya que los servidores desprotegidos están expuestos a riesgos de seguridad.

Paso 5 En el cuadro de diálogo de confirmación, haga clic en **OK**.

----Fin

3.5.4 Actualización de su edición

Puede actualizar a una edición superior y disfrutar de características de seguridad más fuertes.

Si tiene la edición básica o empresarial, puede actualizarla a la edición empresarial, premium o WTP según sea necesario.

Precauciones

- Las ediciones WTP y contenedor son las ediciones más altas y no se pueden actualizar.
- Una edición se puede actualizar directamente a la edición empresarial o premium. Para actualizar a la edición WTP, debe comprarla por separado y luego vincularla a un servidor.
- La edición básica se puede actualizar a la edición empresarial, premium o WTP. La edición empresarial se puede actualizar a la edición premium o WTP. La edición premium solo se puede actualizar a la edición WTP.

Prerrequisitos

- El **Usage Status** de una cuota debe ser **Idle**.
- El **Quota Status** de una cuota debe ser **Normal**.

Actualización a la edición Enterprise/Premium

Para actualizar una cuota que se utiliza para proteger un servidor, desvinúelo del servidor primero.

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

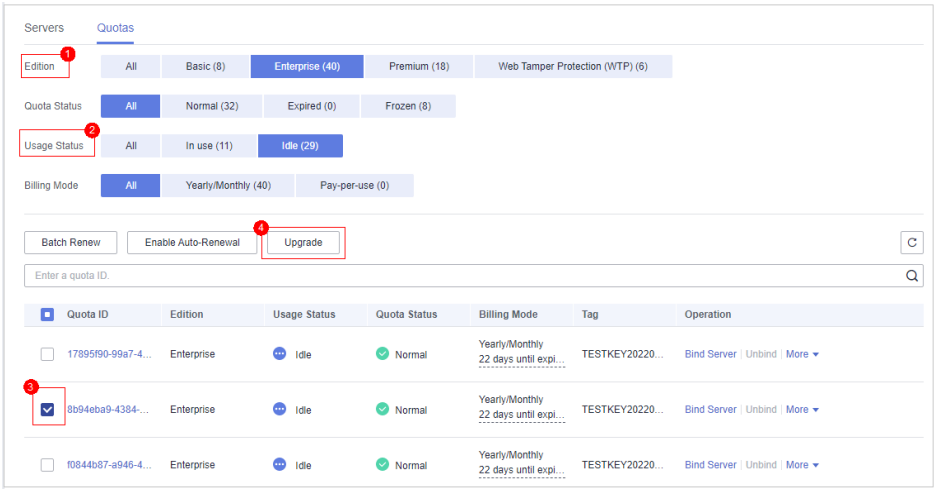
Paso 3 En la página **Servers & Quota**, haga clic en **Quotas**.

Paso 4 En la lista de cuotas, filtre las cuotas inactivas de la edición básica o de empresa. Seleccione una cuota y haga clic en **Upgrade**.

NOTA

- Antes de actualizar una cuota en uso, **desvincularla** del servidor que protege.
- La desvinculación no afecta a los servicios.

Figura 3-38 Selección de una cuota

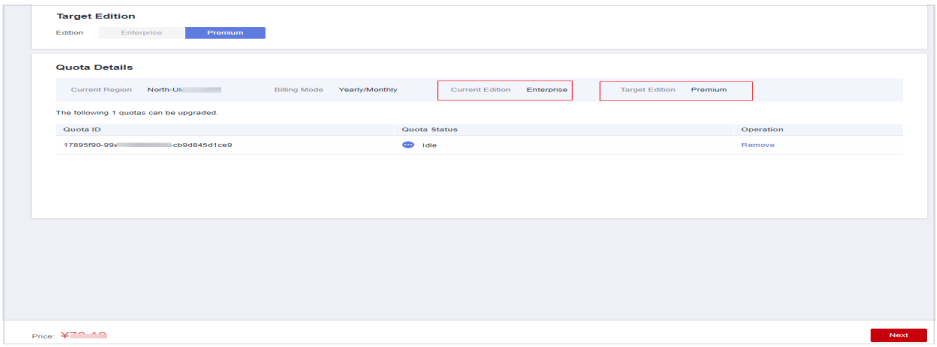


Paso 5 Configurar la información de actualización.

NOTA

La edición básica se puede actualizar a la edición empresarial o premium. La edición empresarial se actualiza a la edición premium de forma predeterminada.

Figura 3-39 Confirmación de la información de actualización



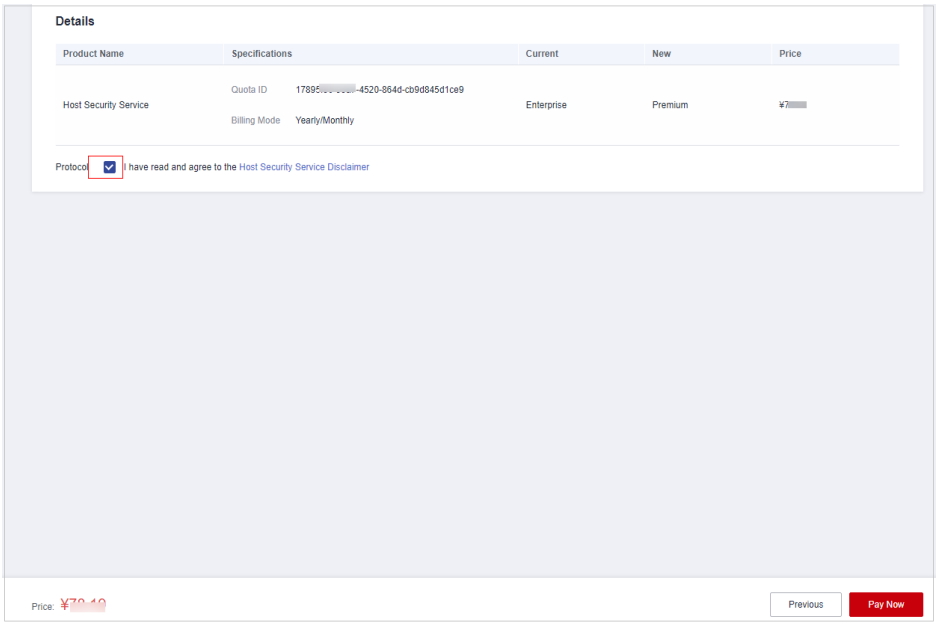
Paso 6 Confirme la versión de actualización y haga clic en **Next**.

NOTA

Cuando paga por la mejora, solo necesitas compensar la diferencia.

Paso 7 Confirme la información de compra, seleccione **I have read and agree to the Host Security Service Disclaimer** y haga clic en **Pay Now**.

Figura 3-40 Confirmación de la información del pedido



Paso 8 Espere hasta que se complete el pago. Volver a la **lista de cuotas**. Localice la cuota por su ID y verifique su edición.

Paso 9 **Vicular la cuota** a un servidor y habilitar la protección.

----Fin

Actualización a la edición WTP

La edición WTP no se puede actualizar directamente desde una edición inferior y debe comprarse por separado. Antes de proteger un servidor con WTP, asegúrese de que el servidor no está vinculado a ninguna cuota.

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En la esquina superior derecha de la página **Dashboard**, haz clic en **Buy HSS**.

Paso 4 En la página **Buy HSS**, seleccione la edición WTP.

Figura 3-41 Compra de una cuota WTP

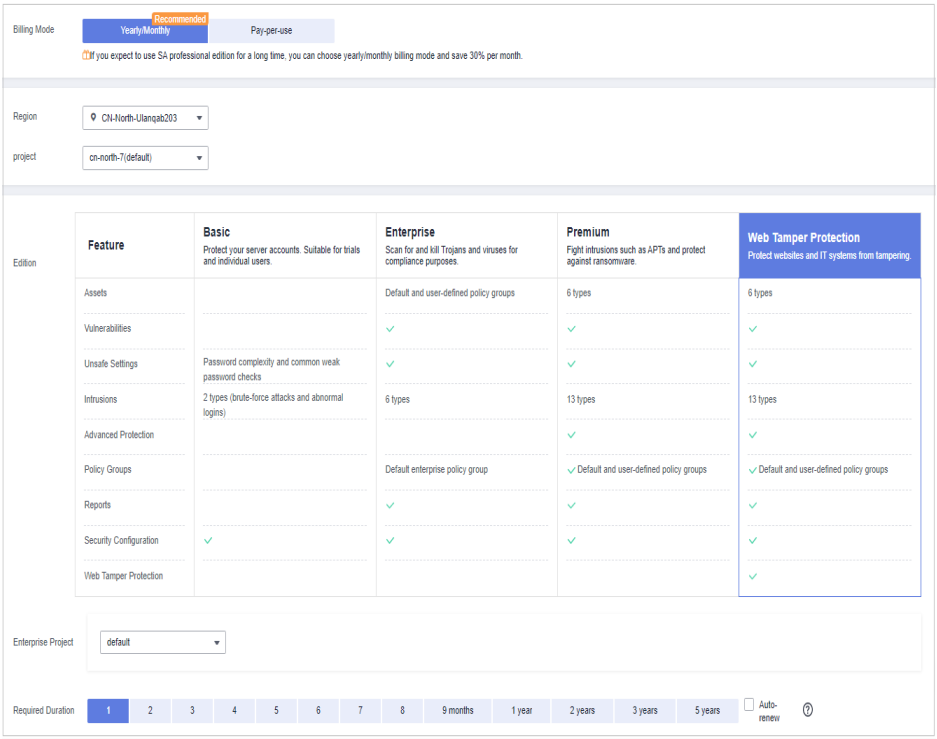


Tabla 3-12 Parámetros para la compra de HSS

Parámetro	Descripción	Valor de ejemplo
Billing Mode	Seleccione el modo de facturación de **Yearly/Monthly** o de **Pay-per-use** según sus requisitos. ● Anual/Mensual: puede seleccionar la edición empresarial, la edición definitiva o la edición de protección contra manipulaciones web. Puede comprar la edición por un período de tiempo fijo. La tarifa es un 30% más baja que la del pago por uso. Si utiliza la edición durante mucho tiempo, le aconsejamos que la compre periódicamente. ● En el modo de pago por uso, solo puede comprar la edición empresarial. Debe habilitar esta edición en la lista de servidores. Usted paga por la duración de uso de los recursos. Los precios se calculan por hora y no se requiere una tarifa mínima. **NOTA** Procedimiento para permitir la cuota de pago por uso: 1. En la página de compra, selecciona **Pay-per-use**. La edición **Enterprise** se seleccionará automáticamente. En la esquina inferior derecha, haz clic en **Enable Now**. Será redirigido a la lista de servidores. 2. En la columna **Operation** de un servidor, haga clic en **Enable**. Establezca **Billing Mode** en **Pay-per-use** y establezca **Edition** en **Enterprise**. También puede seleccionar **Basic**, que es gratuito durante 30 días. 3. Confirme la información y haga clic en **OK**.	Yearly/ Monthly

Parámetro	Descripción	Valor de ejemplo
Region	● Para minimizar los problemas de conexión, compre la cuota en la región de sus servidores.	CN-Hong Kong
Edition	Puede adquirir la edición **Basic (free)**, **Enterprise**, **Premium**, o **Web Tamper Protection**. Para obtener más información sobre las diferencias entre ediciones, consulte **Ediciones**. **AVISO** ● No es necesario adquirir la edición básica. Puede **habilitarlo** en la lista de servidores. ● Si adquirió la edición básica, empresarial o premium, habilítela en la página **Asset Management** > **Servers & Quota**. ● Si adquirió la edición WTP, habilitela en la lista de servidores de la página **Prevention** > **Web Tamper Protection**.	Enterprise
Enterprise Project	Esta opción sólo está disponible cuando ha iniciado sesión con una cuenta de empresa o cuando ha habilitado proyectos de empresa. Puede ponerse en contacto con su administrador de servicio para activar esta función y poner los recursos de la nube y los miembros en proyectos empresariales para una gestión centralizada. Seleccione un proyecto de empresa en la lista desplegable. **NOTA** ● Los recursos y los gastos incurridos se gestionan en el proyecto de empresa seleccionado. ● Valor **default** indica el proyecto de empresa predeterminado. Los recursos que no están asignados a ningún proyecto de empresa de su cuenta se muestran en el proyecto de empresa predeterminado. ● La opción **default** está disponible en la lista desplegable **Enterprise Project** solo después de comprar HSS en su cuenta de Huawei Cloud.	default
Required duration	● Seleccione una duración en función de sus requisitos. En el modo de **Pay-per-use**, no es necesario seleccionar una duración. ● Le recomendamos que seleccione **Auto-renew** para asegurarse de que sus servidores estén siempre protegidos. ● Si selecciona **Auto-renew**, el sistema renovará automáticamente tu suscripción siempre y cuando el saldo de tu cuenta sea suficiente. El período de renovación es el mismo que la duración requerida. ● Si no selecciona **Auto-renew**, renueve manualmente el servicio antes de que caduque.	1 year
Server Quota	Introduzca el número de cuotas de HSS que se van a comprar. En el modo de **Pay-per-use**, no es necesario configurar esta opción. **AVISO** ● Todos sus servidores deben estar protegidos, por lo que si un virus (como ransomware o un programa de minería) infecta uno de ellos, no será capaz de propagarse a otros y dañar toda su red. ● No se puede modificar la cuota de una edición una vez completada su compra. Puede darse de baja de él y comprar de nuevo.	20

Parámetro	Descripción	Valor de ejemplo
Tag	Puede poner etiquetas en los recursos de la nube del mismo tipo para ayudarle a buscar rápidamente recursos de la nube. En el modo de **Pay-per-use**, no es necesario configurar las etiquetas.	data

Paso 5 En la esquina inferior derecha de la página, haz clic en **Next**.

Para obtener más información sobre los precios, consulte **Detalles de precios del producto**.

Paso 6 Después de confirmar que el pedido, seleccione **I have read and agree to the Host Security Service Disclaimer** y haga clic en **Pay Now**.

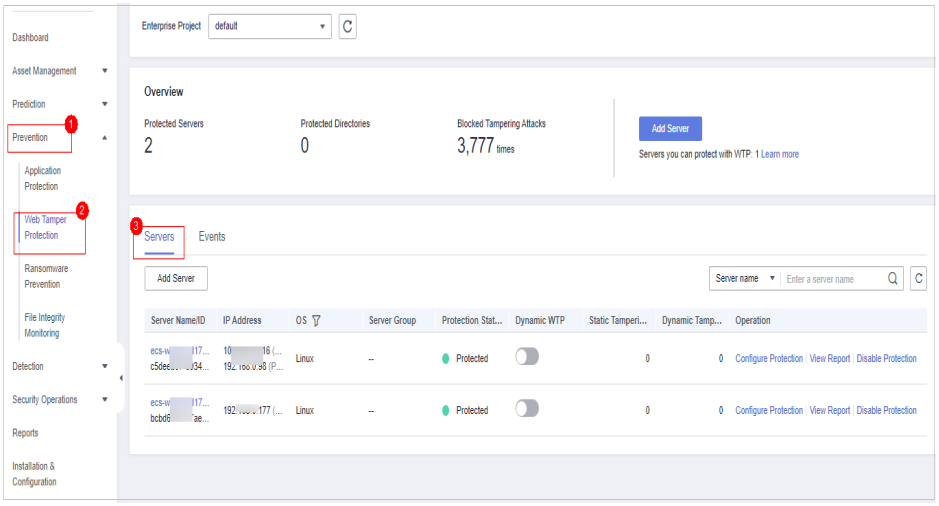
Paso 7 En la página mostrada, haga clic en **Pay** y complete el pago.

Paso 8 En el panel de navegación, elija **Prevention** > **Web Tamper Protection**. En la pestaña **Servers**, haga clic en **Add Server**.

AVISO

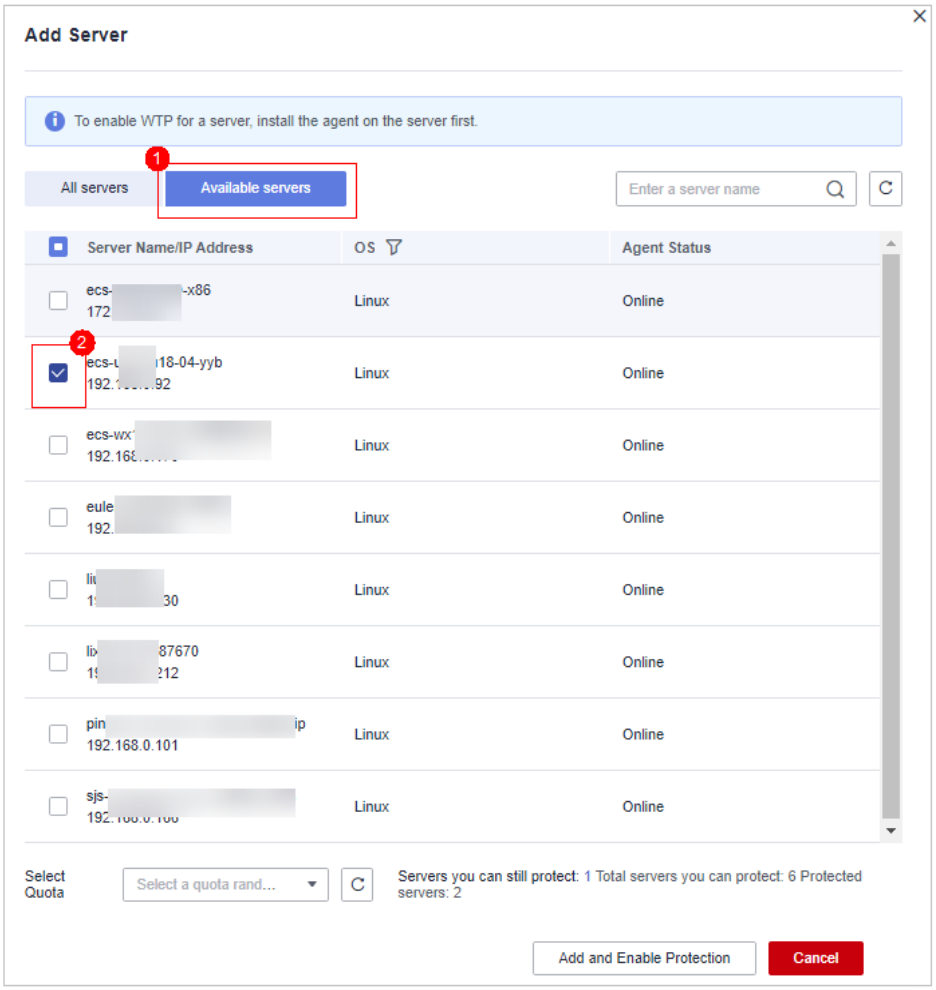
- Asegúrese de que el servidor que va a ser protegido por WTP no está vinculado a otras cuotas. Elija **Asset Management** > **Servers & Quota** y haga clic en la pestaña **Servers**. Si el estado de protección del servidor es **Protected**, indica que el servidor está enlazado a otra cuota. En este caso, haga clic en **Disable** en la columna **Operation**.
- La desvinculación de un servidor de una cuota no afecta a los servicios.

Figura 3-42 Página de configuración de protección



Paso 9 Haga clic en **Add Server**, seleccione un servidor y haga clic en **Add and Enable Protection**.

Figura 3-43 Selección de un servidor



Paso 10 Verifique las configuraciones de WTP. Elija **Asset Management** > **Servers & Quota** y haga clic en la pestaña **Servers**. Si se muestra **WTP** en la columna **Edition/Expiration Date**, se ha habilitado la edición WTP.

NOTA

Si no necesita reemplazar la cuota por WTP, puede darse de baja de ella. Elija **Asset Management** > **Servers & Quota** y haga clic en **Quotas**. En la columna **Operation** de la cuota, elija **More** > **Unsubscribe**.

----Fin

4 Prevención de Riesgos

4.1 Gestión de vulnerabilidades

4.1.1 Descripción general de la gestión de vulnerabilidades

HSS detecta vulnerabilidades de Linux, Windows, Web-CMS y aplicaciones y proporciona una visión general de la vulnerabilidad, que incluye detalles de detección de vulnerabilidades de host, estadísticas de vulnerabilidad, distribución de tipos de vulnerabilidad, 5 vulnerabilidades principales y 5 servidores de riesgo principales, lo que le ayuda a aprender las vulnerabilidades de host en tiempo real.

Mecanismos de detección

Tabla 4-1 Mecanismos de detección de vulnerabilidad

Tipo	Mecanismo
Linux vulnerability management	CWPP detecta vulnerabilidades en el sistema y el software (como SSH, OpenSSL, Apache y MySQL) basándose en bibliotecas de vulnerabilidades, informa los resultados a la consola de gestión y genera alarmas.
Windows vulnerability	CWPP se suscribe a las actualizaciones oficiales de Microsoft, comprueba si los parches en el servidor se han actualizado, envía parches oficiales de Microsoft, informa los resultados a la consola de gestión y genera alarmas de vulnerabilidad.
Web-CMS vulnerabilities	CWPP comprueba los directorios web y los archivos para detectar vulnerabilidades de Web-CMS, informa los resultados a la consola de gestión y genera alarmas de vulnerabilidad.
Application Vulnerabilities	CWPP detecta las vulnerabilidades en los paquetes de software y dependencias que se ejecutan en el servidor, informa las vulnerabilidades de riesgo a la consola y muestra las alarmas de vulnerabilidad.

NOTA

Se muestran las vulnerabilidades detectadas en las últimas 24 horas. El nombre de servidor en una notificación de vulnerabilidad es el nombre utilizado cuando se detectó la vulnerabilidad y puede ser diferente del nombre de servidor más reciente.

Restricciones

No se admite el estándar de Windows Server 2012.

Frecuencia de comprobación

HSS realiza automáticamente una verificación completa a primera hora de la mañana todos los días.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación izquierdo, elija **Prediction** > **Vulnerabilities**.

----Fin

Detalles de Detección de Vulnerabilidad del Host

Se muestra el número total de servidores, así como el número de servidores detectados, no detectados y afectados.

Vulnerabilidades

Se muestra el número de vulnerabilidades no controladas, urgentes y menores.

Distribución de sistema operativo

Se muestra el número total de vulnerabilidades de Linux, Windows, aplicaciones y Web-CMS.

Puede comprobar los números de cada tipo de vulnerabilidad haciendo clic en el nombre correspondiente.

Las 5 principales vulnerabilidades

Se muestran las 5 principales vulnerabilidades.

Los 5 mejores servidores arriesgados

Se muestran los 5 mejores servidores arriesgados.

4.1.2 Consulta de detalles de una vulnerabilidad

Vulnerabilidades de Linux/Vulnerabilidades de Windows/Vulnerabilidades de Web-CMS/Vulnerabilidades de aplicaciones

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación izquierdo, elija **Prediction** > **Vulnerabilities**.

Paso 4 En la página mostrada, haga clic en **Linux Vulnerabilities**, **Windows Vulnerabilities**, **Application Vulnerabilities**, o **Web-CMS Vulnerabilities**.

Paso 5 Haga clic en un nombre de vulnerabilidad para ver la información básica, la solución y la descripción de CVE.

Paso 6 Haga clic en la pestaña correspondiente para ver los servidores afectados por la vulnerabilidad y manejar la vulnerabilidad.

- Para corregir la vulnerabilidad, haga clic en **Handle**.
- Para ignorar la vulnerabilidad, haga clic en **Ignore**. HSS ya no generará alarmas para esta vulnerabilidad.
- Una vez que se corrija la vulnerabilidad, puede hacer clic en **Verify** para verificar la corrección.

  HSS realiza un chequeo completo cada mañana temprano. Si no realiza una verificación manual, puede ver el resultado de la comprobación del sistema al día siguiente después de corregir la vulnerabilidad.

  Si aún se detecta una vulnerabilidad después de corregirla, rectifique la falla consultando **¿Por qué se siguen mostrando las alarmas de vulnerabilidades fijas?**

  Si no se puede corregir una vulnerabilidad, haga clic en **View Cause** para comprobar los detalles.

----Fin

Exportación de un informe de vulnerabilidad

Vaya a la pestaña de la vulnerabilidad de destino. En la esquina superior derecha de la lista de vulnerabilidades, haga clic en para exportar los informes de vulnerabilidades.

NOTA

Se puede exportar un máximo de 5000 vulnerabilidades de aplicación a la vez.

4.1.3 Corrección de vulnerabilidades y verificación del resultado

- Vulnerabilidades de Linux o Windows

  Puede seleccionar servidores y hacer clic en **Handle** para corregir las vulnerabilidades, o arreglarlas manualmente según las sugerencias proporcionadas.

A continuación, puede utilizar la función de verificación para comprobar rápidamente si la vulnerabilidad se ha corregido.

AVISO

Para corregir las vulnerabilidades de Windows, debe conectarse a Internet.

- Vulnerabilidades de CMS web

  Solucionarlos manualmente en función de las sugerencias proporcionadas en la página.
- Vulnerabilidades de aplicación

  Solucionarlos manualmente en función de las sugerencias proporcionadas en la página.

Precauciones

- Las operaciones de corrección de vulnerabilidad no se pueden revertir. Si una vulnerabilidad no se soluciona, es probable que se interrumpan los servicios y que se produzcan problemas de incompatibilidad en aplicaciones de middleware o de capa superior. Para evitar errores irrecuperables, se recomienda utilizar Cloud Server Backup Service (CSBS) para hacer una copia de seguridad de sus servidores. Para obtener más información, consulte **Creación de una copia de seguridad CSBS**. A continuación, utilice servidores inactivos para simular el entorno de producción y probar la vulnerabilidad. Si la revisión de prueba se realiza correctamente, corrija la vulnerabilidad en los servidores que se ejecutan en el entorno de producción.
- Los servidores necesitan acceder a Internet y utilizar fuentes de imágenes externas para corregir vulnerabilidades. Si sus servidores no pueden acceder a Internet o las fuentes de imagen externas no pueden proporcionar servicios estables, puede usar la fuente de imagen proporcionada por Huawei Cloud para corregir vulnerabilidades.

  Antes de corregir vulnerabilidades en línea, configure las fuentes de imagen de Huawei Cloud que coincidan con los sistemas operativos de su servidor. Para obtener más información, consulte **Gestión de orígenes de imágenes**.

Urgencia

- **High**: Esta vulnerabilidad debe corregirse lo antes posible. Los atacantes pueden aprovechar esta vulnerabilidad para dañar el servidor.
- **Medium**: Se recomienda corregir la vulnerabilidad para mejorar la seguridad de su servidor.
- **Safe for now**: Esta vulnerabilidad tiene una pequeña amenaza para la seguridad del servidor. Puede elegir arreglarlo o ignorarlo.

Pantalla de vulnerabilidades

- Las vulnerabilidades que no se han solucionado o que no se han manejado siempre se muestran en la lista de vulnerabilidades.
- Las vulnerabilidades corregidas permanecerán en la lista dentro de los 30 días posteriores a su corrección.

Corrección de vulnerabilidades en un solo clic

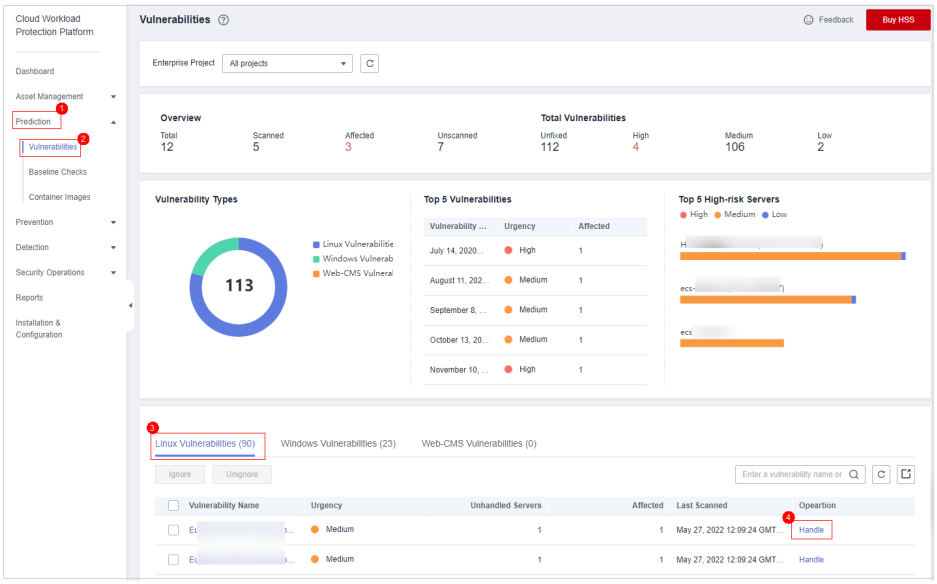
Puede corregir vulnerabilidades en el sistema operativo Linux o Windows con un solo clic en la consola.

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Haga clic en **Handle**, como se muestra en **Figura 4-1**.

Figura 4-1 Corrección de vulnerabilidades



Paso 4 En la página mostrada, seleccione los servidores afectados y haga clic en **Fix**, como se muestra en **Figura 4-2**.

Figura 4-2 Solución de vulnerabilidad con un solo clic

Paso 5 En el cuadro de diálogo que se muestra, seleccione "I am aware that if I have not backed up my ECSs before fixing vulnerabilities, services may be interrupted and fail to be rolled back during maintenance."

Paso 6 Haga clic en **OK** para corregir la vulnerabilidad en modo de un solo clic. El estado de vulnerabilidad cambiará a **Fixing**.

Si se corrige una vulnerabilidad, su estado cambiará a **Fixed**. Si no se corrige, su estado cambiará a **Failed**.

NOTA

Reinicie el sistema después de corregir una vulnerabilidad del kernel de Linux, o HSS probablemente continuará advirtiéndole de esta vulnerabilidad.

----Fin

Reparación manual de vulnerabilidades de software

Solucione la vulnerabilidad detectada en función de las sugerencias de corrección en la columna **Solution**. Para obtener más información sobre los comandos de corrección de vulnerabilidades, consulte **Tabla 4-2**.

- Corrija las vulnerabilidades en secuencia según las sugerencias.
- Si varios paquetes de software en el mismo servidor tienen la misma vulnerabilidad, solo necesita corregir la vulnerabilidad una vez.

NOTA

Reinicie el sistema después de corregir una **Windows OS** o **Linux kernel vulnerability**, o HSS probablemente continuará advirtiéndole de esta vulnerabilidad.

Tabla 4-2 Comandos de corrección de vulnerabilidad

Sistema operativo	Comando
CentOS/Fedora/EulerOS/Red Hat/Oracle	**yum update** *Software_name*
Debian/Ubuntu	**apt-get update && apt-get install** *Software_name* **--only-upgrade**
Gentoo	Consulte las sugerencias de corrección de vulnerabilidades para obtener más detalles.

La corrección de la vulnerabilidad puede afectar a la estabilidad del servicio. Se recomienda utilizar cualquiera de los siguientes métodos para evitar tal impacto:

Método 1: Crear una nueva VM para corregir la vulnerabilidad.

1. Cree una imagen para que el ECS se solucione. Para obtener más información, consulte **Creación de una imagen de ECS completa mediante un ECS**.
2. Utilice la imagen para crear un ECS. Para obtener más información, consulte **Creación de ECS mediante una imagen**.
3. Solucione la vulnerabilidad en el nuevo ECS y verifique el resultado.
4. Cambie los servicios al nuevo ECS y verifique que se estén ejecutando de forma estable.
5. Libera el ECS original. Si se produce un error después de la conmutación del servicio y no se puede rectificar, puede cambiar los servicios de nuevo al ECS original.

Método 2: Solucionar la vulnerabilidad en el servidor de destino.

1. Cree una copia de respaldo para que el ECS se solucione. Para obtener más información, consulte **Creación de una copia de respaldo CSBS**.

2. Corregir vulnerabilidades en el servidor actual.
3. Si los servicios no están disponibles después de corregir la vulnerabilidad y no se pueden recuperar oportunamente, utilice la copia de respaldo para restaurar el servidor. Para obtener más información, consulte **Uso de copias de seguridad para restaurar servidores**.

NOTA

- Utilice el método 1 si va a corregir una vulnerabilidad por primera vez y no puede estimar el impacto en los servicios. Se recomienda elegir el modo de facturación de pago por uso para el ECS recién creado. Después del cambio de servicio, puede cambiar el modo de facturación a anual/mensual. De esta manera, puede liberar el ECS en cualquier momento para ahorrar costos si la vulnerabilidad no se soluciona.
- Utilice el método 2 si ha corregido anteriormente la vulnerabilidad en servidores similares.

Ignorar vulnerabilidades

Algunas vulnerabilidades son riesgosas solo en condiciones específicas. Por ejemplo, si una vulnerabilidad solo se puede explotar a través de un puerto abierto, pero el servidor de destino no abre ningún puerto, la vulnerabilidad no dañará al servidor. Tales vulnerabilidades pueden ser ignoradas.

HSS no generará alarmas para vulnerabilidades ignoradas.

Verificación de la solución de vulnerabilidades

Una vez que se corrija una vulnerabilidad, se recomienda verificarla inmediatamente.

Verificación manual

- Haga clic en **Verify** en la página de detalles de vulnerabilidad.
- Asegúrese de que el software se ha actualizado a la última versión. La siguiente tabla proporciona los comandos para comprobar el resultado de la actualización de software.

Tabla 4-3 Comandos de verificación

Sistema operativo	Comando de verificación
CentOS/Fedora/EulerOS/Red Hat/Oracle	rpm -qa | grep *Software_name*
Debian/Ubuntu	dpkg -l | grep *Software_name*
Gentoo	emerge --search *Software_name*

- **Comprobar manualmente si hay vulnerabilidades** y ver los resultados de la corrección de vulnerabilidades.

Verificación automática

HSS realiza un chequeo completo cada mañana temprano. Si no realiza una verificación manual, puede ver el resultado de la comprobación del sistema al día siguiente después de corregir la vulnerabilidad.

4.2 Inspección de línea de base

4.2.1 Descripción general de la inspección de línea de base

HSS detecta políticas complejas, contraseñas débiles y detalles de configuración, incluida la tasa de configuración segura, los 5 mejores servidores con configuraciones inseguras, los servidores con contraseñas débiles y los 5 mejores servidores con contraseñas débiles. HSS comprueba de forma proactiva las políticas de complejidad de contraseñas débiles y otras configuraciones inseguras, y proporciona **sugerencias** para solucionar los riesgos detectados.

Prerrequisitos

Sólo se comprueban los servidores protegidos por la edición empresarial o superior.

Frecuencia de comprobación

- HSS realiza automáticamente una verificación completa a las 04:00 todos los días.
- Si desea personalizar el período y el tiempo de verificación, puede comprar ediciones premium, Web Tamper Protection (WTP) y Container Guard Security (CGS). Para más detalles, consulte **Comprobación de configuración**.
- Puede elegir **Prediction** > **Baseline Checks**, seleccionar la política de línea de base de destino y hacer clic en **Scan** en la esquina derecha para realizar una comprobación manual con un solo clic en los servidores asociados a la política de línea de base.

Elementos de comprobación

Elementos	Descripción
Password Complexity Policy Detection	Compruebe las políticas de complejidad de las contraseñas y modifíquelas según las sugerencias proporcionadas por HSS para mejorar la seguridad de las contraseñas.
Common Weak Password Detection	Cambie las contraseñas débiles por contraseñas más fuertes según los resultados y sugerencias del análisis HSS.
Unsafe Configurations	Compruebe las configuraciones de inicio de sesión inseguras de Tomcat, Nginx y SSH encontradas por HSS.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, seleccione **Prediction** > **Baseline Checks**.

Paso 4 Haga clic en distintas pestañas de la página mostrada para comprobar las configuraciones inseguras detectadas. **Tabla 4-4** enumera los parámetros correspondientes.

Figura 4-3 Descripción general de la comprobación de línea de base

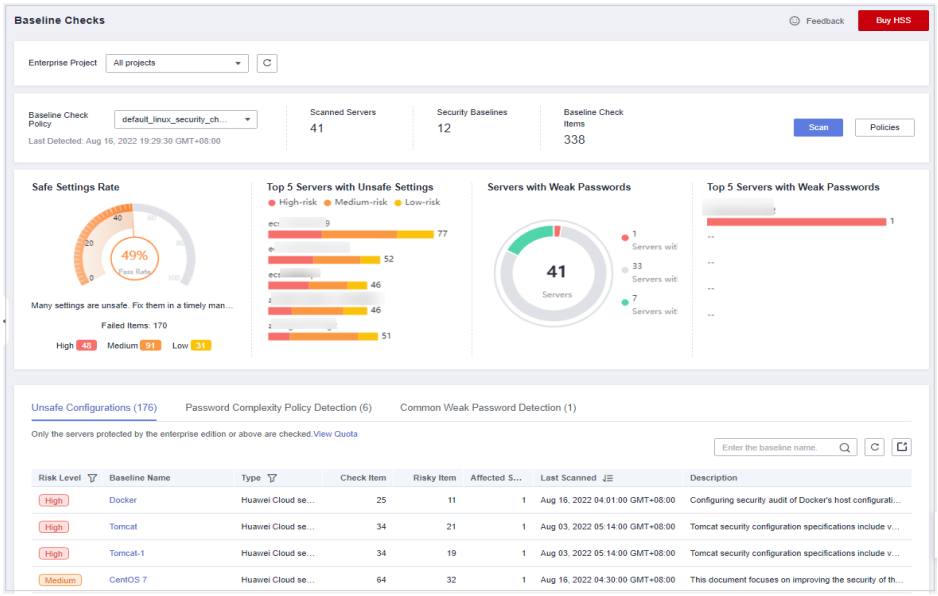


Tabla 4-4 Descripción general de la comprobación de línea de base

Parámetro	Descripción
Baseline Check Policy	Políticas de comprobación de línea de base disponibles que se han agregado. Puede seleccionar, crear, editar y eliminar estas políticas.
Scanned Servers	Número total de servidores detectados.
Security Baselines	Número de líneas de base ejecutadas durante la detección del servidor.
Baseline Check Items	Número total de elementos de configuración del servidor comprobados.
Safe Settings Rate	Porcentaje de elementos de configuración que pasaron la inspección de línea de base al número total de elementos de comprobación y al número total de elementos fallidos de diferentes niveles de riesgo.
Top 5 Servers with Unsafe Settings	Estadísticas sobre servidores con riesgos de configuración de servidores. Los 5 mejores servidores con los mayores riesgos se clasifican preferentemente. Si no existe una configuración de alto riesgo, los servidores se clasifican en los de riesgo medio y bajo en secuencia.

Parámetro	Descripción
Servers with Weak Passwords	Número total de servidores detectados, así como el número de servidores con contraseñas débiles, aquellos sin contraseñas débiles, y aquellos con detección de contraseñas débiles desactivados.
Top 5 Servers with Weak Passwords	Estadísticas sobre los 5 mejores servidores con los riesgos de contraseña más débiles.
Unsafe Configurations	Generación de alarmas para todos los servidores con riesgos de configuración y estadísticas de riesgos.
Password Complexity Policy Detection	Estadísticas sobre servidores con contraseñas débiles que no cumplen con los requisitos de línea de base.
Common Weak Password Detection	Estadísticas sobre servidores con contraseñas débiles y cuentas involucradas.

----Fin

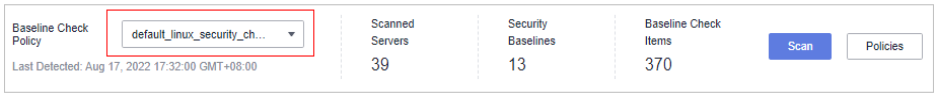
Realización de Comprobación de Línea de Base Manualmente

AVISO

- La comprobación manual se centra en los servidores asociados a la política de línea base de destino. Si se utiliza la política predeterminada, **asocie el servidor** y a continuación realice la comprobación manual.
- Antes de realizar la comprobación manual, compruebe si se puede seleccionar la política de destino en la lista desplegable **Baseline Check Policy**. Si necesita crear una política, consulte **Creación de una política de comprobación de línea de base**.

Paso 1 Seleccione **Prediction** > **Baseline Checks**, y seleccione la política de comprobación de línea base de destino.

Figura 4-4 Selección de la política de línea de base de destino



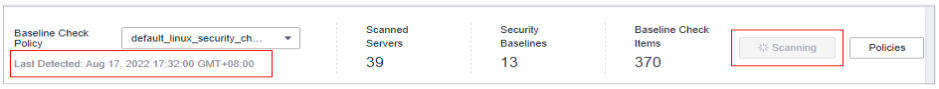
Paso 2 Haga clic en **Scan** en la esquina superior derecha de la página para realizar la comprobación manual.

Paso 3 Si la hora que se muestra en el área **Last Detected** bajo la **Baseline Check Policy** es la hora de comprobación real, la comprobación se ha completado.

NOTA

- Después de realizar una comprobación manual, el estado del botón cambia a **Scanning**. Si el tiempo de comprobación supera los 30 minutos, el botón estará disponible automáticamente. Espere a que se complete la comprobación hasta que la hora mostrada en el área **Last Detected** se convierta en la hora de comprobación actual.
- Una vez completada la comprobación, puede ver los resultados de la comprobación y las sugerencias de manejo consultando **Consulta de Detalles de Comprobación de Líneas de Bse**.

Figura 4-5 Comprobación del estado de comprobación



----Fin

Exportación del informe de comprobación de línea de base

Puede filtrar y exportar el informe de comprobación de línea de base según sea necesario.

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

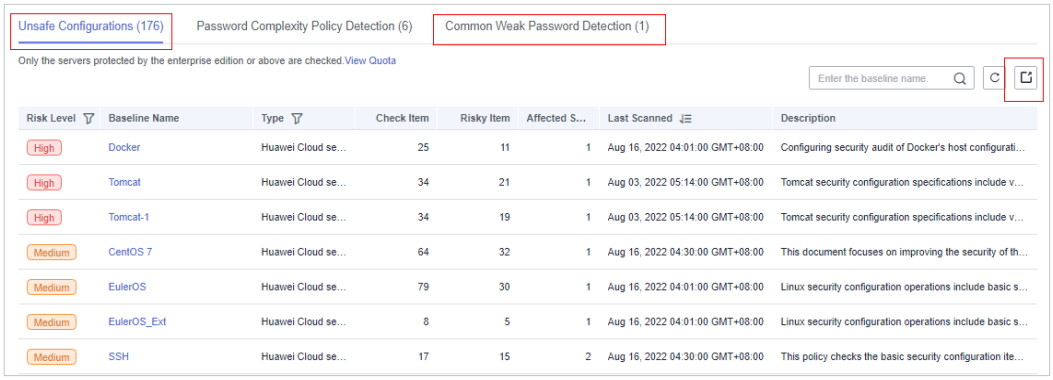
Paso 3 En el panel de navegación de la izquierda, seleccione **Prediction** > **Baseline Checks**.

Paso 4 Haga clic en diferentes pestañas de la página mostrada para comprobar los riesgos detectados.

NOTA

Actualmente, solo se pueden exportar los informes en las páginas **Unsafe Configurations** y **Common Weak Password Detection**.

Figura 4-6 Ver la lista de riesgos



Paso 5 Haga clic en la pestaña **Unsafe Configurations** o **Common Weak Password Detection** y haga clic en la esquina superior derecha de la lista para descargar las alarmas de riesgo filtradas.

NOTA

En la página **Unsafe Configurations**, puede hacer clic en la imagen de la columna correspondiente para filtrar las alarmas según el nivel de riesgo y el tipo.

En la página **Common Weak Password Detection**, puede usar la lista desplegable de la derecha para filtrar y descargar las alarmas.

Se puede descargar un máximo de informes de verificación de riesgo 5,000 a la vez desde las páginas **Unsafe Configurations** y **Common Weak Password Detection**.

----Fin

4.2.2 Consulta de Detalles de Comprobación de Líneas de Bse

HSS comprueba su software en busca de políticas débiles de complejidad de contraseñas y otras configuraciones inseguras, y proporciona sugerencias para solucionar los riesgos detectados. Para obtener más información sobre la comprobación de línea de base, consulte **Inspección de línea de base**.

Prerrequisitos

Sólo se comprueban los servidores protegidos por la edición empresarial o superior.

Elementos de comprobación

Tabla 4-5 Elementos de comprobación

Elementos	Descripción
Unsafe configurations	Actualmente, se admiten los siguientes estándares y tipos de comprobación: ● Para Linux OSs: – La línea de base de la práctica de seguridad de Huawei Cloud puede comprobar Apache2, Docker, MongoDB, Redis, MySQL5, Nginx, Tomcat, SSH, vsftp, CentOS7, EulerOS y EulerOS_ext. – La línea de base de cumplimiento de DJCP MLPS puede comprobar Apache2, MongoDB, MySQL5, Nginx, Tomcat, CentOS6, CentOS7, CentOS8, Debian9, Debian10, Debian11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu 12, Ubuntu 14, Ubuntu 16 y Ubuntu 18. ● Para los sistemas operativos Windows: – La línea de base de la práctica de seguridad de Huawei Cloud puede comprobar MongoDB, Apache2, MySQL, Nginx, Redis, Tomcat, Windows_2008 y Windows_2012.
Password complexity policies	Políticas de complejidad de contraseñas en cuentas del sistema.

Elementos	Descripción
Common weak passwords	Contraseñas débiles definidas en la biblioteca de contraseñas débiles comunes. Contraseñas débiles comunes de MySQL, FTP y cuentas del sistema.

Consulta de configuraciones inseguras

Vea las estadísticas de riesgos de configuraciones inseguras y las sugerencias de manejo correspondientes.

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, seleccione **Prediction** > **Baseline Checks**.

Paso 4 Haga clic en la pestaña **Unsafe Configurations** para ver los elementos de riesgo. **Tabla 4-6** enumera los parámetros correspondientes.

Figura 4-7 Consulta de detalles de configuración inseguros

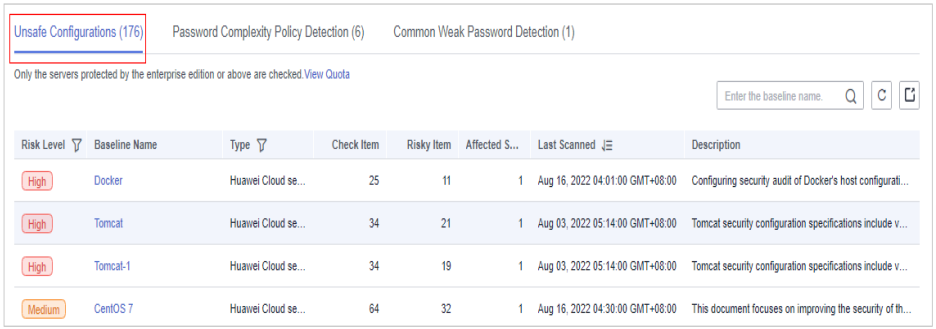


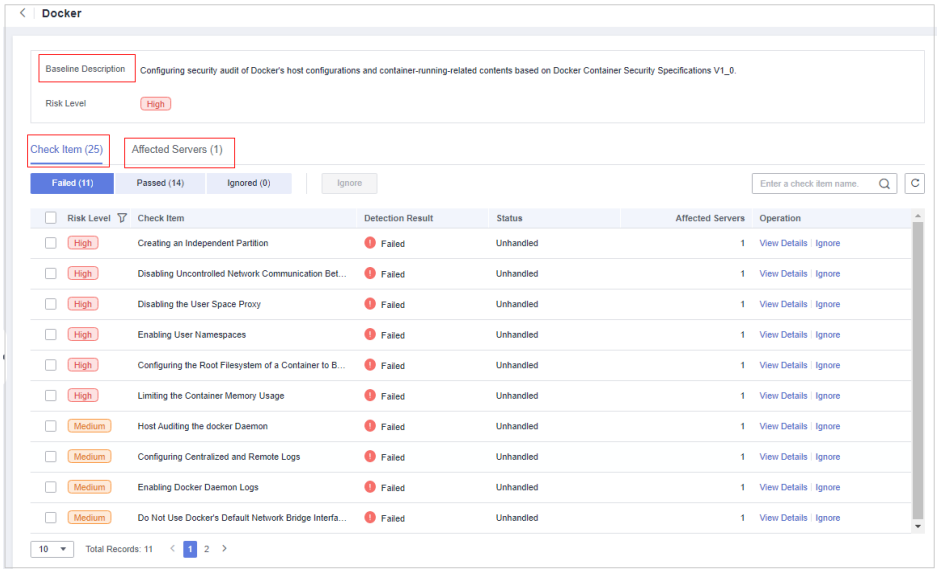
Tabla 4-6 Descripción del parámetro

Parámetro	Descripción
Risk Level	Nivel del resultado de detección basado en el estándar de referencia. ● High ● Low ● Medium ● Safe
Baseline Name	Nombre de la línea de base que se comprueba.
Type	Tipo de política de la línea de base que se ha comprobado. ● Prácticas de seguridad de Huawei Cloud ● DJCP MLPS

Parámetro	Descripción
Item	Número total de elementos de configuración que se comprueban.
Risky Item	Número total de configuraciones arriesgadas.
Affected Servers	Número total de servidores afectados por la línea de base arriesgada de destino.
Description	Descripción de la línea de base de riesgo objetivo.

Paso 5 Haga clic en el nombre de la línea base de destino en la lista para ver la descripción de la línea base, los servidores afectados y los detalles sobre todos los elementos de comprobación.

Figura 4-8 Consulta de la lista de elementos de comprobación de configuración



Paso 6 Haga clic en **View Details** en la columna **Operation** del elemento de comprobación de destino para ver la descripción y las sugerencias de manejo.

Es necesario comprobar si un elemento de riesgo es crítico o necesita ser manejado.

En caso afirmativo, modifique el elemento de comprobación de acuerdo con las sugerencias de manipulación. Si no, haga clic en **Ignore** en la columna **Operation** del elemento de comprobación de la lista a la que ha accedido en el **paso 8** para ignorarlo.

Figura 4-9 Consulta de los detalles del artículo de comprobación

----Fin

Consulta de la Detección de políticas de complejidad de contraseñas

Vea las estadísticas de riesgos y las sugerencias de gestión de la detección de políticas de complejidad de contraseñas.

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, seleccione **Prediction** > **Baseline Checks**.

Paso 4 Haga clic en la pestaña **Password Complexity Policy Detection** para ver los elementos estadísticos de riesgo y las sugerencias de gestión. **Tabla 4-7** enumera los parámetros correspondientes.

Figura 4-10 Consulta de los detalles de detección de políticas de complejidad de contraseñas

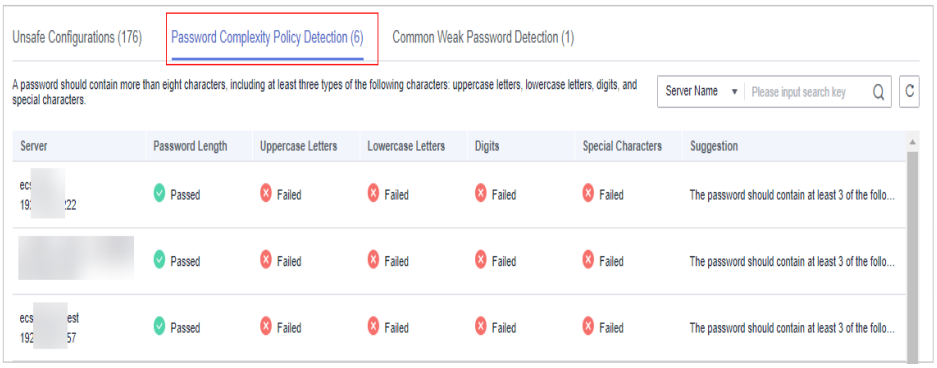


Tabla 4-7 Descripción del parámetro

Parámetro	Descripción
Server	Nombre y dirección IP del servidor detectado.
Password Length	Si la longitud de la contraseña del servidor de destino cumple con los requisitos. ● Passed ● Failed
Uppercase Letters	Si las letras mayúsculas utilizadas en la contraseña del servidor de destino cumplen los requisitos. ● Passed ● Failed
Lowercase Letters	Si las letras minúsculas utilizadas en la contraseña del servidor de destino cumplen los requisitos. ● Passed ● Failed
Digits	Si los dígitos utilizados en la contraseña del servidor de destino cumplen los requisitos. ● Passed ● Failed
Special characters	Si los caracteres especiales utilizados en la contraseña del servidor de destino cumplen los requisitos. ● Passed ● Failed
Suggestion	Sugerencia de manejo para la contraseña de riesgo detectada del servidor de destino.

----Fin

Visualización de la detección común de contraseñas poco seguras

Vea las estadísticas de riesgo de detección de contraseñas débiles y las sugerencias de manejo correspondientes.

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, seleccione **Prediction** > **Baseline Checks**.

Paso 4 Haga clic en la pestaña **Common Weak Password Detection** para ver las estadísticas de las cuentas de contraseñas débiles de riesgo en el servidor. **Tabla 4-8** enumera los parámetros correspondientes.

Figura 4-11 Consulta de la detección de contraseña débil común

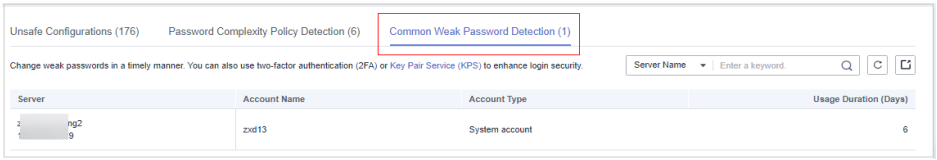


Tabla 4-8 Descripción del parámetro

Parámetro	Descripción
Server	Nombre y dirección IP del servidor detectado.
Account Name	Cuentas con contraseñas débiles que se detectan en el servidor de destino.
Account Type	Tipo de cuenta.
Usage Duration (Days)	Período para usar una contraseña poco segura.

NOTA

- Para mejorar la seguridad del servidor, se recomienda mejorar las contraseñas de las cuentas utilizadas para iniciar sesión en los servidores, como las cuentas SSH.
- Para proteger los datos internos de sus servidores, se recomienda mejorar las contraseñas de las cuentas de software, como las cuentas MySQL y las cuentas FTP.

Después de modificar las contraseñas débiles, se recomienda realizar una detección manual de inmediato para verificar el resultado. Si no realiza la verificación manual, HSS comprobará automáticamente la configuración al día siguiente por la mañana temprano.

- Una contraseña debe contener más de ocho caracteres, incluyendo al menos tres tipos de los siguientes caracteres: letras mayúsculas, letras minúsculas, dígitos y caracteres especiales.

----Fin

4.2.3 Sugerencias sobre la fijación de ajustes inseguros

En este tema se proporcionan sugerencias sobre cómo corregir la configuración insegura encontrada por HSS.

Cambio de la Política de Complejidad de Contraseñas

- Para supervisar la política de complejidad de contraseñas en un servidor Linux, instale los módulos de autenticación conectables (PAM) en el servidor. Para obtener más información, consulte **¿Cómo instalo un PAM en un sistema operativo Linux?**
- Para obtener más información sobre cómo modificar la política de complejidad de contraseñas en un servidor Linux, consulte **¿Cómo instalo un PAM y establezca una política de complejidad de contraseñas adecuada en un sistema operativo Linux?**
- Para obtener más información acerca de cómo modificar la política de complejidad de contraseñas en un servidor Windows, consulte **¿Cómo configuro una política de complejidad de contraseñas seguras en un sistema operativo Windows?**

Después de modificar la política de complejidad de contraseñas, se recomienda realizar una detección manual en la parte superior de la página **Baseline Checks** para verificar el

resultado. Si no realiza la verificación manual, HSS comprobará automáticamente la configuración al día siguiente por la mañana temprano.

Cambio de contraseñas débiles

- Para mejorar la seguridad del servidor, se recomienda modificar las cuentas con contraseñas débiles para iniciar sesión en el sistema de manera oportuna, como las cuentas SSH.
- Para proteger los datos internos de su servidor, se recomienda modificar las cuentas de software que utilizan contraseñas débiles, como las cuentas MySQL y las cuentas FTP.

Después de modificar las contraseñas débiles, se recomienda realizar una detección manual de inmediato para verificar el resultado. Si no realiza la verificación manual, HSS comprobará automáticamente la configuración al día siguiente por la mañana temprano.

Manejo de la configuración insegura

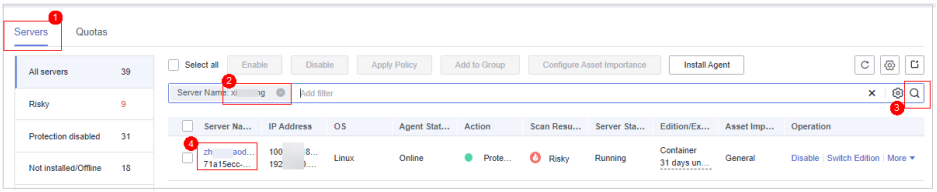
Las configuraciones inseguras de las aplicaciones clave probablemente serán explotadas por los piratas informáticos para entrometerse en los servidores. Tales configuraciones incluyen algoritmos de encriptación inseguros usados por SSH y Tomcat startup con permisos de root.

HSS puede detectar configuraciones inseguras y proporcionar sugerencias detalladas.

Paso 1 En la consola HSS, elija **Asset Management** > **Servers & Quota** y haga clic en la pestaña **Servers**.

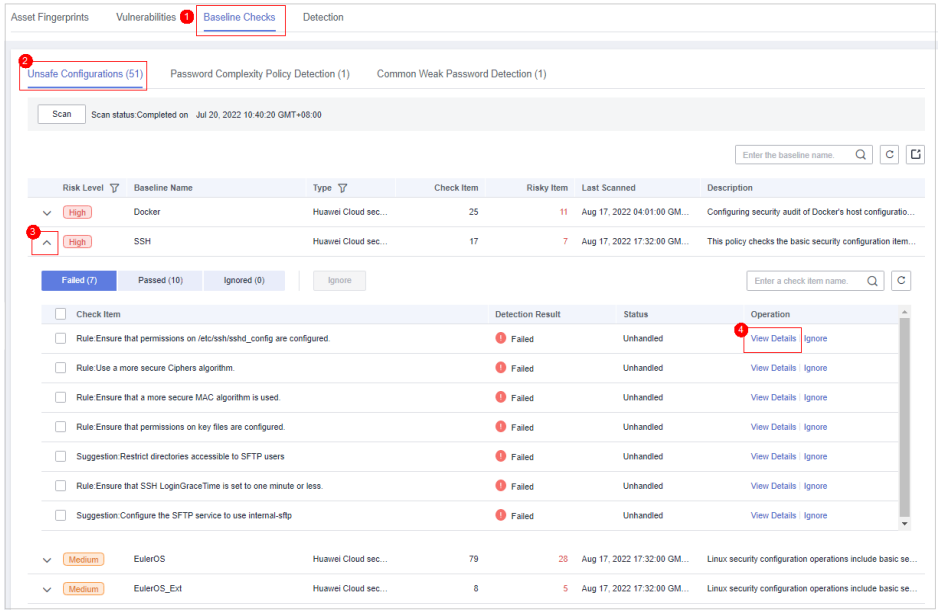
Paso 2 Busque el servidor de destino y haga clic en el nombre del servidor para ir a la página de detalles del servidor.

Figura 4-12 Localización del servidor de destino



Paso 3 Haga clic en **Baseline Checks** y haga clic en la pestaña **Unsafe Configurations**. Haga clic en el icono antes de un elemento de riesgo para expandir y ver todos los detalles del elemento de comprobación.

Figura 4-13 Consulta de los detalles del artículo de comprobación



Paso 4 Manejar elementos de riesgo.

- Ignorar riesgos

  Haga clic en **Ignore** en la columna **Operation** del elemento de comprobación de destino para omitir un único elemento de comprobación.

  Seleccione varios elementos de comprobación y haga clic en **Ignore** para ignorarlos por lotes.

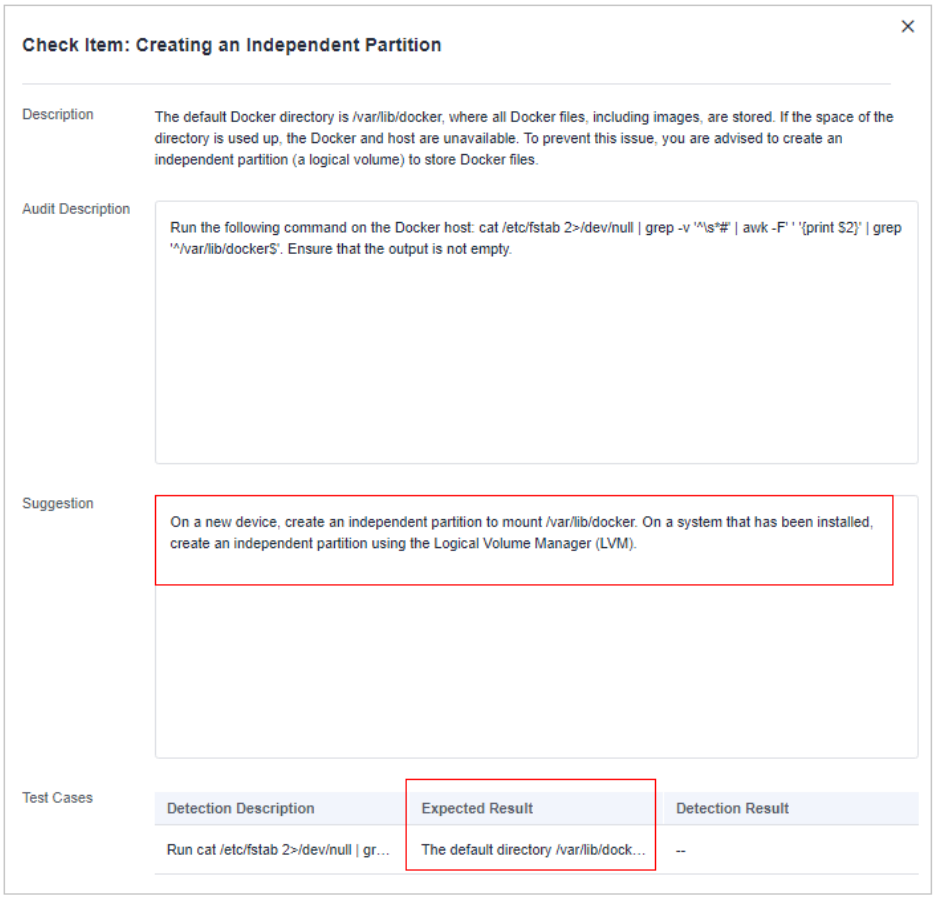
- Fijación de riesgos

  a. Haga clic en **View Details** en la columna **Operation** del elemento de riesgo de destino para ver los detalles del elemento de comprobación.

  b. Vea la descripción de la auditoría y las sugerencias, y maneje los riesgos basándose en las sugerencias o los resultados esperados de la información del caso de prueba.

  > NOTA
  >
  > Solucione inmediatamente la configuración con alta severidad y repare las de mediana o baja severidad según los requisitos de servicio.

Figura 4-14 Consulta de las sugerencias de manejo



----Fin

4.2.4 Gestión de políticas de comprobación de línea de base

Puede crear, editar y eliminar directivas de comprobación para comprobaciones de línea base manuales y personalizar el elemento de comprobación según sea necesario.

Restricciones

Las políticas de la página **Prediction** > **Baseline Checks** sólo tienen efecto en las comprobaciones de línea de base manuales. Para obtener más información sobre cómo configurar las directivas, consulte "Comprobación de configuración" y "Análisis de contraseña débil" en **Modificación de una política**.

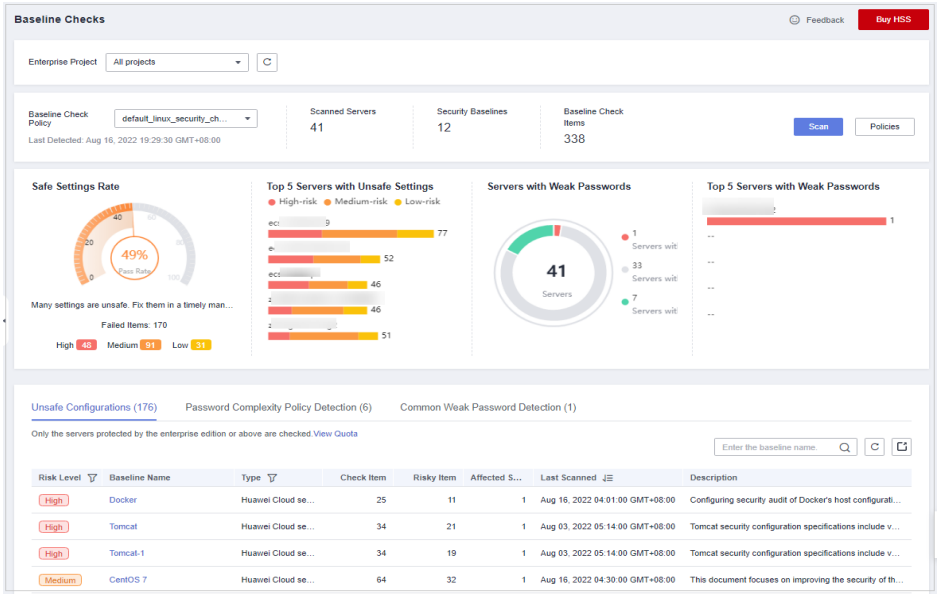
Creación de una política de comprobación de línea de base

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

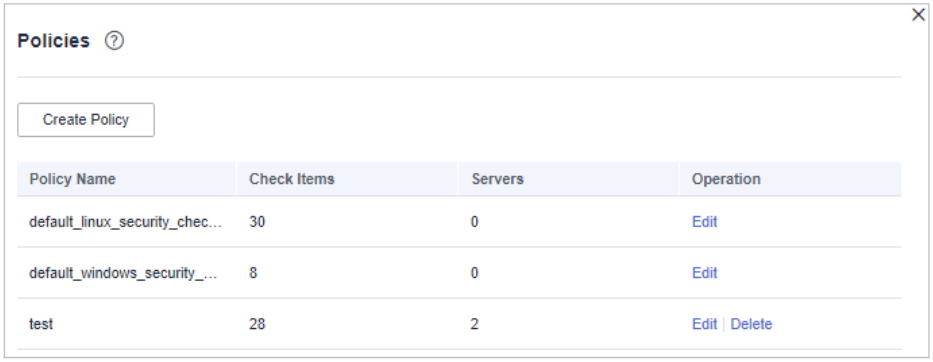
Paso 3 En el panel de navegación de la izquierda, seleccione **Prediction** > **Baseline Checks**.

Figura 4-15 Descripción general de la comprobación de línea de base



Paso 4 Haga clic en **Policies** en la esquina superior derecha de la página.

Figura 4-16 Políticas



Paso 5 Haga clic en **Create Policy** y configure la información de política. Para obtener más información, consulte **Tabla 4-9**.

Figura 4-17 Creación de una política

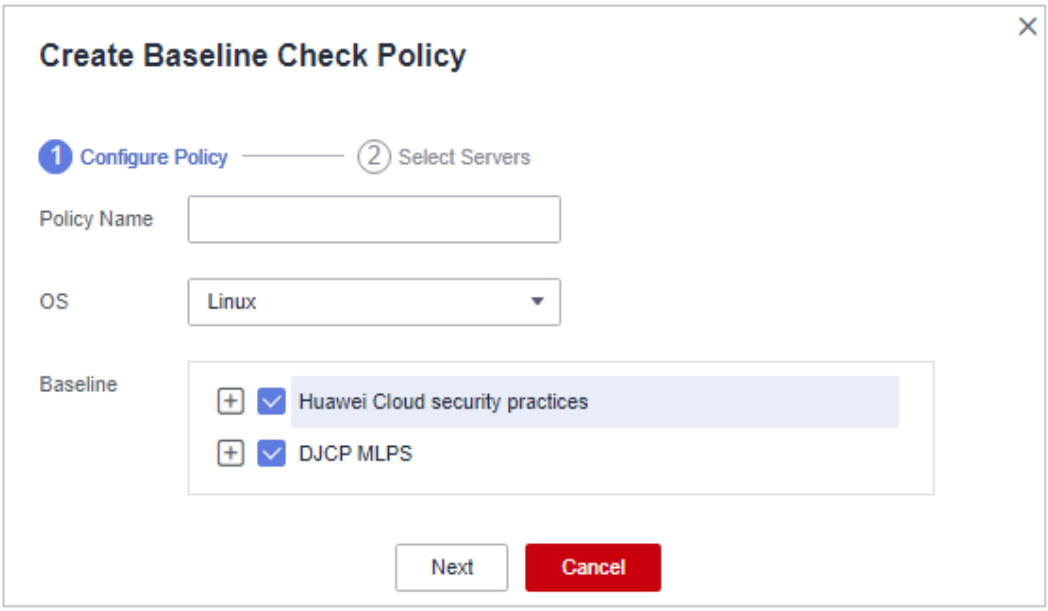


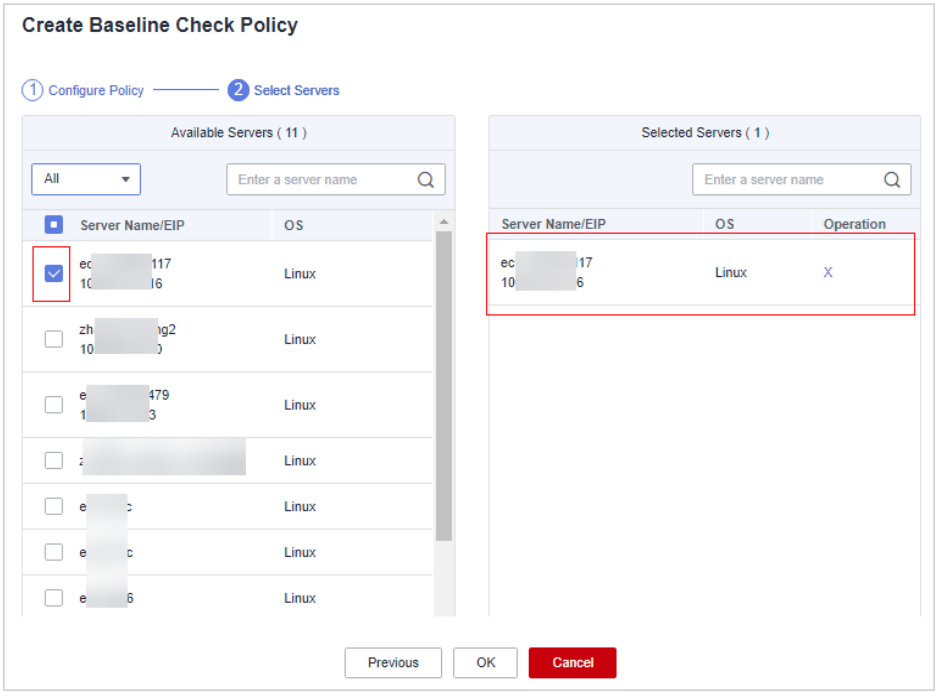
Tabla 4-9 Parámetros de política de línea de base

Parámetro	Descripción	Valor de ejemplo
Policy Name	Nombre de la política	linux_web1_security_policy
OS	Sistema operativo que se comprobará ● Linux ● Windows	Linux

Parámetro	Descripción	Valor de ejemplo
Baseline	Línea base utilizada para una comprobación. Compruebe los elementos de la siguiente manera: ● Para Linux, – La línea de base de la práctica de seguridad de Huawei Cloud puede comprobar Apache2, Docker, MongoDB, Redis, MySQL5, Nginx, Tomcat, SSH, vsftp, CentOS7, EulerOS y EulerOS_ext. – La línea de base de cumplimiento de DJCP MLPS puede comprobar Apache2, MongoDB, MySQL5, Nginx, Tomcat, CentOS6, CentOS7, CentOS8, Debian9, Debian10, Debian11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu 12, Ubuntu 14, Ubuntu 16 y Ubuntu 18. ● Para Windows, – La línea de base de la práctica de seguridad de Huawei Cloud puede comprobar MongoDB, Apache2, MySQL, Nginx, Redis, Tomcat, Windows_2008 y Windows_2012.	**Huawei Cloud security practices**: Select all. **DJCP MLPS**: Select all.

Paso 6 Confirme la configuración, haga clic en **Next** y seleccione servidores.

Figura 4-18 Selección de servidores



Paso 7 Confirme la información y haga clic en **OK**. La política de línea de base se mostrará en la lista de políticas.

----Fin

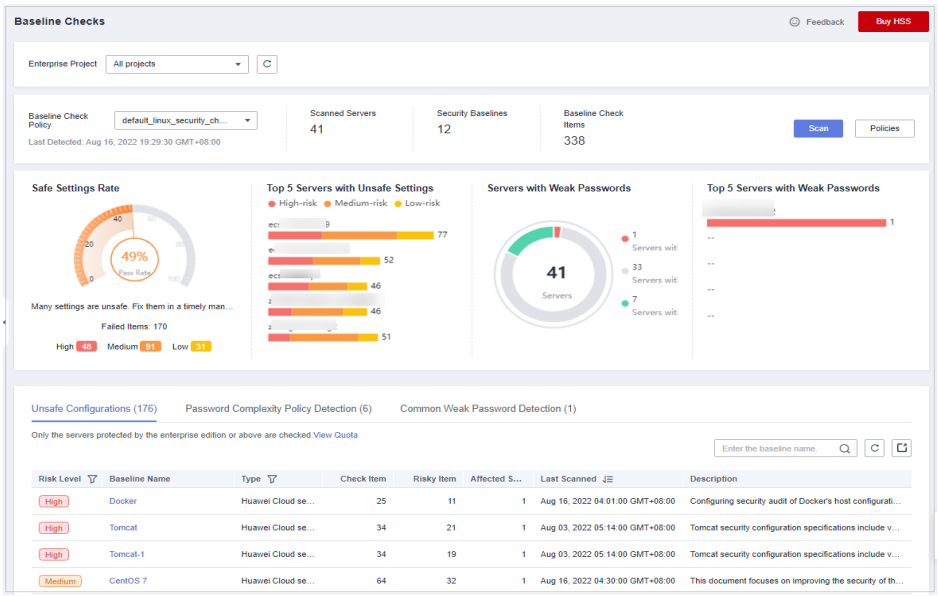
Edición de una política de comprobación de línea de base

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

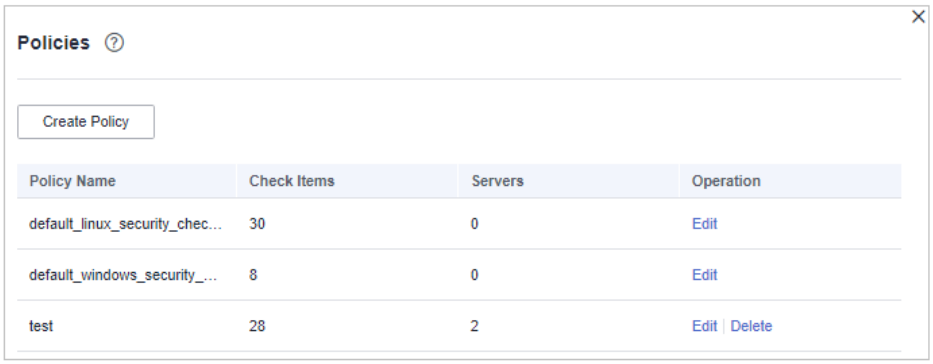
Paso 3 En el panel de navegación de la izquierda, seleccione **Prediction** > **Baseline Checks**.

Figura 4-19 Descripción general de la comprobación de línea de base



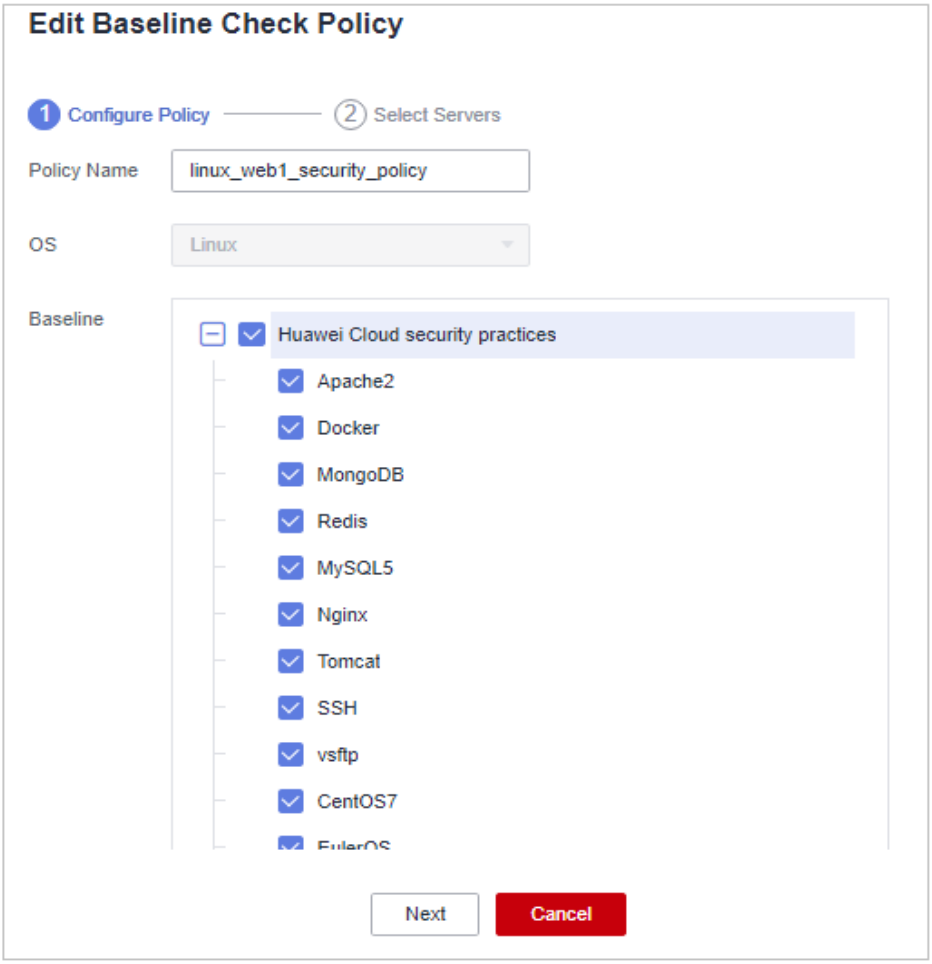
Paso 4 Haga clic en **Policies** en la esquina superior derecha de la página.

Figura 4-20 Políticas



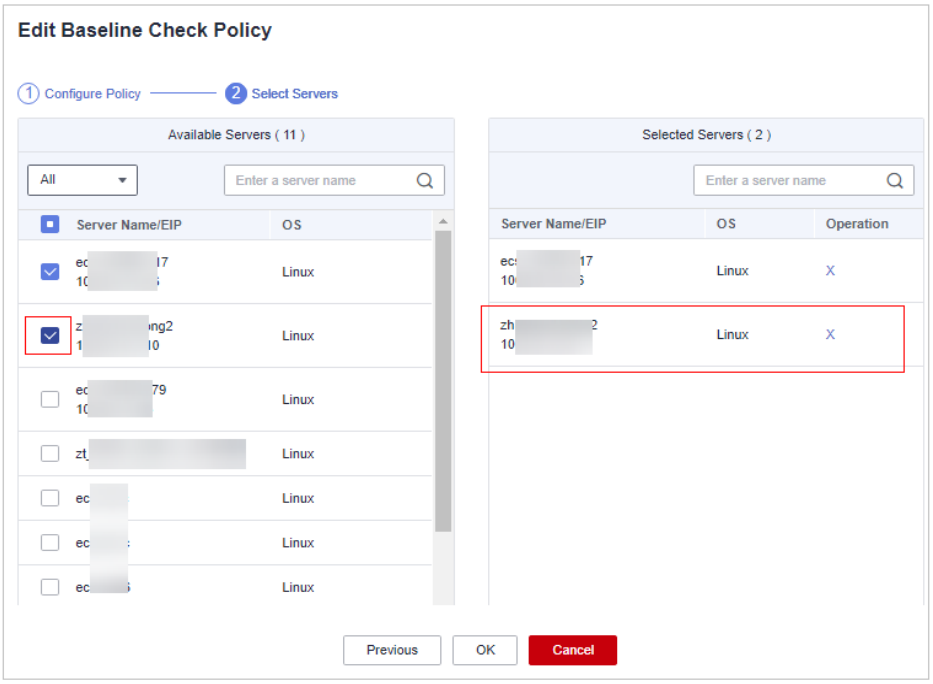
Paso 5 Haga clic en **Edit** en la columna **Operation** de una política. En la página de detalles de política que se muestra, configure el nombre de política y los elementos de comprobación.

Figura 4-21 Edición de una política



Paso 6 Confirme la configuración, haga clic en **Next** y seleccione servidores.

Figura 4-22 Selección de servidores



Paso 7 Confirme la información y haga clic en **OK**. Puede ver la política actualizada en la lista de políticas.

----Fin

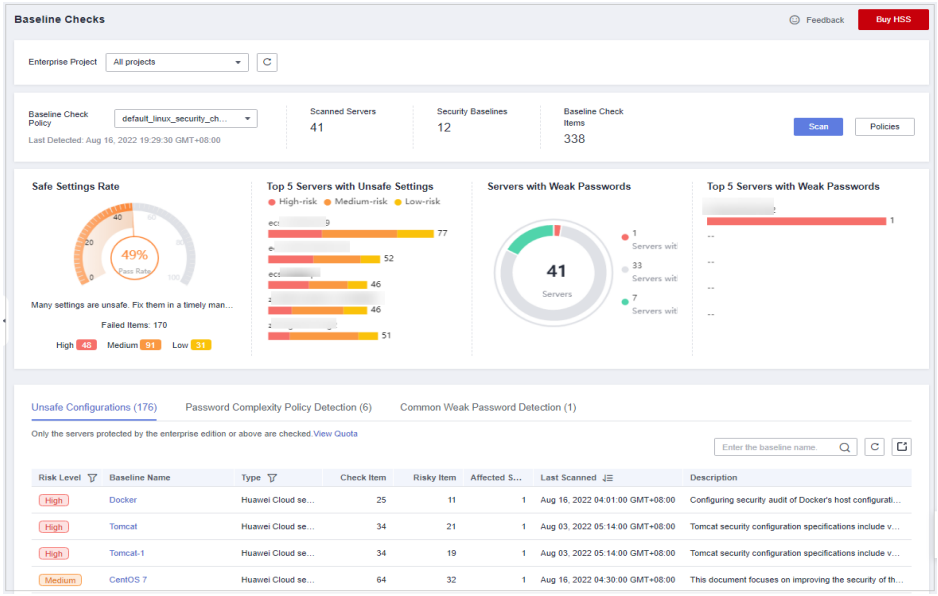
Supresión de una política de comprobación de línea de base

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

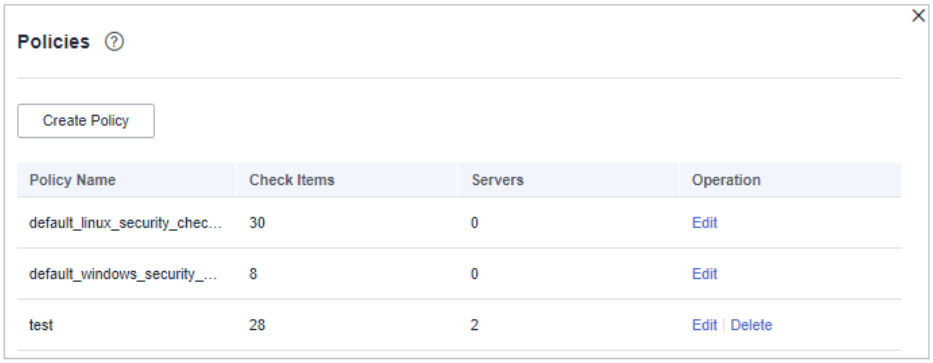
Paso 3 En el panel de navegación de la izquierda, seleccione **Prediction** > **Baseline Checks**.

Figura 4-23 Descripción general de la comprobación de línea de base



Paso 4 Haga clic en **Policies** en la esquina superior derecha de la página.

Figura 4-24 Políticas



Paso 5 Haga clic en **Delete** en la columna **Operation** de una política. En el cuadro de diálogo que se muestra, confirme la información y haga clic en **OK**.

----Fin

4.3 Comprobación de la seguridad de la imagen del contenedor

4.3.1 Vulnerabilidades de la imagen del contenedor

Esta sección describe cómo comprobar las vulnerabilidades en la imagen local y determinar si ignorar las vulnerabilidades.

Método de detección

Después de habilitar la protección de clústeres, los clústeres se analizan automáticamente.

Prerrequisitos

Se ha habilitado la función de protección de clústeres.

Consulta de vulnerabilidades en imágenes locales

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, seleccione **Prediction** > **Container Images**. En la página mostrada, haga clic en **Image Vulnerabilities** y haga clic en **Local Image Vulnerabilities** para ver las vulnerabilidades de imagen local.

Tabla 4-10 Descripción del parámetro

Parámetro	Descripción	Operación
Vulnerability Name	-	• Haga clic en para ver los detalles de una vulnerabilidad, incluidos **CVE ID**, **CVSS Score**, **Disclosed**, y **Vulnerability Details**. • Haga clic en el nombre de una vulnerabilidad para ver las imágenes afectadas por la vulnerabilidad. Para obtener más información, consulte **paso 6**.
Repair Urgency	Muestra si la vulnerabilidad debe repararse inmediatamente.	-
Unprocessed Images	Muestra el número de imágenes donde se detecta la vulnerabilidad pero aún no se ha corregido.	-
Historically Affected Images	Muestra el número de imágenes afectadas.	-
Solution	Proporciona una solución para corregir la vulnerabilidad.	Haga clic en el vínculo de la columna **Solution** para ver la solución.

Paso 4 Haga clic en un nombre de vulnerabilidad para ver la información básica sobre las imágenes afectadas.

----Fin

Consulta de vulnerabilidades en imágenes privadas

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, seleccione **Prediction** > **Container Images**. En la página mostrada, haga clic en **Image Vulnerabilities** y haga clic en **Private Image Vulnerabilities** para ver las vulnerabilidades de imagen privada.

NOTA

Haga clic en una imagen de riesgo para ver su descripción general de vulnerabilidades, incluyendo el nombre de la vulnerabilidad, urgencia, estado, información de software; y elija corregir o ignorar la vulnerabilidad.

Tabla 4-11 Descripción del parámetro

Parámetro	Descripción	Operación
Vulnerability Name	-	● Haga clic en para ver los detalles de una vulnerabilidad, incluidos **CVE ID**, **CVSS Score**, **Disclosed**, y **Vulnerability Details**. ● Haga clic en el nombre de una vulnerabilidad para ver las imágenes afectadas por la vulnerabilidad. Para más detalles, consulte **Paso 4**.
Repair Urgency	Muestra si la vulnerabilidad debe repararse inmediatamente.	-
Historically Affected Images	Muestra el número de imágenes afectadas.	-
Solution	Proporciona una solución para corregir la vulnerabilidad.	Haga clic en el vínculo de la columna **Solution** para ver la solución.

Paso 4 Haga clic en un nombre de vulnerabilidad para ver la información básica sobre las imágenes afectadas

----Fin

Ignorar vulnerabilidades en imágenes locales

Una vulnerabilidad sin riesgo o pequeños riesgos puede ser ignorada. Una vez que se ignora una vulnerabilidad, la vulnerabilidad no se cuenta para la imagen, pero sigue estando en la lista de vulnerabilidades.

Paso 1 Haga clic en **Image Vulnerabilities** y haga clic en **Local Image Vulnerabilities**.

Paso 2 Ignore el impacto de la vulnerabilidad en todas las imágenes o ignore el impacto de la vulnerabilidad en una imagen. Para más detalles, consulte **Tabla 4-12**.

Tabla 4-12 Operación

Operación	Procedimiento
Ignorar el impacto de una vulnerabilidad en todas las imágenes	1. En la lista de vulnerabilidades, seleccione una vulnerabilidad que desee **Ignore** y haga clic en Omitir en la esquina superior izquierda. 2. En el cuadro de diálogo que se muestra, haga clic en **OK** para omitir la vulnerabilidad seleccionada.
Ignorar el impacto de una vulnerabilidad en una imagen	● Método 1: 1. En la lista de vulnerabilidades, haga clic en el nombre de la vulnerabilidad de destino para comprobar las imágenes afectadas. En la columna **Operation** de la imagen, haga clic en **Ignore**. 2. En el cuadro de diálogo que se muestra, haga clic en **OK** para ignorar la vulnerabilidad. ● Método 2: 1. Haga clic en el nombre de la imagen para ver la vulnerabilidad y su estado de procesamiento. En la columna **Operation** de la vulnerabilidad, haga clic en **Ignore**. 2. En el cuadro de diálogo que se muestra, haga clic en **OK** para ignorar la vulnerabilidad.

----Fin

Cancelar omitir una vulnerabilidad

- Vaya a la lista de vulnerabilidades, seleccione la vulnerabilidad ignorada y haga clic en **Unignore** en la esquina superior izquierda de la lista de vulnerabilidades para cancelar la ignoración de una vulnerabilidad.
- Vaya a la lista de imágenes afectadas por la vulnerabilidad ignorada. En la columna **Operation** de la imagen, haga clic en **Unignore** para cancelar la omisión de una vulnerabilidad.
- Vaya a la lista de vulnerabilidades en la imagen. En la fila que contiene la vulnerabilidad ignorada, haga clic en **Unignore** en la columna **Operation** para cancelar la ignoración de una vulnerabilidad.

4.3.2 Consulta de resultados de detección de archivos maliciosos

Los archivos maliciosos en las imágenes privadas se pueden detectar automáticamente, lo que le ayuda a descubrir y eliminar las amenazas de seguridad en sus activos.

Frecuencia de comprobación

Todos los días se realiza una verificación completa de forma automática a primera hora de la mañana.

Prerrequisitos

Ha adquirido la edición empresarial. Los usuarios de la edición básica y bajo demanda no pueden usar la función de comprobación de configuraciones inseguras.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el árbol de navegación de la izquierda, elija **Prediction** > **Container Images**.

Paso 4 Haga clic en la pestaña **Malicious Files** para ver detalles sobre los archivos maliciosos en imágenes privadas, eliminar los archivos maliciosos o crear imágenes de nuevo según sea necesario según el resultado de la detección.

- Los archivos maliciosos incluyen caballos de Troya, gusanos, virus y Adware.
- En la columna **Image Tag**, haga clic en una versión de imagen para ver su informe de vulnerabilidad.

----Fin

4.3.3 Comprobación de línea base de imagen

Su repositorio de imágenes privadas se analiza en busca de configuraciones inseguras y proporciona sugerencias para modificar las configuraciones, lo que le ayuda a combatir las intrusiones y cumplir con los requisitos de cumplimiento.

Frecuencia de comprobación

El HSS realiza automáticamente una verificación completa a primera hora de la mañana todos los días.

Prerrequisitos

Usted ha comprado CGS. Los usuarios de la edición básica y bajo demanda no pueden utilizar la función de comprobación de configuración insegura.

Elementos de comprobación

- Cuentas con nombres o UID duplicados
- Cuentas no root cuyos UID son 0
- Contraseñas codificadas
- Cuentas con valores hash de contraseña duplicados
- Algoritmos de hash de contraseña débiles

- Cuentas con contraseñas en blanco
- Nombres de grupo o GID duplicados
- Cuenta no privilegiada incluida incorrectamente en el grupo de privilegios
- Old "+" entries en el /etc/passwd file
- Old "+" entries en el /etc/shadow file
- Old "+" entries en el /etc/group file
- Asegurar que todos los grupos del /etc/passwd file estén en el /etc/group file
- La configuración del período de validez de la contraseña
- Asegurarse de que las fechas de cambio de contraseña de todos los usuarios son fechas pasadas.
- Deshabilitación del establecimiento de relaciones de confianza de host
- Deshabilitación del establecimiento de relaciones de confianza preestablecidas a nivel de root
- Asegurarse de que el GID del grupo predeterminado de usuario **root** es **0**.
- Asegurarse de que el grupo de sombras esté vacío.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el árbol de navegación de la izquierda, elija **Prediction** > **Container Images**.

Paso 4 Haga clic en la pestaña **Unsafe Settings** para ver la configuración insegura en la imagen.

Paso 5 Haga clic  junto a un elemento de verificación para ver sus detalles y sugerencias, y modifique su configuración insegura en consecuencia.

----Fin

5 Prevención

5.1 Protección de aplicaciones

5.1.1 Consulta de la protección de aplicaciones

Para proteger sus aplicaciones con RASP, simplemente necesita agregar sondas a ellas, sin tener que modificar los archivos de aplicación.

Principios técnicos

Las sondeos (código de control y protección) se añaden a los puntos de control (funciones clave) de las aplicaciones a través de la inyección dinámica de código. Los sondeos identifican ataques basados en reglas predefinidas, datos que pasan a través de los puntos de control y contextos (lógica de aplicación, configuraciones, datos y flujos de eventos).

Prerrequisitos

Usted ha comprado la edición premium de HSS.

Restricciones

Actualmente, solo se admiten servidores Linux.

Hasta ahora, solo las aplicaciones Java pueden ser protegidas.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰ y elija **Security & Compliance** > **Host Security Service**.

Paso 3 Elija **Prevention** > **Application Protection**.

Paso 4 Haga clic en la pestaña **Protection Servers** y compruebe la lista de servidores. La tabla siguiente describe los parámetros.

Tabla 5-1 Descripción del parámetro

Parámetro	Descripción
Server Name/ID	Nombre e ID del servidor
IP Address	Dirección IP privada y dirección EIP del servidor
OS	Sistema operativo del servidor
Server Group	Grupo al que pertenece el servidor
Protection Status	Estado de protección de un servidor ● **Protected** ● **Unprotected**
Microservice Protection	Estado de protección de microservicios. Su valor puede ser: ● **Active** ● **Installing** ● **Configuration pending** ● **Installation failed**
RASP Protection.	Estado de protección RASP. Su valor puede ser: ● **Installing** ● **Configuration pending** ● **Installation failed**
Detected Attacks	Número de ataques detectados por RASP.

Paso 5 Haga clic en la pestaña **Events**. Comprueba las alarmas y los eventos. Para obtener más información, consulte **Tabla 5-2**.

Puede hacer clic en un nombre de alarma para ver la información de ataque (como la información de solicitud y la dirección IP de origen de ataque) e información ampliada (como reglas de detección y sondeos), y solucionar el problema en consecuencia.

Tabla 5-2 Parámetros del evento

Parámetro	Descripción
Severity	Gravedad de la alarma
Server Name	Servidor que activa una alarma
Alarm Name	Nombre de la alarma
Alarm Time	Hora en que se informa de una alarma
Attack Source IP Address	Dirección IP del servidor que activa la alarma
Attack Source URL	URL del servidor que activa la alarma

----Fin

5.1.2 Habilitación de la protección de aplicaciones

Prerrequisitos

Usted ha comprado la edición premium de HSS.

Restricciones

Actualmente, solo se admiten servidores Linux.

Hasta ahora, solo las aplicaciones Java pueden ser protegidas.

Procedimiento

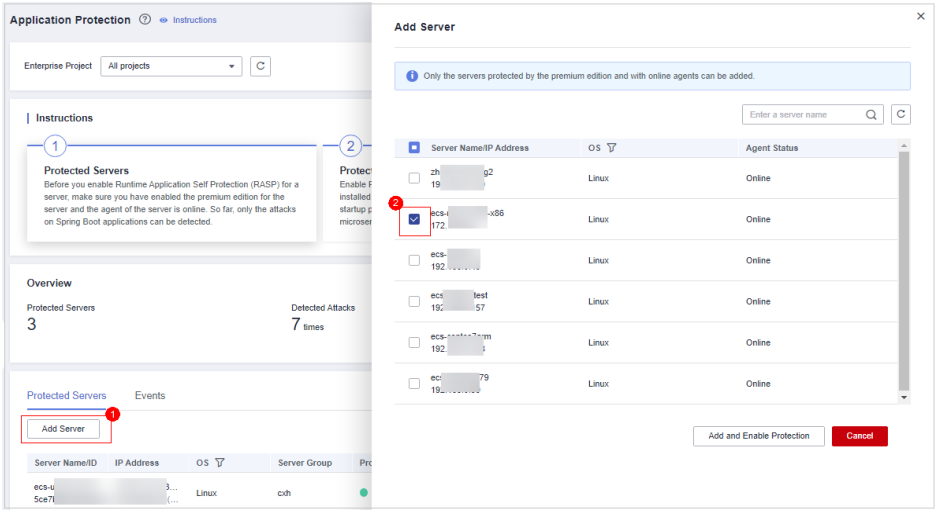
Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰ y elija **Security & Compliance** > **Host Security Service**.

Paso 3 Elija **Prevention** > **Application Protection**. Haga clic en la pestaña **Protected Servers**.

Paso 4 Haga clic en **Add Server**. Seleccione servidores en el cuadro de diálogo que se muestra.

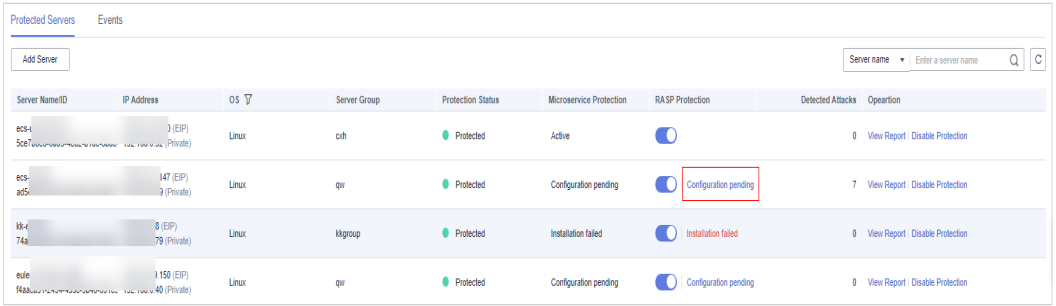
Figura 5-1 Selección de servidores



Paso 5 Haga clic en **Add and Enable Protection**.

Paso 6 En la pestaña **Protected Servers**, haga clic en el estado de la columna **RASP Protection**.

Figura 5-2 Ver el progreso de la protección habilitante

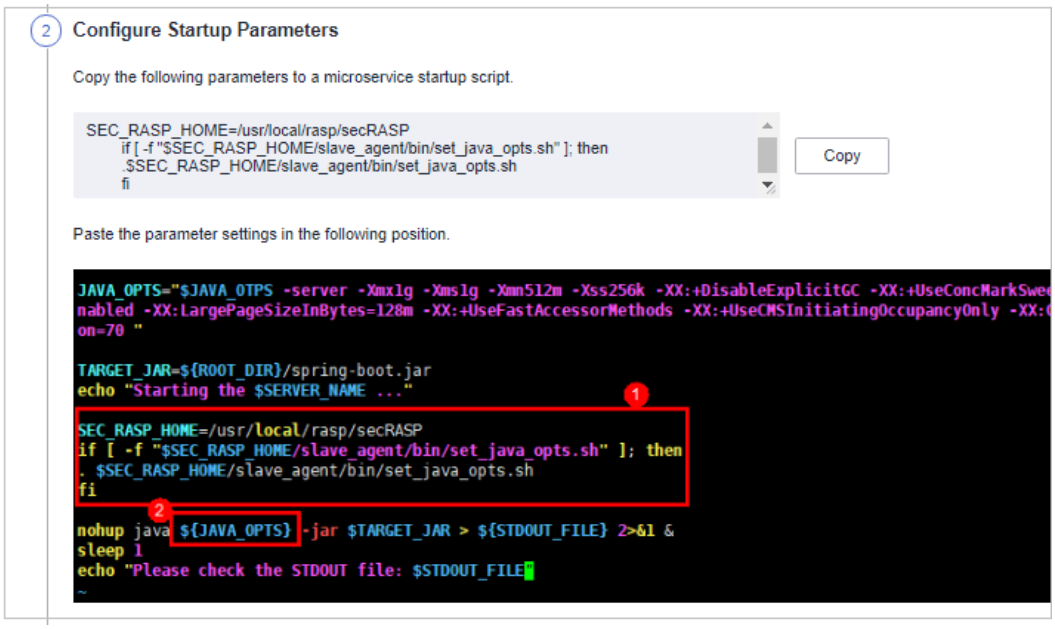


Paso 7 Compruebe el progreso de la instalación del software RASP. Espere hasta que aparezca el mensaje "Installation completed."

Figura 5-3 Instalación completada

Paso 8 Inicie sesión en el servidor, vaya a la ruta de inicio de Spring Boot y copie los parámetros del paso **Configure Startup Parameters** al cuadro de comando. Consulte **Figura 5-4**.

Figura 5-4 Configuración de parámetros de inicio



Paso 9 Reinicie el microservicio para aplicar la configuración de protección.

Paso 10 En la pestaña **Protected Servers**, compruebe el estado de protección en la columna **Microservice Protection**. Si el estado es **Active**, se ha habilitado la protección.

----Fin

5.1.3 Gestión de protección de aplicaciones

Prerrequisitos

Usted ha comprado la edición premium de HSS.

Restricciones

Actualmente, solo se admiten servidores Linux.

Hasta ahora, solo las aplicaciones Java pueden ser protegidas.

Ver el informe

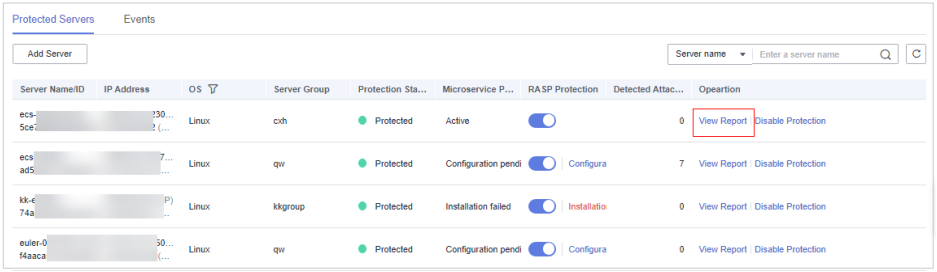
Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰ y elija **Security & Compliance** > **Host Security Service**.

Paso 3 Elija **Prevention** > **Application Protection**. Haga clic en la pestaña **Protected Servers**.

Paso 4 Haga clic en **View Report** en la columna **Operation** de un servidor para ver los detalles de detección.

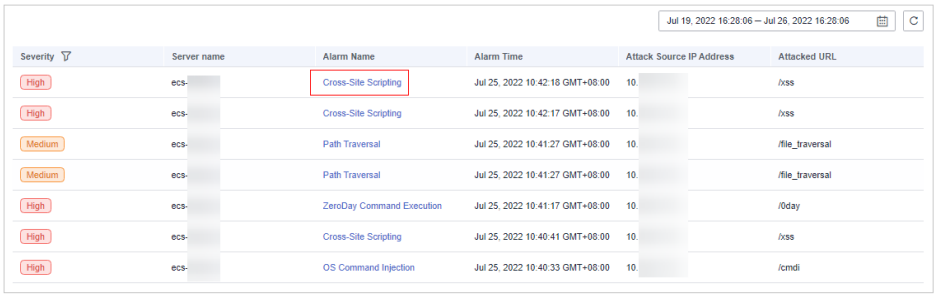
Figura 5-5 Consulta de un informe



Paso 5 Haga clic en un nombre de alarma para ver sus detalles.

Puede ver la información de ataque (como la información de solicitud y la dirección IP de origen de ataque) e información ampliada (como reglas de detección y sondeos), y solucionar el problema en consecuencia.

Figura 5-6 Ver detalles de alarma



----Fin

5.1.4 Deshabilitación de RASP para un microservicio

Prerrequisitos

Usted ha comprado la edición premium de HSS.

Restricciones

Actualmente, solo se admiten servidores Linux.

Hasta ahora, solo las aplicaciones Java pueden ser protegidas.

Procedimiento

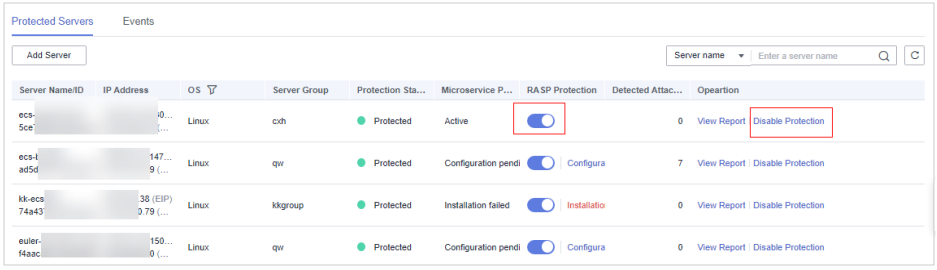
Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en y elija **Security & Compliance** > **Host Security Service**.

Paso 3 Elija **Prevention** > **Application Protection**. Haga clic en la pestaña **Protected Servers**.

Paso 4 Desactive el interruptor en la columna **RASP Protection** o haga clic en **Disable Protection** en la columna **Operation**.

Figura 5-7 Deshabilitación de protección



Paso 5 En el cuadro de diálogo que se muestra, confirme la información del servidor y haga clic en **OK**.

NOTA

Después de deshabilitar RASP par a un servidor, el servidor se eliminará de la pestaña **Protected Servers**. Para obtener más información sobre cómo habilitar la protección, consulte **Habilitación de la protección de aplicaciones**.

----Fin

5.2 WTP

5.2.1 Adición de un directorio protegido

WTP supervisa los directorios de sitios web en tiempo real, realiza copias de seguridad de archivos y restaura archivos manipulados mediante la copia de respaldo, protegiendo los sitios web de troyanos, enlaces ilegales y manipulaciones.

Restricciones y limitaciones

- WTP solo protege los archivos en los directorios protegidos que establezca. No protege los archivos especificados por los vínculos en los archivos protegidos.
- Asegúrese de que la ruta de copia de respaldo local es válida o que los directorios especificados no estén protegidos.
- La ruta de copia de respaldo local no puede superponer los directorios protegidos del servidor, o la copia de respaldo local fallará.

- El disco de la ruta de copia de respaldo local debe tener suficiente espacio, o no se puede evitar la manipulación.

Adición de un directorio protegido

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Elija Prevention > **Web Tamper Protection**, y haga clic en **Configure Protection**.

Paso 4 Haga clic en **Settings** en **Protected Directory Settings**.

Paso 5 Puede agregar un máximo de 50 directorios protegidos.

1. Haga clic en **Add**. En el cuadro de diálogo **Add Protected Directory**, establezca los parámetros necesarios. Para más detalles, consulte **Tabla 5-3**.

Tabla 5-3 Parámetros para un directorio protegido

Parámetro	Descripción	Restricción
Protected Directory	Los archivos y carpetas de este directorio son de sólo lectura.	No lo establezca en ningún directorio del sistema operativo.
Excluded Subdirectory	Subdirectorios que no necesitan estar protegidos en el directorio protegido, como los directorios de archivos temporales. Separar subdirectorios con punto y coma (;).	El subdirectorio es un directorio relativo en el directorio protegido.
Excluded File Types	Tipos de archivos que no necesitan estar protegidos en el directorio protegido, como los archivos de registro. Tipos de archivo separados con punto y coma (;). Para registrar el estado de ejecución del servidor en tiempo real, excluya los archivos de registro del directorio protegido. Puede conceder permisos de lectura y escritura altos para los archivos de registro para evitar que los atacantes vean o manipulen los archivos de registro.	-

Parámetro	Descripción	Restricción
Local Backup Path	Después de habilitar WTP, los archivos en el directorio protegido se copian automáticamente en la ruta de copia de respaldo local. Generalmente, la copia de respaldo se completa en 10 minutos. La duración real depende del tamaño de los archivos en el directorio protegido. La protección entra en vigor inmediatamente cuando se completa la copia de respaldo. No se realiza una copia de seguridad de los subdirectorios y tipos de archivos excluidos. Si WTP detecta que un archivo en un directorio protegido está manipulado, inmediatamente utiliza el archivo de copia de respaldo en el servidor local para restaurar el archivo.	La ruta de copia de respaldo local no puede superponerse con el directorio protegido añadido.

2. Haga clic en **OK**.

   Si necesita modificar archivos en el directorio protegido, detenga primero la protección para el directorio protegido. Después de modificar los archivos, reanudar la protección para el directorio de manera oportuna.

Paso 6 Habilitar la copia de respaldo remota.

De forma predeterminada, HSS realiza una copia de respaldo de los archivos de los directorios protegidos (excluyendo los subdirectorios y tipos de archivo especificados) en el directorio de copia de respaldo local especificado al agregar directorios protegidos. Para proteger los archivos de copia de respaldo locales contra manipulaciones, debe habilitar la función de copia de respaldo remota.

Para obtener más información sobre cómo agregar un servidor de copia de respaldo remoto, consulte **Gestión de servidores de copia de respaldo remota**.

1. En la página **Protected Directory Settings**, haga clic en **Enable Remote Backup**.
2. Seleccione un servidor de copia de respaldo en el cuadro de lista desplegable.
3. Haga clic en **OK**.

----Fin

Procedimiento posterior

- Suspender protección: Puede suspender WTP para un directorio si es necesario. Se recomienda que reanude WTP de manera oportuna para evitar que los archivos en el directorio sean manipulados.
- Editar un directorio protegido: puede modificar el directorio protegido añadido según sea necesario.

- Eliminar un directorio protegido: Puede eliminar los directorios que no necesitan ser protegidos.

AVISO

- Después de suspender la protección de un directorio protegido, eliminarlo o modificar su ruta, los archivos del directorio ya no estarán protegidos. Antes de realizar estas operaciones, asegúrese de haber tomado otras medidas para proteger los archivos.
- Después de suspender la protección de un directorio protegido, eliminarlo o modificar su ruta, si encuentra los archivos que faltan en el directorio, búsquelos en la ruta de copia de respaldo local o remota.

5.2.2 Gestión de servidores de copia de respaldo remota

De forma predeterminada, HSS realiza una copia de respaldo de los archivos de los directorios protegidos (excluyendo los subdirectorios y tipos de archivo especificados) en el directorio de copia de respaldo local especificado al agregar directorios protegidos. Para proteger los archivos de copia de respaldo locales contra manipulaciones, debe habilitar la función de copia de respaldo remota.

Si un directorio de archivos o un directorio de copia de respaldo del servidor local no es válido, puede utilizar el servicio de copia de respaldo remota para restaurar la página Web manipulada.

Prerrequisitos

Los siguientes servidores se pueden utilizar como servidores de copia de respaldo remota:

Huawei Cloud Servidores de Linux cuyo **Server Status** es **Running** y el **Agent Status** es **Online**

AVISO

- La función de copia de respaldo remota se puede utilizar cuando el servidor de copia de respaldo de Linux está conectado a su servidor en la nube. Para garantizar una copia de respaldo adecuada, se recomienda seleccionar un servidor de copia de respaldo en la misma intranet que su servidor en la nube.
- Se recomienda utilizar servidores de intranet menos expuestos a ataques como los servidores de copia de respaldo remotos.

Adición de un servidor de copia de respaldo remota

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Elija Prevention > **Web Tamper Protection**, y haga clic en **Configure Protection**.

Paso 4 Haga clic en **Settings** en **Protected Directory Settings**.

Paso 5 Haga clic en la pestaña correspondiente para gestionar un servidor de copia de respaldo remoto. Para más detalles, consulte **Tabla 5-4**.

Tabla 5-4 Descripción del parámetro

Parámetro	Descripción
Address	Esta dirección es la dirección de red privada del servidor Huawei Cloud.
Port	Asegúrese de que el puerto no esté bloqueado por ningún grupo de seguridad o firewall u ocupado.
Backup Path	Ruta de los archivos de copia de respaldo remota. ● Si se realiza una copia de respaldo de los directorios protegidos de varios servidores en el mismo servidor de copia de respaldo remoto, los datos se almacenarán en carpetas separadas con el nombre de ID de agente. Supongamos que los directorios protegidos de los dos servidores son//**hss01** y **hss02**, y los ID de agente de los dos servidores son **f1fdbabc-6cdc-43af-acab-e4e6f086625f** y **f2ddbabc-6cdc-43af-abcd-e4e6f086626f**, y la ruta de copia de respaldo remota es **/hss01**. Las rutas de copia de respaldo correspondientes son **/hss01/f1fdbabc-6cdc-43af-acab-e4e6f086625f** y **/hss01/f2ddbabc-6cdc-43af-abcd-e4e6f086626f**. ● Si WTP está habilitado para el servidor remoto de copia de respaldo, no establezca la ruta remota de copia de respaldo en ningún directorio protegido por WTP. De lo contrario, la copia de respaldo remota fallará.

Paso 6 Haga clic en **OK**.

----Fin

Habilitación de copia de respaldo remoto

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Elija Prevention > **Web Tamper Protection**, y haga clic en **Configure Protection**.

Paso 4 Haga clic en **Settings** en **Protected Directory Settings**.

Paso 5 Haga clic en **Enable Remote Backup** y seleccione un servidor de copia de respaldo remota.

Paso 6 Haga clic en OK para iniciar la copia de respaldo remota.

----Fin

Cambio de un servidor de copia de respaldo remota

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Elija Prevention > **Web Tamper Protection**, y haga clic en **Configure Protection**.

Paso 4 Haga clic en **Settings** en **Protected Directory Settings**.

Paso 5 Haga clic en la pestaña correspondiente para cambiar un servidor de copia de respaldo remoto. Puede seleccionar un servidor de copia de respaldo remoto de destino en la lista desplegable.

Paso 6 Haga clic en **OK**.

----Fin

Procedimiento posterior

Deshabilitación del copia de respaldo remoto

Tenga cuidado al realizar esta operación. Si la copia de respaldo remota está deshabilitada, HSS dejará de hacer copias de seguridad de los archivos de sus directorios protegidos.

5.2.3 Configuración de la protección WTP programada

Puede programar la protección WTP para permitir actualizaciones de sitios web en períodos específicos.

NOTA

Tenga cuidado al establecer los períodos para deshabilitar WTP, ya que los archivos no estarán protegidos en esos períodos.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Elija Prevention > **Web Tamper Protection**, y haga clic en **Configure Protection**.

Paso 4 Haga clic en la página **Configure Protection** y habilite la protección programada.

Paso 5 Haga clic en **OK**.

Paso 6 Haga clic en **Settings** y configure el período desprotegido y los días de una semana para desactivar automáticamente la protección.

Paso 7 Confirme la información y haga clic en **OK**.

----Fin

Reglas para establecer un período desprotegido

- Periodo desprotegido >= 5 minutos
- Periodo desprotegido < 24 horas
- Períodos (excepto los que comienzan a las 00:00 o terminan a las 23:59) no puede superponerse y debe tener un intervalo de al menos 5 minutos.
- Un período no puede durar dos días.
- La hora del servidor se utiliza como base de tiempo.

5.2.4 Habilitación de WTP dinámico

El WTP dinámico protege sus páginas web mientras se ejecutan las aplicaciones Tomcat y puede detectar manipulaciones de datos dinámicos, como los datos de bases de datos. Se puede habilitar con WTP estático o por separado.

Prerrequisitos

Está utilizando un servidor que ejecuta el sistema operativo Linux.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Elija Prevention > **Web Tamper Protection**, y haga clic en **Configure Protection**.

Paso 4 Haga clic en **Configure Protection** y haga clic en **Dynamic WTP** para habilitar WTP dinámico.

Paso 5 En el cuadro de diálogo que se muestra, modifique **Tomcat bin Directory**.

Es necesario modificar primero el directorio bin de Tomcat para habilitar el WTP dinámico. El sistema preestablece el script **setenv.sh** en el directorio bin para establecer los parámetros de inicio del programa antimanipulación. Después de habilitar el WTP dinámico, reinicie Tomcat para que esta configuración tenga efecto.

Paso 6 Haga clic en **OK** para activar WTP dinámico.

----Fin

5.2.5 Consulta de informes WTP

Una vez que WTP está habilitado, HSS comprobará exhaustivamente los directorios protegidos que usted especificó. Puede comprobar los registros de los ataques de manipulación detectados.

Prerrequisitos

- Se han obtenido las credenciales de inicio de sesión.
- El estado del **Agent Status** está **Online** y su **WTP Status** está **Enabled**.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Elija **Prevention** > **Web Tamper Protection**, y haga clic en **View Report**.

Paso 4 Vea los detalles en la página del informe.

----Fin

5.2.6 Consulta de eventos WTP

Una vez que WTP está habilitado, el servicio HSS comprobará exhaustivamente los directorios protegidos que usted especificó. Puede comprobar los registros sobre la manipulación detectada de los archivos de protección del host.

Prerrequisitos

- Ha obtenido una cuenta y su contraseña para iniciar sesión en la consola de gestión.
- El estado del **Agent Status** está **Online** y su **WTP Status** está **Enabled**.
- WTP estático está habilitado.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Seleccione **Prevention** > **Web Tamper Protection** y haga clic en **Events** para ver los registros de manipulación de los archivos de protección de host.

----Fin

5.3 Prevención de ransomware

5.3.1 Prevención del ransomware

Prerrequisitos

Ha adquirido Host Security Service edición premium o WTP.

Restricciones

Solo los hosts en la nube de Huawei admiten la protección contra ransomware.

Comprobación de la Descripción General sobre Prevención de Ransomware

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰ y elija **Security & Compliance** > **Host Security Service**.

Paso 3 En el panel de navegación, elija **Prevention** > **Ransomware Prevention**. Compruebe las estadísticas de protección, las estadísticas de copia de respaldo, la política de copia de respaldo, los servidores protegidos y los detalles de la política. **Tabla 5-5** describe los parámetros.

Tabla 5-5 Parámetros de prevención de ransomware

Parámetro		Descripción	Valor de ejemplo
Enterprise Project		-	-
Time range		Seleccione un intervalo de tiempo para comprobar las estadísticas de defensa del ransomware. Valores válidos: **Last 24 hours**, **Last 3 days**, **Last 7 days**, **Last 30 days**	Last 30 days
Protection Statistics	Protected Servers	Número de servidores bajo protección contra ransomware.	-
	Events	Número de eventos detectados por el ransomware dentro del intervalo de tiempo especificado.	-
Backup Statistics	Backed Up Servers	Número de servidores cuyos datos han sido respaldados.	-
	Backup and Restoration Tasks	Número de tareas de restauración de datos del servidor. Puede hacer clic en el número para ver el progreso de la tarea.	-
	Used/Total capacity	Capacidad ocupada por los datos de copia de respaldo y la capacidad total de copia de respaldo.	-
Backup Policies		Políticas de copia de respaldo y retención. Puede **modificar la política de copia de respaldo**.	-
Protected Servers	Server Name/ID	Nombre e ID del servidor. Puede hacer clic en un nombre de servidor para ver sus detalles.	-
	IP Address	EIP y dirección IP privada de un servidor.	-
	OS	Sistema operativo del servidor.	Linux

Parámetro		Descripción	Valor de ejemplo
	Server Status	Estado del servidor. ● Running ● Stopped	-
	Ransomware Protection Status	Estado de protección contra ransomware de un servidor. Su valor puede ser: ● **Enabling** ● **Enabled** ● **Disabling** ● **Disabled**	Enabled
	Policy	Política utilizada para el servidor.	-
	Events	Número de eventos detectados dentro del intervalo de tiempo seleccionado.	-
	Backup	Estado de la función de copia de respaldo. Su valor puede ser: ● **Enabled**: Se ha habilitado la copia de respaldo automática de datos para un servidor. ● **Disabled**: La copia de respaldo automática de datos completa está deshabilitada para un servidor.	Enabled
Policies	Policy	Nombre de la política.	-
	Action	Acción de una política. Su valor puede ser: ● **Report alarm**: Si se detecta un virus, se reportará una alarma. ● **Report alarm and isolate**: Si se detecta un virus, se informará de una alarma y se aislará el virus.	Report alarm and isolate
	Bait File	Archivos y directorios que almacenan datos no válidos en servidores y se utilizan como honeypots. Si la prevención de ransomware está habilitada, esta función está habilitada de forma predeterminada. Después de habilitar la protección de cebos, el sistema despliega archivos de cebos en directorios protegidos y directorios clave (a menos que los usuarios especifiquen lo contrario). Un archivo de cebo ocupa solo unos pocos recursos y no afecta el rendimiento del servidor.	Enabled

Parámetro		Descripción	Valor de ejemplo
	Associated Servers	Número de servidores asociados a la política.	-

----Fin

Consulta de tareas de restauración de copia de respaldo

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰ y elija **Security & Compliance** > **Host Security Service**.

Paso 3 En el panel de navegación, elija **Prevention** > **Ransomware Prevention**. Haga clic en el número de tareas de restauración de copia de respaldo.

Paso 4 En el cuadro de diálogo que se muestra, vea los detalles de la tarea de restauración de copia de respaldo. Puede filtrar o buscar un servidor por su nombre o estado. Para obtener más información, consulte **Tabla 5-6**.

Tabla 5-6 Parámetros de tarea de restauración de copia de respaldo

Parámetro	Descripción	Valor de ejemplo
Server Name/ID	Nombre o ID de un servidor que ejecuta una tarea de restauración.	-
Backup Name	Nombre de un archivo de copia de respaldo.	-
Restoration Status	Estado de restauración de un servidor. ● Succeeded ● Skipped ● Failed ● Ongoing ● Timed out ● Waiting Si se omite una tarea, se ha producido un error o se ha agotado el tiempo de espera, vuelva a realizar la restauración.	Succeeded
Start/End Time	Hora de inicio y finalización de la restauración de copias de seguridad.	-

----Fin

Restauración de datos del servidor

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en y elija **Security & Compliance** > **Host Security Service**.

Paso 3 En el panel de navegación, elija **Prevention** > **Ransomware Prevention**. Haga clic en la pestaña **Protected Servers**. En la **Operation**, haga clic en **Restore**.

Paso 4 En el cuadro de diálogo que se muestra, vea la información sobre el servidor que se va a restaurar. Puede buscar el origen de datos de copia de respaldo que se va a restaurar filtrando el estado de la copia de respaldo y buscando el nombre de la copia de respaldo. **Tabla 5-7** describe los parámetros.

Tabla 5-7 Parámetros de origen de datos de copia de respaldo

Parámetro	Descripción	Valor de ejemplo
Backup Name	Nombre de un archivo de copia de respaldo.	-
Backup Status	Estado de la copia de respaldo. ● Available ● Creating ● Deleting ● Restoring ● Error La copia de respaldo se puede utilizar para la restauración si está en el estado disponible.	-
Created	Hora en la que se realizó una copia de respaldo del origen de datos.	-

Paso 5 En la columna **Operation** de una copia de respaldo, haga clic en **Restore**.

NOTA

Solo se puede restaurar una copia de respaldo en el estado disponible.

Paso 6 En el cuadro de diálogo mostrado, confirme la información sobre el servidor y el origen de datos de copia de respaldo y haga clic en **OK**.

----Fin

Aumento de la capacidad de copia de respaldo

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en y elija **Security & Compliance** > **Host Security Service**.

Paso 3 En el panel de navegación, elija **Prevention** > **Ransomware Prevention**. Haga clic en **Buy Capacity**.

Paso 4 En el cuadro de diálogo que se muestra, configure la capacidad.

Paso 5 Haga clic en **OK** y complete el pago.

- Si el pago no se ha completado, se mostrará un mensaje que indica que la capacidad de copia de respaldo está bloqueada. No puede realizar otros pedidos de capacidad de copia de respaldo antes de pagar el pedido actual.
- Si el pago se ha completado, compruebe si su capacidad ha cambiado realizando 4.

----Fin

Modificación de una política de copia de respaldo

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰ y elija **Security & Compliance** > **Host Security Service**.

Paso 3 En el panel de navegación, elija **Prevention** > **Ransomware Prevention**. Haga clic en **Modify Backup Policy**.

Paso 4 Configure la política en el cuadro de diálogo que se muestra.describes the parameters.

Tabla 5-8 Parámetros de política

Parámetro	Descripción	Valor de ejemplo
Backup Frequency	Los datos se pueden respaldar automáticamente en días específicos en una búsqueda, o en un intervalo fijo. ● **Weekly**: Seleccione uno o más días a la semana para realizar una copia de respaldo de los datos. ● **Day based**: El intervalo del intervalo de respaldo es de 1 a 30 días.	Weekly
Execution Time	Hora en que se inicia la copia de respaldo automatizada. **NOTA** Ejemplo de configuraciones de políticas Política 1: Establezca **Backup Frequency** en **Weekly**, seleccione **Wednesday** y **Saturday** y establezca **Execution Time** en **00:00** y **13:00**. Los datos se respaldarán automáticamente a las 00:00 y a las 13:00 todos los miércoles y sábados. Política 2: Establecer **Backup Frequency** en **Day based**. Establezca **Execution Time** en **02:00** y **14:00**. Los datos se respaldarán automáticamente a las 02:00 y 14:00 en un intervalo de dos días.	00:00, 07:00
Timezone	Seleccione la zona horaria de la hora de copia de respaldo.	UTC+08:00

Paso 5 Confirme la configuración y haga clic en **Next**. Configure la regla de retención de copias de respaldo.

- **Type**: **Backup Quantity**

  Configure la regla de copia de respaldo. For more information, see **Tabla 5-9**.

  Tabla 5-9 Parámetros para la retención de datos por cantidad

Parámetro	Descripción	Valor de ejemplo
Rule	Número de copias de respaldo más recientes que se conservarán. **AVISO** Esta configuración tiene efecto independientemente de cómo configure las opciones avanzadas. Por ejemplo, si la regla configurada para mantener las 30 copias de seguridad más recientes y la regla se establece en 3 (es decir, tres meses, aproximadamente 90 días) **Advanced Options** están configuradas para mantener la copia de respaldo más reciente en los últimos 3 meses (90 días), se conservarán las 30 copias de seguridad más recientes.	30
(Optional) Advanced Options	Puede conservar la copia de respaldo más reciente en un día, una semana, un mes o un año. – Copia de respaldo diaria: se conserva la última copia de respaldo en cada uno de los días especificados. – Copia de respaldo semanal: se conserva la última copia de respaldo en cada una de las semanas especificadas. – Copia de respaldo mensual: se conserva la última copia de respaldo en cada uno de los meses especificados. – Copia de respaldo anual: se conserva la última copia de respaldo en cada uno de los años especificados. **NOTA** Si se configuran varias reglas, la regla con el período de retención más largo entra en vigor.	Keep the most recent backup from each of the last three months

- **Type**: **Time period**

  Configure la regla de copia de respaldo. Para obtener más información, consulte **Tabla 5-10**.

Tabla 5-10 Parámetros para la retención de datos por periodo de tiempo

Parámetro	Descripción	Valor de ejemplo
Rule	Seleccione o personalice un período de retención de copias de seguridad. El sistema conservará automáticamente las copias de seguridad y eliminará las antiguas según su configuración. El período de retención puede ser: – Days – 1 month – 3 months – 6 months – 1 year	3 months

- **Type**: **Permanent**

  Los datos de copia de respaldo se almacenarán permanentemente.

  NOTA

  Si el **Retention Type** de una regla cambia de **Time period** a Permanente, las copias de seguridad históricas se eliminarán siguiendo la configuración del **Time period**. Para obtener más información, consulte **¿Por qué la regla de retención no tiene efecto después de ser modificada?**

Paso 6 Haga clic en **OK**.

----Fin

5.3.2 Habilitación de la prevención de ransomware

Prerrequisitos

Ha adquirido Host Security Service edición premium o WTP.

Restricciones

Solo los hosts en la nube de Huawei admiten la protección contra ransomware.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰ y elija **Security & Compliance** > **Host Security Service**.

Paso 3 En el panel de navegación, elija **Prevention** > **Ransomware Prevention**. Haga clic en la pestaña **Protected Servers**. Haga clic en **Add Server**.

Paso 4 En el cuadro de diálogo que se muestra, seleccione **Linux**, active la protección, configure la política y haga clic en **Next**. Para obtener más información, consulte **Tabla 5-11**.

Tabla 5-11 Parámetros de protección contra ransomware

Parámetro	Descripción	Valor de ejemplo
OS	Sistema operativo del servidor a proteger.	Linux
Ransomware Prevention	: habilitado : Dishabilitado	
Policy	Seleccione una política existente o cree una nueva. ● **Use policy**: Seleccione una política existente. ● **Create new**: **Crear una política**.	Use policy
Policy	Seleccione una política existente.	-

Paso 5 Haga clic en **Next**. Configure la regla de copia de respaldo del servidor y la regla de retención.

- Se recomienda habilitar la copia de respaldo del servidor.
- Habilite la copia de respaldo del servidor y configure la regla de retención. Para obtener más información, consulte **Modificación de una directiva de copia de respaldo**.

  NOTA

  Se le aconseja hacer una copia de seguridad periódica de los datos del servidor, o sus servidores no pueden ser recuperados si están dañados por el ransomware.

Paso 6 Haga clic en **Next**. Seleccione los servidores. Puede buscar un servidor por su nombre o por filtrado.

Paso 7 Haga clic en **OK**.

Paso 8 En el panel de navegación, elija **Prevention** > **Ransomware Prevention**. Haga clic en la pestaña **Protected Servers** y compruebe los servidores protegidos.

----Fin

5.3.3 Gestión de políticas

AVISO

Actualmente, puede crear una política de prevención de ransomware solo cuando se habilita la prevención de ransomware.

Creación de una política

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en y elija **Security & Compliance** > **Host Security Service**.

Paso 3 En el panel de navegación, elija **Prevention** > **Ransomware Prevention**. Haga clic en la pestaña **Protected Servers**. Haga clic en **Add Server**.

Paso 4 En el cuadro de diálogo que se muestra, seleccione **Linux**, active la protección y seleccione **Create new**. Para obtener más información, consulte **Tabla 5-12**.

Tabla 5-12 Parámetros de política

Parámetro	Descripción	Valor de ejemplo
OS	Sistema operativo del servidor a proteger.	Linux
Ransomware Prevention	Se recomienda habilitar la protección contra ransomware.  : habilitado  : Dishabilitado	
Policy	Seleccione una política existente o cree una nueva. ● **Use policy**: Seleccione una política existente. ● **Create new**: Crear una política.	Create new
Policy	Nombre de la política.	-
Action	Cómo se maneja un evento. ● Report alarm and isolate ● Report alarm	Report alarm and isolate
Bait File	Archivos y directorios que almacenan datos no válidos en servidores y se utilizan como Honeypots. Un archivo de cebo ocupa solo unos pocos recursos del servidor y no afecta el rendimiento del servidor. Si la prevención de ransomware está habilitada, esta función está habilitada de forma predeterminada.	-
Bait File Directories	Directorios donde se colocan los archivos de cebo. Separar varios directorios con punto y coma (;). Puede configurar hasta 20 directorios.	-
Excluded Directory (Optional)	Directorio donde se almacenan datos válidos. Separar varios directorios con punto y coma (;). Puede configurar hasta 20 directorios excluidos.	-

Parámetro	Descripción	Valor de ejemplo
Protected File Type	Tipos de archivos a proteger. Se pueden proteger más de 70 formatos de archivo, incluyendo bases de datos, contenedores, código, claves de certificado y copias de respaldo.	Select all

Paso 5 Haga clic en **Next**. Configurar la copia de respaldo del servidor.

- Puede habilitar o deshabilitar la copia de respaldo del servidor según sea necesario.
- Habilite la copia de respaldo del servidor y configure la regla de retención. Para obtener más información, consulte **Modificación de una directiva de copia de respaldo**.

  NOTA

  Se le aconseja hacer una copia de seguridad periódica de los datos del servidor, o sus servidores no pueden ser recuperados si están dañados por el ransomware.

Paso 6 Haga clic en **Next**. Seleccione los servidores. Puede buscar un servidor por su nombre o por filtrado.

Paso 7 Haga clic en **OK** para habilitar la protección contra ransomware y crear la política.

Paso 8 En el panel de navegación, elija **Prevention** > **Ransomware Prevention**. Haga clic en la pestaña **Policies** y compruebe la nueva política.

----Fin

Modificación de una política

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰ y elija **Security & Compliance** > **Host Security Service**.

Paso 3 En el panel de navegación, elija **Prevention** > **Ransomware Prevention**. Haga clic en la pestaña **Policies**.

Paso 4 Haga clic en **Edit** en la columna **Operation** de una política. Edite la información de política y los servidores asociados. Para obtener más información, consulte **Tabla 5-13**.

Tabla 5-13 Parámetros de política

Parámetro	Descripción	Valor de ejemplo
Policy	Nombre de la política.	-
Action	Cómo se maneja un evento. ● Report alarm and isolate ● Report alarm	Report alarm and isolate

Parámetro	Descripción	Valor de ejemplo
Bait File	Archivos y directorios que almacenan datos no válidos en servidores y se utilizan como Honeypots. Un archivo de cebo ocupa solo unos pocos recursos y no afecta el rendimiento del servidor. Si la prevención de ransomware está habilitada, esta función está habilitada de forma predeterminada.	-
Bait File Directories	Directorios donde se colocan los archivos de cebo. Separar varios directorios con punto y coma (;). Puede configurar hasta 20 directorios.	/etc
Excluded Directory (Optional)	Directorio donde se almacenan datos válidos. Separar varios directorios con punto y coma (;). Puede configurar hasta 20 directorios excluidos.	/backup
Protected File Type	Tipos de archivos a proteger. Se pueden proteger más de 70 formatos de archivo, incluyendo bases de datos, contenedores, código, claves de certificado y copias de respaldo.	Select all
Associate Servers	Servidores protegidos por la política. Puede eliminar servidores según sea necesario.	-

Paso 5 Confirme la información de la política y haga clic en **OK**.

----Fin

Eliminación de una política

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰ y elija **Security & Compliance** > **Host Security Service**.

Paso 3 En el panel de navegación, elija **Prevention** > **Ransomware Prevention**. Haga clic en la pestaña **Policies**.

Paso 4 Haga clic en **Delete** en la columna **Operation** de la política de destino.

Paso 5 Confirme la información de la política y haga clic en **OK**.

----Fin

5.3.4 Deshabilitación de protección

Prerrequisitos

Ha adquirido Host Security Service edición premium o WTP.

Al menos un servidor está en estado **Protected**.

Deshabilitación de la protección del servidor

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en y elija **Security & Compliance** > **Host Security Service**.

Paso 3 En el panel de navegación, elija **Prevention** > **Ransomware Prevention**. Haga clic en la pestaña **Servers**.

Paso 4 Haga clic en **Disable Protection** en la columna **Operation**.

Paso 5 En el cuadro de diálogo que se muestra, seleccione la función que desea deshabilitar.

- **All protection functions**

  Al seleccionar esto, se deshabilitarán las funciones de protección y copia de respaldo de ransomware.

- **Ransomware prevention**

  Al seleccionar esto solo se deshabilitará la función de prevención de ransomware.

- **Backup**

  Al seleccionar esto solo se deshabilitará la función de copia de respaldo.

Paso 6 Confirme la información y haga clic en **OK**.

----Fin

5.4 Monitoreo de integridad de archivos

Puede consultar las estadísticas y los detalles sobre los cambios en los archivos de los servidores, incluidos los servidores afectados, los tipos de archivos, las rutas y el contenido.

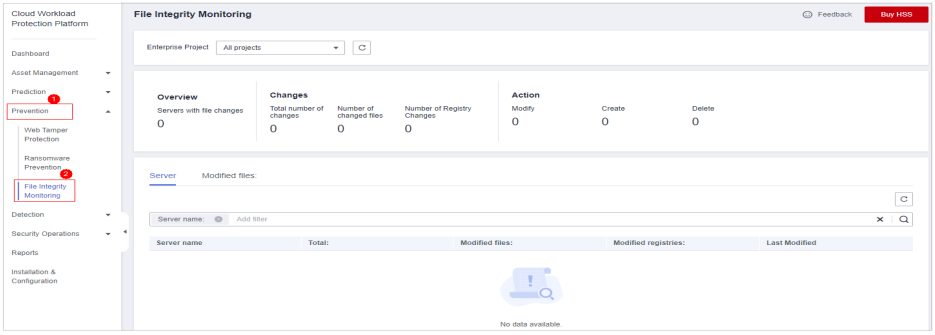
5.4.1 Comprobación de la integridad del archivo

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Vaya a la página de gestión de archivos. Puede seleccionar un proyecto de empresa y comprobar los servidores y los archivos modificados. Consulte **Figura 5-8**.

Figura 5-8 Monitoreo de integridad de archivos



----Fin

5.4.2 Comprobación de los detalles del cambio

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Seleccione **Prevention** > **File Integrity Monitoring**. Se mostrará la pestaña **Server**.

Paso 4 Haga clic en un nombre de servidor para ir a su página de detalles de cambio.

Tabla 5-14 Parámetros sobre los cambios de archivo

Parámetro	Descripción	Valor de ejemplo
File Name	Nombre de un archivo modificado.	du
Path	Ruta de un archivo modificado.	-
Change Description	Descripción del cambio. Para ver los detalles del cambio, coloque el cursor sobre el contenido del cambio.	**SHA2560ba0c4b5e48e55a6** se cambia a **4f6079f5b37d1513**.
Type	Tipo de archivo modificado. Su valor puede ser: ● **File**	File
Action	Cómo se modificó un archivo. ● Create ● Modify ● Delete	Modify
Time Range	Hora en la que se modificó un archivo.	-

----Fin

5.4.3 Comprobación de archivos modificados

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Prevention** > **File Integrity Monitoring**. Haga clic en la pestaña **Monitored Files**. Puede conservar el valor por defecto para **Enterprise Project**. Para obtener más información sobre los parámetros, consulte **Tabla 5-14** en **Comprobación de los detalles del cambio**.

----Fin

6 Detección de intrusiones

6.1 Alarmas

6.1.1 Alarmas de servidor

6.1.1.1 Eventos de alarma de servidor

El servicio genera alarmas en 13 tipos de eventos de intrusión, incluidos ataques de fuerza bruta, comportamiento de procesos anormales, web shells, inicios de sesión anormales y procesos maliciosos. Puede aprender todos estos eventos en la consola y eliminar los riesgos de seguridad en sus activos de manera oportuna.

Tipos de alarma de servidor

Tipo de evento	Nombre de la alarma	Descripción	Edición empresarial	Edición premium	Web Tamper Protection
Malware	Malicious programs	Los programas maliciosos incluyen troyanos y web shells implantados por hackers para robar sus datos o controlar sus servidores. Por ejemplo, los hackers probablemente usarán sus servidores como mineros o zombies DDoS. Esto ocupa un gran número de recursos de CPU y de red, lo que afecta a la estabilidad del servicio. Comprobar malware, como shells web, caballos de Troya, software de minería, gusanos y otros virus y variantes, y matarlos con un solo clic. El malware se encuentra y elimina mediante el análisis de las características y comportamientos del programa, algoritmos de huellas dactilares de imagen AI y escaneo y matanza en la nube.	√ (Isolate and kill)	√ (Isolate and kill)	√ (Isolate and kill)
	Ransomware	Compruebe el ransomware incrustado en medios como páginas web, software, correos electrónicos y medios de almacenamiento. El ransomware se utiliza para cifrar y controlar sus activos de datos, como documentos, correos electrónicos, bases de datos, código fuente, imágenes y archivos comprimidos, para aprovechar la extorsión de las víctimas.	×	√	√
	Web shells	Compruebe si los archivos (a menudo archivos PHP y JSP) en sus directorios web son shells web. Puede configurar la regla de detección de shell web en la regla de **Web Shell Detection** en la página **Policies**. HSS comprobará si hay comandos sospechosos o ejecutados remotamente. Es necesario agregar un directorio protegido en la gestión de políticas. Para más detalles, consulte **Detección de Web Shell**.	×	√	√

Tipo de evento	Nombre de la alarma	Descripción	Edición empresarial	Edición premium	Web Tamper Protection
	Reverse shells	Supervise los comportamientos de los procesos del usuario en tiempo real para detectar shells inversos causados por conexiones no válidas. Se pueden detectar shells inversos para protocolos como TCP, UDP e ICMP. Puede configurar la regla de detección de shell inverso en la regla de **Malicious File Detection** de la página **Policies**. HSS comprobará si hay comandos sospechosos o ejecutados remotamente.	×	√	√
Exploits Used	Exploit Attack	Detecte intrusiones en el servidor explotando vulnerabilidades en tiempo real y reporte alarmas.	√	√	√
Abnormal system behavior	File privilege escalations	Después de que los piratas informáticos intruyan los servidores, intentarán explotar las vulnerabilidades para concederse los permisos de root o agregar permisos para los archivos. De esta manera, pueden crear cuentas del sistema ilegalmente, modificar permisos de cuenta y manipular archivos. HSS detecta la escalada de privilegios para procesos y archivos en el sistema actual. Se pueden detectar las siguientes operaciones de escalada de privilegios anormales: ● Escalada de privilegios raíz mediante la explotación de las vulnerabilidades del programa SUID ● Escalada de privilegios de root mediante la explotación de vulnerabilidades del kernel ● Escalada de privilegios de archivo	×	√	√
	Process privilege escalations				

Tipo de evento	Nombre de la alarma	Descripción	Edición empresarial	Edición premium	Web Tamper Protection
	Important file changes File/ Directory changes	Si los hackers informáticos se introducen en su sistema, es probable que alteren los archivos importantes del sistema para forjar identidades o prepararse para ataques adicionales. ● Supervise los archivos clave (como **ls**, **ps**, **login**, y **top**) y directorios, e informe de alarmas si se detectan modificaciones. Para obtener más información sobre las rutas supervisadas, consulte **Rutas de acceso de archivo importantes supervisadas**. ● La información de cambio de archivo clave incluye las rutas de acceso de los archivos modificados, la última hora de modificación y los nombres de los servidores que almacenan los archivos de configuración. ● La información de cambio de directorio de archivos incluye el alias de archivo, las rutas de acceso de los archivos modificados y los nombres de los servidores que almacenan los archivos de configuración. ● Puede agregar bibliotecas de huellas dactilares de archivos críticos para una mejor recopilación de información de archivos críticos y detección de excepciones. HSS solo comprueba si los directorios o archivos han sido modificados, no si son modificados manualmente o por un proceso.	√	√	√
	Abnormal process behavior	Compruebe los procesos en los servidores, incluidos sus identificadores, líneas de comandos, rutas de proceso y comportamiento. Envíe alarmas sobre operaciones e intrusiones de procesos no autorizados. Se puede detectar el siguiente comportamiento anormal del proceso: ● Uso anormal de la CPU ● Procesos que acceden a direcciones IP maliciosas ● Aumento anormal de las conexiones de proceso simultáneo	√	√	√

Tipo de evento	Nombre de la alarma	Descripción	Edición empresarial	Edición premium	Web Tamper Protection
	High-risk command executions	Puede configurar qué comandos desencadenarán alarmas en la regla **High-risk Command Scan** en la página **Policies**. HSS comprueba los comandos ejecutados en tiempo real y genera alarmas si se detectan comandos de alto riesgo.	×	√	√
	Abnormal shells	Detecte acciones en shells anormales, como mover, copiar y eliminar archivos de shell, y modificar los permisos de acceso y los enlaces duros de los archivos. Puede configurar la regla de detección de shell anormal en la regla de **Malicious File Detection** de la página **Policies**. HSS comprobará si hay comandos sospechosos o ejecutados remotamente.	×	√	√
	Crontab Suspicious Task	Compruebe y enumere los servicios iniciados automáticamente, las tareas programadas, las bibliotecas dinámicas precargadas, las claves de registro de ejecución y las carpetas de inicio. Puede recibir una notificación inmediatamente cuando se detectan elementos de inicio automático anormales y localizar rápidamente troyanos.	×	√	√

Tipo de evento	Nombre de la alarma	Descripción	Edición empresarial	Edición premium	WebTamper Protection
Abnormal user behavior	Brute-force attacks	Si los hackers inician sesión en sus servidores a través de ataques de fuerza bruta, pueden obtener los permisos de control de los servidores y realizar operaciones maliciosas, como robar datos del usuario; implantar ransomware, mineros o troyanos; cifrar datos; o utilizar sus servidores como zombies para realizar ataques DDoS. Detecte ataques de fuerza bruta en cuentas SSH, RDP, FTP, SQL Server y MySQL. ● Si el número de ataques de fuerza bruta (intentos de contraseña incorrectos consecutivos) de una dirección IP alcanza 5 en 30 segundos, la dirección IP se bloqueará. De forma predeterminada, los atacantes SSH sospechosos están bloqueados durante 12 horas. Otros tipos de atacantes sospechosos están bloqueados durante 24 horas. ● Puede comprobar si la dirección IP es confiable en función de su tipo de ataque y cuántas veces ha sido bloqueada. Puede desbloquear manualmente las direcciones IP en las que confía.	√	√	√
	Abnormal logins	Detecte un comportamiento de inicio de sesión anormal, como el inicio de sesión remoto y los ataques de fuerza bruta. Si se reportan inicios de sesión anormales, sus servidores pueden haber sido intruidos por piratas informáticos. ● Compruebe y maneje los inicios de sesión remotos. Puede comprobar las direcciones IP de inicio de sesión bloqueadas y quién las usó para iniciar sesión en qué servidor a qué hora. Si la ubicación de inicio de sesión de un usuario no es una ubicación de inicio de sesión común que establezca, se activará una alarma. ● Activar una alarma si un usuario inicia sesión mediante un ataque de fuerza bruta.	√	√	√

Tipo de evento	Nombre de la alarma	Descripción	Edición empresarial	Edición prémium	Web Tamper Protection
	Invalid accounts	Los hackers probablemente pueden descifrar cuentas inseguras en sus servidores y controlar los servidores. HSS comprueba cuentas ocultas sospechosas y cuentas clonadas y genera alarmas en ellas.	√	√	√

Rutas de acceso de archivo importantes supervisadas

Tipo	Linux
bin	/bin/ls /bin/ps /bin/bash /bin/netstat /bin/login /bin/find /bin/lsmod /bin/pidof /bin/lsof /bin/ss

Tipo	Linux
usr	/usr/bin/ls /usr/bin/ps /usr/sbin/ps /usr/bin/bash /usr/bin/netstat /usr/sbin/netstat /usr/sbin/rsyslogd /usr/sbin/ifconfig /usr/bin/login /usr/bin/find /usr/sbin/lsmod /usr/sbin/pidof /usr/bin/lsof /usr/sbin/lsof /usr/sbin/tcpd /usr/bin/passwd /usr/bin/top /usr/bin/du /usr/bin/chfn /usr/bin/chsh /usr/bin/killall /usr/bin/ss /usr/sbin/ss /usr/bin/ssh /usr/bin/scp
sbin	/sbin/syslog-ng /sbin/rsyslogd /sbin/ifconfig /sbin/lsmod /sbin/pidof

6.1.1.2 Comprobación y manejo de alarmas de servidor

El servicio HSS muestra las estadísticas de alarmas y eventos y su resumen en una sola página. Puede tener una visión general rápida de las alarmas, incluyendo el número de servidores con alarmas, alarmas manejadas, alarmas no manejadas, direcciones IP bloqueadas y archivos aislados.

La página **Events** muestra los eventos de alarma generados en los últimos 30 días.

El estado de un evento controlado cambia de **Unhandled** a **Handled**.

Restricciones y limitaciones

- Para omitir las comprobaciones de la ejecución de comandos de alto riesgo, la escalada de privilegios, los shells inversos, los shells anormales o los web shells, deshabilite manualmente las políticas correspondientes en los grupos de políticas de la página **Policies**. HSS no comprobará los servidores asociados con las directivas deshabilitadas. Para obtener más información, consulte **Comprobación o creación de un grupo de políticas**.
- Otros elementos de detección no se pueden deshabilitar manualmente.

Comprobación de eventos de alarma

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, elija **Detection** > **Alarms**, y haga clic en **Server Alarms**.

Tabla 6-1 Estadísticas de alarmas

Evento de alarma	Descripción
Affected Servers	Número de servidores para los que se generan alarmas.
Alarms to be Handled	Número de alarmas a manejar. De forma predeterminada, todas las alarmas no controladas se muestran en la página **Events**. Para obtener más información, consulte **Manejo de eventos de alarma**.
Handled Alarms	Número de alarmas manejadas.
Blocked IP Addresses	Número de direcciones IP bloqueadas. Puede hacer clic en el número para comprobar la lista de direcciones IP bloqueadas. La lista de direcciones IP bloqueadas muestra los nombres del servidor, las direcciones IP bloqueadas, los tipos de ataques, el número de ataques bloqueados, la primera y la última vez que se bloquean las direcciones IP, la duración del bloque y el estado. Si una dirección IP válida está bloqueada por error, (por ejemplo, después de O&M el personal ingresa contraseñas incorrectas varias veces), puedes desbloquearlo manualmente. Si un servidor es atacado con frecuencia, se recomienda corregir sus vulnerabilidades de manera oportuna y eliminar los riesgos. **AVISO** Después de desbloquear una dirección IP bloqueada, HSS ya no bloqueará las operaciones realizadas por la dirección IP.

Evento de alarma	Descripción
Isolated Files	El servicio HSS puede aislar los archivos de amenazas detectados. Los archivos aislados se muestran en un panel deslizante de la página **Server Alarms**. Puede hacer clic en **Isolated Files** en la esquina superior derecha para comprobarlos. Puede recuperar archivos aislados. Para más detalles, consulte **Gestión de archivos aislados**.

Paso 4 Haga clic en un evento de alarma en la lista de tipos de eventos para ver los servidores afectados y la hora de ocurrencia del evento. Se muestra la siguiente información:

- Número total de alarmas
- Número de cada tipo de alarmas

Paso 5 Haga clic en un nombre de alarma en la lista de tipos de eventos para ver sus detalles.

----Fin

Manejo de eventos de alarma

Esta sección describe cómo debe manejar los eventos de alarma para garantizar la seguridad del servidor.

NOTA

No confíe plenamente en las alarmas para defenderse de los ataques, porque no todos los problemas se pueden detectar de manera oportuna. Se recomienda tomar más medidas para prevenir amenazas, como comprobar y corregir vulnerabilidades y configuraciones inseguras.

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, elija **Detection** > **Alarms**, y haga clic en **Server Alarms**.

Tabla 6-2 Estadísticas de alarmas

Evento de alarma	Descripción
Affected Servers	Número de servidores para los que se generan alarmas.
Alarms to be Handled	Número de alarmas a manejar. De forma predeterminada, todas las alarmas no controladas se muestran en la página **Events**. Para obtener más información, consulte **Manejo de eventos de alarma**.

Evento de alarma	Descripción
Handled Alarms	Número de alarmas manejadas.
Blocked IP Addresses	Número de direcciones IP bloqueadas. Puede hacer clic en el número para comprobar la lista de direcciones IP bloqueadas. La lista de direcciones IP bloqueadas muestra los nombres del servidor, las direcciones IP bloqueadas, los tipos de ataques, el número de ataques bloqueados, la primera y la última vez que se bloquean las direcciones IP, la duración del bloque y el estado. Si una dirección IP válida está bloqueada por error, (por ejemplo, después de O&M el personal ingresa contraseñas incorrectas varias veces), puedes desbloquearlo manualmente. Si un servidor es atacado con frecuencia, se recomienda corregir sus vulnerabilidades de manera oportuna y eliminar los riesgos. **AVISO** Después de desbloquear una dirección IP bloqueada, HSS ya no bloqueará las operaciones realizadas por la dirección IP.
Isolated Files	El servicio HSS puede aislar los archivos de amenazas detectados. Los archivos aislados se muestran en un panel deslizante de la página **Server Alarms**. Puede hacer clic en **Isolated Files** en la esquina superior derecha para comprobarlos. Puede recuperar archivos aislados. Para más detalles, consulte **Gestión de archivos aislados**.

Paso 4 Haga clic en un tipo de evento, seleccione eventos y haga clic en **Handle**. **Tabla 6-3** describe los métodos de procesamiento que puede elegir.

NOTA

También puede hacer clic en **Handle** en la fila donde reside una alarma.

Los eventos de alarma se muestran en la página **Server Alarms**. Aquí puede consultar hasta 30 días de eventos históricos.

Compruebe y maneje los eventos de alarma según sea necesario. El estado de un evento controlado cambia de **Unhandled** a **Handled**. HSS ya no recopilará sus estadísticas ni las mostrará en la página **Dashboard**.

Tabla 6-3 Parámetros de gestión de eventos

Método	Descripción
Ignore	Ignore la alarma actual. Cualquier nueva alarma del mismo tipo seguirá siendo reportada por el HSS.

Método	Descripción
Isolate and kill	Si un programa es aislado y eliminado, se terminará inmediatamente y ya no podrá realizar operaciones de lectura o escritura. Los archivos de origen aislados de programas o procesos se muestran en el panel desplegable **Isolated Files** y no pueden dañar los servidores. Puede hacer clic en **Isolated Files** en la esquina superior derecha para comprobar los archivos. Para más detalles, consulte **Gestión de archivos aislados**. Los siguientes tipos de eventos de alarma admiten el aislamiento y la matanza en línea: ● Malware ● Abnormal process behavior **NOTA** Cuando un programa se aísla y finaliza, el proceso del programa finaliza inmediatamente. Para evitar el impacto en los servicios, verifique el resultado de la detección y cancele el aislamiento de los programas maliciosos (si los hay).
Mark as handled	Marque el evento como manejado. Puede agregar comentarios para el evento para registrar más detalles.
Add to whitelist	Agregue elementos de falsa alarma de los tipos de **Brute-force attack** y de **Abnormal login** a la lista blanca de inicio de sesión. HSS ya no reportará la alarma en los elementos de la lista blanca.
Add to alarm whitelist	Agregue elementos de falsa alarma de los siguientes tipos a la lista blanca de inicio de sesión. HSS ya no reportará la alarma en los elementos de la lista blanca. ● Reverse shell ● Web shell ● Abnormal process behavior ● Process privilege escalation ● File privilege escalation ● High-risk command execution ● Malware ● Critical file change

----Fin

6.1.1.3 Gestión de archivos aislados

El servicio HSS puede aislar los archivos de amenazas detectados. Los archivos aislados se muestran en un panel deslizante de la página **Server Alarms**. Puede hacer clic en **Isolated Files** en la esquina superior derecha para comprobarlos y puede recuperar archivos aislados en cualquier momento.

Los siguientes tipos de eventos de alarma admiten el aislamiento y la matanza en línea:

- Programas maliciosos

- Comportamiento de procesos anormales

Aislamiento y eliminación de archivos

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, elija **Detection** > **Alarms**, and click **Server Alarms**.

Paso 4 Seleccione un evento del tipo de **Malware** o **Abnormal process behavior**, y haga clic en **Handle**. En el cuadro de diálogo que se muestra, haga clic en **Isolate and Kill**.

Paso 5 Haga clic en **OK** para aislar y eliminar el malware o los comportamientos de procesos anormales. Los archivos aislados se muestran en un panel deslizante de la página **Server Alarms** y no pueden dañar los servidores. Puede hacer clic en **Isolated Files** en la esquina superior derecha para comprobarlos.

----Fin

Comprobación de archivos aislados

Paso 1 En el área **Alarm Statistics** de la página **Server Alarms**, haga clic en **View Details** en **Isolated Files** para comprobar los archivos aislados.

Paso 2 Compruebe los servidores, nombres, rutas y tiempo de modificación de los archivos aislados.

----Fin

Recuperación de archivos aislados

Paso 1 Haga clic en **Restore** en la columna **Operation** de un archivo aislado.

Paso 2 Haga clic en **OK**.

NOTA

Los archivos recuperados ya no estarán aislados. Tenga cuidado al realizar esta operación.

----Fin

6.1.2 Alarmas de contenedores

6.1.2.1 Eventos de Alarma de Contenedores

Después de habilitar la protección de nodos, el escudo CGS se instalará como un conjunto de demonios para supervisar el estado del contenedor en los nodos del clúster en tiempo real. CGS puede detectar fugas, llamadas al sistema de alto riesgo, procesos anormales, archivos anormales; y puede comprobar el entorno del contenedor. Puede conocer los eventos de alarma de forma exhaustiva en la página **Container Alarms**, y eliminar los riesgos de seguridad en sus activos de manera oportuna.

Tipos de alarmas de contenedores

Tipo de evento	Nombre de la alarma	Mecanismo
Exploits Used	Vulnerability escapes	HSS informa de una alarma si detecta el comportamiento del proceso del contenedor que coincide con el comportamiento de vulnerabilidades conocidas (como Dirty COW, brute-force attack, runC, y shocker).
	File escapes	HSS informa de una alarma si detecta que un proceso contenedor accede a un directorio de archivos clave (por ejemplo, **/etc/shadow** o **/etc/crontab**). Los directorios que cumplen con las reglas de asignación de directorios de contenedores también pueden activar tales alarmas.
Abnormal System Behavior	High-risk system calls	CGS informa de una alarma si detecta una llamada de alto riesgo, como open_by_handle_at, ptrace, setns o reboot.
	Abnormal container processes	● Programa de contenedores maliciosos HSS monitorea el comportamiento del proceso del contenedor y las huellas dactilares del archivo de proceso. Informa de una alarma si detecta un proceso cuyas características de comportamiento coinciden con las de un programa malicioso predefinido. ● Procesos anormales Si está seguro de que sólo se ejecutan procesos específicos en un contenedor, puede incluir los procesos en la página **Policy Groups** y asociar la política al contenedor. HSS informa de una alarma si detecta que un proceso que no está en la lista blanca se está ejecutando en el contenedor.
	Sensitive file access	HSS supervisa los archivos de imagen de contenedor asociados a las directivas de protección de archivos e informa de una alarma si se modifican los archivos.

Tipo de evento	Nombre de la alarma	Mecanismo
	Abnormal container startups	HSS supervisa los inicios de contenedores e informa de una alarma si detecta que se ha iniciado un contenedor con demasiados permisos. Esta alarma no indica un ataque real. Los ataques que explotan este riesgo activarán otras alarmas de contenedores HSS. Los elementos de comprobación de contenedores HSS incluyen: ● Inicio de contenedor privilegiado (**privileged:true**) Las alarmas son activadas por los contenedores iniciados con los permisos máximos. Los ajustes que pueden desencadenar tales alarmas incluyen el parámetro **–privileged=true** en el comando **docker run**, y **privileged: true** en el **securityContext** del contenedor en un pod de Kubernetes. Dichas alarmas contienen **privileged:true**, lo que indica que el contenedor alarmado se inicia en modo privilegiado. ● Demasiadas capacidades de contenedores (**capability:[xxx]**) En los sistemas operativos Linux, los permisos del sistema se dividen en grupos antes de asignarlos a los contenedores. Un contenedor solo tiene un número limitado de permisos, y el alcance de impacto de este contenedor es limitado en el caso de un incidente. Sin embargo, los usuarios malintencionados pueden conceder todos los permisos del sistema a un contenedor modificando sus configuraciones de inicio. Tales alarmas contienen **capabilities:[xxx]**, lo que indica que el contenedor alarmado se inicia con demasiadas capacidades. ● Seccomp no habilitado (**seccomp=unconfined**) El modo de computación segura (seccomp) es una característica del kernel de Linux. Puede restringir las llamadas al sistema invocadas por procesos para reducir la superficie de ataque del núcleo. Si **seccomp=unconfined** se configura cuando se inicia un contenedor, las llamadas al sistema no estarán restringidas para el contenedor. Tales alarmas contienen **seccomp=unconfined**, lo que indica que el contenedor alarmado se inicia sin habilitar seccomp. **NOTA** Si seccomp está habilitado, se verificarán los permisos para cada llamada al sistema. Las verificaciones probablemente afectarán a los servicios si las llamadas al sistema son frecuentes. Antes de decidir si desea habilitar seccomp, le aconsejamos que lo pruebe y analice el impacto en sus servicios. ● Escalada de privilegios de contenedor (**no-new-privileges:false**) CGS informa de una alarma si detecta que un proceso intenta escalar permisos ejecutando el comando **sudo** y utilizando el bit SUID o SGID. Si **–no-new-privileges=false** se especifica cuando se inicia un contenedor, el contenedor puede escalar privilegios.

Tipo de evento	Nombre de la alarma	Mecanismo
		Tales alarmas contienen **no-new-privileges:false**, lo que indica que los privilegios no están restringidos para los contenedores con alarma. ● Asignación de directorios de alto riesgo (**mounts:[...]**) For convenience purposes, when a container is started on a server, the directories of the server can be mapped to the container. De esta manera, los servicios en el contenedor pueden leer y escribir recursos directamente en el servidor. Sin embargo, este mapeo conlleva riesgos de seguridad. Si cualquier directorio crítico en el sistema operativo del servidor se asigna al contenedor, las operaciones incorrectas en el contenedor probablemente dañarán el sistema operativo del servidor. HSS informa de una alarma si detecta que una ruta crítica del servidor (**/boot**, **/dev**, **/etc**, **/sys**, **/var/run**) está montada durante el inicio del contenedor. Estas alarmas contienen **mounts: [{"source":"xxx","destination":"yyy"...]**. **NOTA** Las alarmas no se activarán para los archivos a los que los contenedores Docker necesitan acceder con frecuencia, como **/etc/hosts** y **/etc/resolv.conf**.

6.1.2.2 Comprobación y manejo de alarmas de contenedores

El servicio HSS muestra las estadísticas de alarmas y eventos y su resumen en una sola página. Puede tener una visión general rápida de las alarmas, incluyendo el número de contenedores con alarmas, alarmas manejadas y alarmas no manejadas.

La página **Events** muestra los eventos de alarma generados en los últimos 30 días.

El estado de un evento controlado cambia de **Unhandled** a **Handled**.

Consulta de alarmas de contenedores

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, elija **Detection** > **Alarms**, y haga clic en **Container Alarms**.

Tabla 6-4 Estadísticas de alarmas

Evento de alarma	Descripción
Contenedores con alarmas	Número de servidores para los que se generan alarmas.
Alarmas a Manejar	Número de alarmas a manejar. De forma predeterminada, todas las alarmas no controladas se muestran en la página **Events**. Para obtener más información, consulte **Manejo de eventos de alarma**.
Alarmas manejadas	Número de alarmas manejadas.

Paso 4 Haga clic en un evento de alarma en la lista de tipos de eventos para ver los servidores afectados y la hora de ocurrencia del evento. Se muestra la siguiente información:

- Número total de alarmas
- Número de cada tipo de alarmas

Paso 5 Haga clic en un nombre de alarma en la lista de tipos de eventos para ver sus detalles.

----Fin

Manejo de eventos de alarma

Esta sección describe cómo debe manejar los eventos de alarma para garantizar la seguridad del servidor.

NOTA

No confíe plenamente en las alarmas para defenderse de los ataques, porque no todos los problemas se pueden detectar de manera oportuna. Se recomienda tomar más medidas para prevenir amenazas, como comprobar y corregir vulnerabilidades y configuraciones inseguras.

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, elija **Detection** > **Alarms**, y haga clic en **Container Alarms**.

Paso 4 Haga clic en un tipo de evento, seleccione eventos y haga clic en **Handle**. **Tabla 6-5** describe los métodos de procesamiento que puede elegir.

NOTA

También puede hacer clic en **Handle** en la fila donde reside una alarma.

Los eventos de alarma se muestran en la página **Server Alarms**. Aquí puede consultar hasta 30 días de eventos históricos.

Compruebe y maneje los eventos de alarma según sea necesario. El estado de un evento controlado cambia de **Unhandled** a **Handled**. HSS ya no recopilará sus estadísticas.

Tabla 6-5 Parámetros de gestión de eventos

Marcado como	Descripción
Ignore	Ignore la alarma actual. Cualquier nueva alarma del mismo tipo seguirá siendo reportada por el HSS.
Mark as handled	Marque el evento como manejado. Puede agregar comentarios para el evento para registrar más detalles.

----Fin

6.2 Listas blancas

6.2.1 Configuración de la lista blanca de inicio de sesión

En la lista blanca de inicio de sesión, puede configurar las direcciones IP de los servidores de destino, las direcciones IP de inicio de sesión y los nombres de usuario de inicio de sesión.

NOTA

- Si la dirección IP del servidor de destino, la dirección IP de inicio de sesión y el nombre de usuario de un inicio de sesión están todos incluidos en la lista blanca, este inicio de sesión se permitirá sin verificación.
- Después de agregar una dirección IP a una lista blanca siguiendo las instrucciones en **Adición de información de inicio de sesión a la lista blanca de inicio de sesión**, las alarmas (si las hay) que se han generado para la dirección IP no se borrarán automáticamente. Manejar las alarmas haciendo referencia a **Comprobación y manejo de alarmas de servidor**.

Para agregar información de inicio de sesión a la lista blanca de inicio de sesión, puede:

- Agrega elementos de falsa alarma de los **Brute-force attack** y **Abnormal login types** a la lista blanca de inicio de sesión cuando los manipules. Para más detalles, consulte **Comprobación y manejo de alarmas de servidor**.
- Agréguelo a la lista blanca de inicio de sesión en la pestaña **Login Whitelist**.

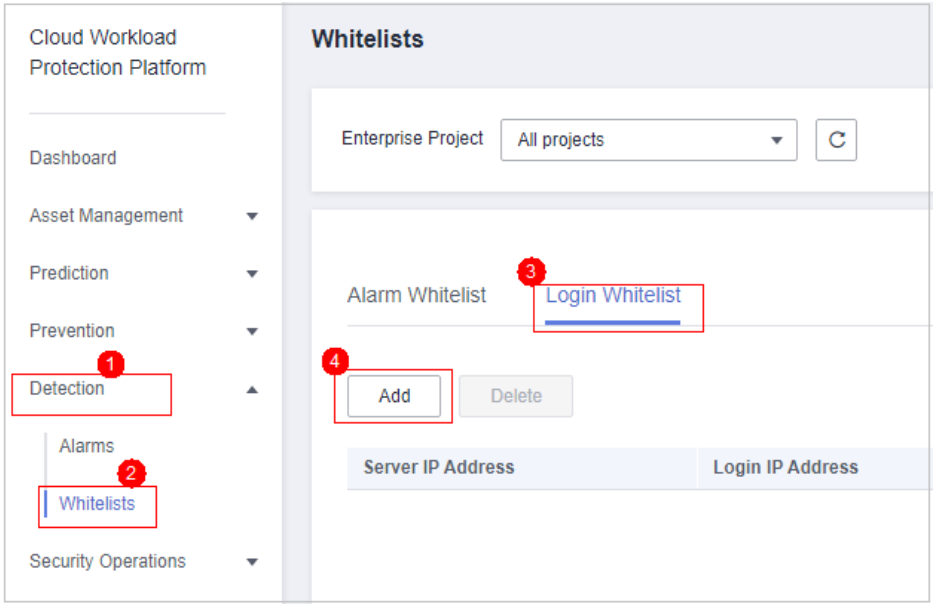
Adición de información de inicio de sesión a la lista blanca de inicio de sesión

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 Access the **Whitelists** page displayed by referring to **Figura 6-1**, and click **Add**.

Figura 6-1 Adición de una lista blanca de inicio de sesión



Paso 4 En la página mostrada, introduzca la dirección IP del servidor, la dirección IP de inicio de sesión y el nombre de usuario de inicio de sesión.

NOTA

- Las direcciones IP pueden ser direcciones IPv4 o IPv6.
- Puede introducir uno o más valores en cada cuadro de texto de dirección IP. Direcciones IP, rangos y máscaras son compatibles, y deben estar separados por comas (,). Ejemplo: **192.168.1.1, 192.168.2.1-192.168.6.1, 192.168.7.0/24**.

Paso 5 Haga clic en **OK**.

----Fin

Otras operaciones

Eliminar información de inicio de sesión de la lista blanca de inicio de sesión

Para eliminar una información de inicio de sesión de la lista blanca, selecciónela y haga clic en **Delete**, o haga clic en **Delete** en la fila en la que reside.

NOTA

Tenga cuidado al realizar la operación de eliminación porque no se puede revertir.

6.2.2 Gestión de la lista blanca de alarmas

Puede configurar la lista blanca de alarmas para reducir las falsas alarmas. Los eventos se pueden eliminar de la lista blanca.

Los eventos incluidos en la lista blanca no activarán alarmas.

En la página **Alarms**, puede agregar alarmas falsas a la lista blanca de alarmas. HSS ya no generará alarmas para él.

Agregar eventos a la lista blanca de alarmas

Tabla 6-6 Configuración de la lista blanca de alarmas

Método	Descripción
Añadir a la lista blanca de alarmas	Elija agregar la alarma a la lista blanca cuando la maneje. Para obtener más información, consulte "Manejo de eventos de alarma" en **Comprobación y manejo de alarmas de servidor**. Los siguientes tipos de eventos se pueden agregar a la lista blanca de alarmas: ● Reverse shell ● Web shell ● Abnormal process behavior ● Process privilege escalation ● File privilege escalation ● High-risk command ● Malicious program

Comprobación de la lista blanca de alarmas

Realice los siguientes pasos para comprobar la lista blanca de alarmas:

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, elija **Detection** > **Whitelists**.

Paso 4 Haga clic en **Alarm Whitelist** para ver la lista blanca de alarmas agregada. Para obtener más información, consulte **Tabla 6-7**.

Tabla 6-7 Descripción del parámetro

Nombre del parámetro	Descripción
Alarm Type	Nombre del tipo de lista blanca de alarma.
SHA256	Valor hash del archivo de destino.
Path	Ruta de acceso que almacena el archivo del servidor.
Data Source	Fuente de la lista blanca de destino.

----Fin

Procedimiento posterior

Eliminación de alarmas de la lista blanca

Para eliminar una alarma de la lista blanca, selecciónela y haga clic en **Delete**.

NOTA

Las alarmas eliminadas de la lista blanca se activarán. Las eliminaciones no se pueden revertir. Tenga cuidado al realizar esta operación.

7 Operaciones de seguridad

7.1 Gestión de políticas

7.1.1 Consulta de un grupo de políticas

Puede agrupar directivas y servidores para aplicar directivas por lotes a servidores y contenedores, adaptándose fácilmente a escenarios empresariales.

Antes de empezar

- Cuando habilita la edición empresarial, el grupo de políticas del lado del inquilino de esta edición (incluidas las políticas de detección de shell de sitios web y contraseñas débiles) entrará en vigor para todos los servidores.
- Cuando habilita la edición premium que compró por separado o que se incluyó con la edición WTP, el grupo de pólizas del lado del inquilino de esta edición entra en vigor.

  Para crear su propio grupo de políticas, puede copiar el grupo de políticas del lado del inquilino y agregar o quitar políticas en la copia.

Lista de políticas

Política	Acción	Sistema operativo soportado	Edición empresarial	Edición prémium	Edición WTP	Seguridad de contenedores
Asset Discovery	Escanee y muestre todo el software en un solo lugar, incluido el nombre del software, la ruta y las principales aplicaciones, lo que le ayudará a identificar activos anormales.	Linux	×	√	√	√

Política	Acción	Sistema operativo soportado	Edición empresarial	Edición prémium	Edición WTP	Seguridad de contenedores
Weak Password Detection	Cambie las contraseñas débiles por contraseñas más fuertes según los resultados y sugerencias del análisis HSS.	Linux	√ (Compruebe solo contraseñas débiles personalizadas)	√	√	√
Configuration Check	Compruebe las configuraciones de inicio de sesión inseguras de Tomcat, Nginx y SSH encontradas por HSS.	Linux	×	√	√	√
Container Information Collection	Compruebe si hay tiempo de ejecución del contenedor anormal, incluyendo inicio anormal y configuraciones incorrectas.	Linux	×	×	×	√
Web Shell Detection	Escanee directorios web en servidores en busca de shells web.	Linux	√ (Comprobar sólo rutas especificadas)	√	√	√
Container File Monitoring	Detectar el acceso a archivos que infringe las políticas de seguridad. El personal de O&M de seguridad puede comprobar si los hackers están intruyendo y manipulando archivos confidenciales.	Linux	×	×	×	√
Container Process Whitelist	Compruebe si hay inicios de procesos que infrinjan las políticas de seguridad.	Linux	×	×	×	√

Política	Acción	Sistema operativo soportado	Edición empresarial	Edición prémium	Edición WTP	Seguridad de contenedores
File Protection	Compruebe los archivos en el sistema operativo Linux, las aplicaciones y otros componentes para detectar manipulaciones.	Linux	×	√	√	√
Login Security Check	Detecte ataques de fuerza bruta en cuentas SSH, FTP y MySQL. Si el número de ataques de fuerza bruta (intentos de contraseña incorrectos consecutivos) de una dirección IP alcanza 5 en 30 segundos, la dirección IP se bloqueará. De forma predeterminada, los atacantes SSH sospechosos están bloqueados durante 12 horas. Otros tipos de atacantes sospechosos están bloqueados durante 24 horas. Puede comprobar si la dirección IP es confiable en función de su tipo de ataque y cuántas veces ha sido bloqueada. Puede desbloquear manualmente las direcciones IP en las que confía.	Linux	×	√	√	√

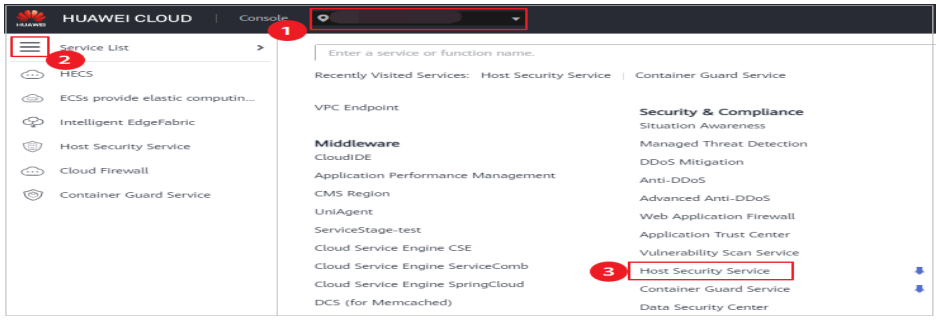
Política	Acción	Sistema operativo soportado	Edición empresarial	Edición prémium	Edición WTP	Seguridad de contenedores
Malicious File Detection	● Supervise los comportamientos de los procesos del usuario en tiempo real para detectar shells inversos causados por conexiones no válidas. ● Detecte acciones en shells anormales, como mover, copiar y eliminar archivos de shell, y modificar los permisos de acceso y los enlaces duros de los archivos.	Linux	×	√	√	√
Abnormal process behaviors	Todos los procesos en ejecución en todos sus servidores son monitoreados por usted. Puede crear una lista blanca de procesos para ignorar las alarmas en procesos de confianza y puede recibir alarmas sobre comportamientos e intrusiones de procesos no autorizados.	Linux	×	√	√	√
Root privilege escalation	Detecte la escalada de privilegios para procesos y archivos en el sistema actual.	Linux	×	√	√	√

Comprobación de la lista de grupos de políticas

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Figura 7-1 Acceso a HSS



Paso 3 En el árbol de navegación de la izquierda, elija **Security Operations** > **Policies** para comprobar los grupos de políticas mostrados. Para obtener más información, consulte **Tabla 7-1**.

NOTA

- **tenant_linux_container_default_policy_group** es el grupo de políticas de Linux por defecto de la edición contenedora. Este grupo de políticas sólo se puede ver y no se puede copiar ni eliminar.
- **tenant_linux_enterprise_default_policy_group** es el grupo de políticas de Linux predeterminado de la edición de empresa. Este grupo de políticas sólo se puede ver y no se puede copiar ni eliminar.
- **tenant_windows_enterprise_default_policy_group** es el grupo de políticas de Windows predeterminado de la edición de empresa. Este grupo de políticas sólo se puede ver y no se puede copiar ni eliminar.
- **tenant_linux_premium_default_policy_group** es el grupo de políticas de Linux predeterminado de la edición premium. Puede crear un grupo de políticas copiando este grupo predeterminado y modificando la copia.
- **tenant_windows_premium_default_policy_group** es el grupo de políticas de Windows predeterminado de la edición premium. Puede crear un grupo de políticas copiando este grupo predeterminado y modificando la copia.
- Para actualizar la lista, haga clic en en la esquina superior derecha.
- Para ver detalles acerca de los servidores asociados a un grupo de políticas, haga clic en el número de la columna **Servers** del grupo.

Tabla 7-1 Parámetros del grupo de políticas

Parámetro	Descripción
Policy Group	Nombre de un grupo de políticas
ID	ID único de un grupo de políticas
Description	Descripción de un grupo de políticas
Supported Version	Versión admitida por el grupo de políticas.

Paso 4 Haga clic en el nombre de un grupo de políticas para comprobar los detalles de las políticas, incluidos los nombres, los estados, las categorías de funciones y el tipo de sistema operativo de las políticas.

NOTA

- De forma predeterminada, todas las políticas de los grupos **tenant_enterprise_policy_group** y **tenant_premium_policy_group** están habilitadas.
- Puede hacer clic en **Enable** o **Disable** en la columna **Operation** de una política para controlar qué comprobar.

Paso 5 Haga clic en el nombre de una política para comprobar sus detalles.

NOTA

Para obtener más información sobre cómo modificar una política, consulte **Modificación de una política**.

----Fin

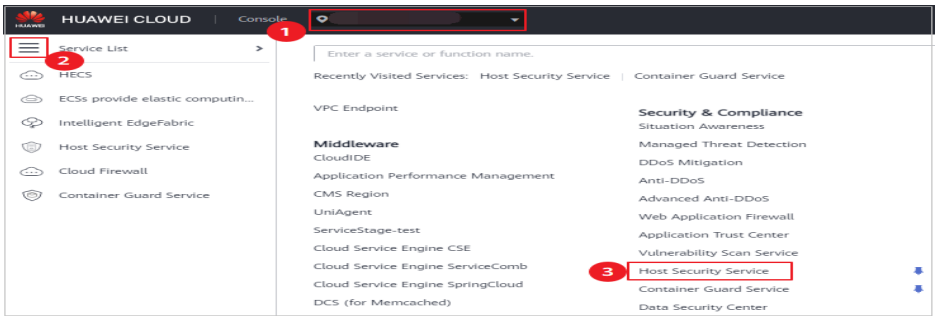
7.1.2 Creación de un grupo de políticas

Creación de un grupo de políticas

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Figura 7-2 Acceso a HSS



Paso 3 En el árbol de navegación de la izquierda, elija **Security Operations** > **Policies** para comprobar los grupos de políticas mostrados. Para obtener más información, consulte **Tabla 7-2**.

NOTA

- **tenant_linux_container_default_policy_group** es el grupo de políticas de Linux por defecto de la edición contenedora. Este grupo de políticas sólo se puede ver y no se puede copiar ni eliminar.
- **tenant_linux_enterprise_default_policy_group** es el grupo de políticas de Linux predeterminado de la edición de empresa. Este grupo de políticas sólo se puede ver y no se puede copiar ni eliminar.
- **tenant_windows_enterprise_default_policy_group** es el grupo de políticas de Windows predeterminado de la edición de empresa. Este grupo de políticas sólo se puede ver y no se puede copiar ni eliminar.
- **tenant_linux_premium_default_policy_group** es el grupo de políticas de Linux predeterminado de la edición premium. Puede crear un grupo de políticas copiando este grupo predeterminado y modificando la copia.
- **tenant_windows_premium_default_policy_group** es el grupo de políticas de Windows predeterminado de la edición premium. Puede crear un grupo de políticas copiando este grupo predeterminado y modificando la copia.
- Para actualizar la lista, haga clic en  en la esquina superior derecha.
- Para ver detalles acerca de los servidores asociados a un grupo de políticas, haga clic en el número de la columna **Servers** del grupo.

Tabla 7-2 Parámetros del grupo de políticas

Parámetro	Descripción
Policy Group	Nombre de un grupo de políticas
ID	ID único de un grupo de políticas
Description	Descripción de un grupo de políticas
Supported Version	Versión admitida por el grupo de políticas.

Paso 4 Seleccione el grupo de políticas **tenant_linux_premium_default_policy_group**. Busque la fila en la que reside este grupo de políticas, haga clic en **Copy** en la columna **Operation.**

Paso 5 En el cuadro de diálogo que se muestra, escriba el nombre y la descripción de un grupo de políticas y haga clic en **OK**.

NOTA

- El nombre de un grupo de políticas debe ser único o no se creará el grupo.
- El nombre del grupo de políticas y su descripción pueden contener sólo letras, dígitos, guiones bajos (_), guiones (-) y espacios, y no pueden comenzar o terminar con un espacio.

Paso 6 Haga clic en **OK**.

Paso 7 Haga clic en el nombre del grupo de políticas que acaba de crear. Se mostrarán las políticas del grupo.

Paso 8 Haga clic en un nombre de política y modifique su configuración según sea necesario. Para más detalles, consulte **Modificación de una política**.

Paso 9 Habilite o deshabilite la política haciendo clic en el botón correspondiente en la columna **Operation**.

----Fin

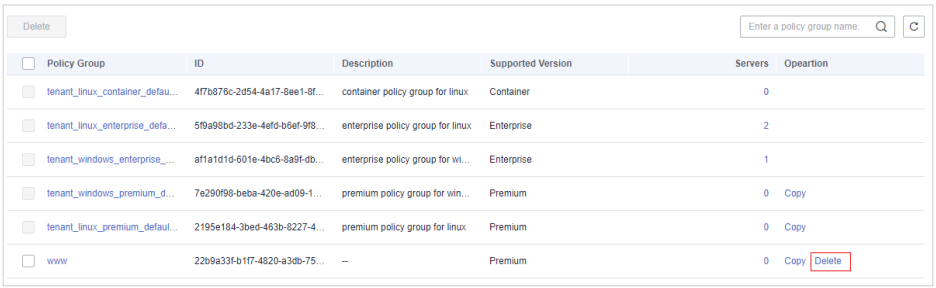
Operaciones de seguimiento

Supresión de un grupo de políticas

Después de eliminar un grupo de políticas, la columna **Policy Group** de los servidores asociados al grupo estará en blanco.

Paso 1 , como se muestra en **Figura 7-3**. En la página que se muestra, puede eliminar una política o varias políticas en lotes.

Figura 7-3 Supresión de grupos de políticas



NOTA

Puede hacer clic en **Delete** en la columna **Operation** de un grupo de políticas para eliminarlo.

También puede seleccionar varios grupos de políticas y hacer clic en **Delete** encima de la lista para eliminarlos por lotes.

Paso 2 En el cuadro de diálogo mostrado, haga clic en **OK**.

----Fin

7.1.3 Modificación de una política

Puede modificar políticas en un grupo de políticas.

AVISO

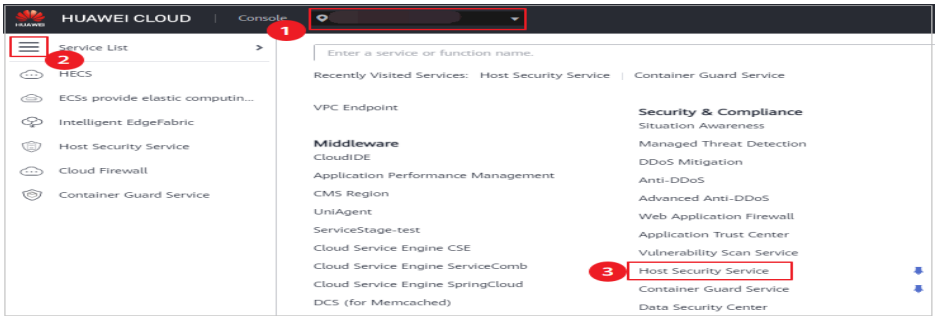
Las modificaciones de una política sólo tienen efecto en el grupo al que pertenece.

Acceso a la página Policies

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Figura 7-4 Acceso a HSS



Paso 3 En el árbol de navegación de la izquierda, elija **Security Operations** > **Policies**

Paso 4 Haga clic en el nombre del grupo de políticas para acceder a la lista de detalles de políticas, como se muestra en **Figura 7-5**. Puede modificar la política haciendo clic en su nombre.

Figura 7-5 Lista de detalles de políticas

Policy	Status	Category	OS	Opeartion
Asset Discovery	Enabled	Asset management	Linux	Disabled
Configuration Check	Enabled	Unsafe settings	Linux	Disabled
Weak Password Detection	Enabled	Unsafe settings	Linux	Disabled
Web Shell Detection	Enabled	Intrusion detection	Linux	Disabled
File Protection	Enabled	Intrusion detection	Linux	Disabled
Login Security Check	Enabled	Intrusion detection	Linux	Disabled
Malicious File Detection	Enabled	Intrusion detection	Linux	Disabled
Abnormal process behaviors	Enabled	Intrusion detection	Linux	Disabled
Root privilege escalation	Enabled	Intrusion detection	Linux	Disabled
Real-time Process	Enabled	Intrusion detection	Linux	Disabled

----Fin

Descubrimiento de activos

Paso 1 Haga clic en **Asset Discovery**.

Paso 2 En la página mostrada, modifique la configuración según sea necesario. Para obtener más información, consulte **Tabla 7-3**.

Tabla 7-3 Descripción del parámetro

Parámetro	Descripción
Startup Item Check Interval (s)	Intervalo entre dos comprobaciones consecutivas de elementos de inicio. El rango de valores es de 0 a 86,400s.
Software Scanned	● Nombre del software. Un nombre puede contener un máximo de 5,000 caracteres sin espacio. Utilice comas (,) para separar los nombres de software. ● Si no se especifica este parámetro, la información sobre todo el software instalado se recuperará como su valor.
WiseEye Account Change Time Threshold (min)	Límite de tiempo para cambiar la cuenta WiseEye. El rango de valores es de 1 a 10 minutos.
Software Scanned	Ruta de búsqueda de software. Este parámetro no es necesario para un servidor Windows.
Obtain Account Information	Obtiene información de cuenta. ●  : habilitar ●  : deshabilitar
Obtain LDAP Account Information	Obtiene información de cuenta LDAP. ●  : habilitar ●  : deshabilitar
Check Web Directory	Comprueba las rutas web. ●  : habilitar ●  : deshabilitar
Main Applications/ Components	● **Software Name** ● **Software Main Program** ● **Execute Command** ● **Operation**: Puede hacer clic en **Add** o **Remove** para modificar las operaciones.
Obtain UDP Port	Obtiene información del puerto UDP y comprueba los directorios web. ●  : habilitar ●  : deshabilitar
Port Information Check Interval (s)	Intervalo entre dos comprobaciones consecutivas de puerto. El rango de valores es de 30s a 86,400s.

Parámetro	Descripción
Obtain TCP Connection Information	Obtiene información de puerto UDP. ●  : habilitar ●  : deshabilitar
Ignored Processes	Procesos ignorados

Paso 3 Seleccione **Custom Baseline** o haga clic en **Add** en **Key System Configuration Collection** para agregar una tarea de recopilación de configuración del sistema.

Paso 4 Haga clic en **OK**.

----Fin

Escaneo de contraseña débil

Las contraseñas débiles no se atribuyen a cierto tipo de vulnerabilidades, pero no conllevan menos riesgos de seguridad que cualquier tipo de vulnerabilidad. Los datos y programas se volverán inseguros si sus contraseñas son descifradas.

El servicio HSS detecta de forma proactiva las cuentas utilizando contraseñas débiles y genera alarmas para las cuentas. También puede agregar una contraseña que se haya filtrado a la lista de contraseñas débiles para evitar que las cuentas de servidor usen la contraseña.

Paso 1 En la lista de grupos de políticas, haga clic en **Weak Password Detection**.

Paso 2 En el área **Policy Details**, modifique la configuración según sea necesario. Para obtener más información, consulte **Tabla 7-4**.

Tabla 7-4 Descripción del parámetro

Parámetro	Descripción
URL of Weak Password Dictionary	URL del sitio web del que recibe actualizaciones el diccionario de contraseñas débiles
Weak Password Dictionary SHA256	SHA256 del diccionario de contraseñas débiles
Scan Time	Punto de tiempo en el que se realizan las detecciones. Puede ser preciso al minuto.
Random Deviation Time (s)	Tiempo de desviación aleatoria de la contraseña débil. El rango de valores es de 30 a 86,400s.
Scan Days	Días en una semana en que se analizan las contraseñas débiles. Puede seleccionar uno o más días.

Parámetro	Descripción
Detection Break Time (ms)	Intervalo entre las comprobaciones de una sola contraseña débil. El rango de valores es de 0 a 2,000 ms.
User-defined Weak Passwords	Puede agregar una contraseña que se haya filtrado a este cuadro de texto de contraseña débil para evitar que las cuentas de servidor usen la contraseña.
Use Basic Weak Password Dictionary	Habilita el diccionario de contraseñas débiles. ●  : habilitar ●  : deshabilitar
Mask Weak Password	Enmascarar contraseñas débiles. Puede desactivarlo si lo encuentra innecesario.
Report Weak Password Hashes	Puede activar o desactivar esta función según sea necesario.

Paso 3 Confirme la información y haga clic en **OK**.

----Fin

Comprobación de configuración

Paso 1 Haga clic en **Configuration Check**.

Paso 2 En la página mostrada, modifique la configuración según sea necesario. Para obtener más información, consulte **Tabla 7-5**.

Tabla 7-5 Descripción del parámetro

Parámetro	Descripción
Scan Time	Punto de tiempo en el que se realizan las detecciones. Puede ser preciso al minuto.
Random Deviation Time (Seconds)	Tiempo de desviación aleatoria de la detección del sistema. El rango de valores es de 30 a 86,400s.
Scan Days	Día en una semana cuando se realiza una detección. Puede seleccionar cualquier día de lunes a domingo.

Paso 3 Seleccione la línea de base que se va a detectar o personalice una línea de base.

Paso 4 Haga clic en **OK**.

----Fin

Detección de Web Shell

Paso 1 En la lista de grupos de políticas, haga clic en el nombre del grupo que contiene la política de destino.

Paso 2 Haga clic en **Web Shell Detection**.

Paso 3 En la página **Web Shell Detection**, modifique la configuración según sea necesario. Para obtener más información, consulte **Tabla 7-6**.

Tabla 7-6 Descripción del parámetro

Parámetro	Descripción
Scan Time	Punto de tiempo en el que se realizan las detecciones. Puede ser preciso al minuto.
Random Deviation Time (Seconds)	Tiempo de desviación aleatorio. El rango de valores es de 30 a 86,400s.
Scan Days	Días en una semana en que se escanean web shells. Puede seleccionar uno o más días.
User-defined Scan Paths	Rutas web que se analizarán. Una ruta de archivo debe: ● Comienza con una barra (/) y termina sin barras (/). ● Termina con un número de puerto. ● Ocupar una línea independiente y no puede contener espacios.
Important System Paths	Ruta de exploración predeterminada. ● Comienza con una barra (/) y termina sin barras (/). ● Termina con un número de puerto. ● Ocupar una línea independiente y no puede contener espacios.
Monitor File Modification	Supervisa las modificaciones de los archivos. ●  : habilitar ●  : deshabilitar
Monitored Files Types	Extensiones de archivos a comprobar. Los valores válidos incluyen **jsp**, **jspx**, **jspf**, **php**, **php5**, **php4**.
Max. Scanned File Size (KB):	Tamaño máximo de un archivo que se va a analizar. El rango de valores es de 1,048,576 a 10,727,418,240.
Max. Files Uploaded Per Day	Número máximo de archivos cargados por día. El rango de valores es de 0 a 1,000.

Paso 4 Haga clic en **OK**.

----Fin

Protección de archivos

Paso 1 Haga clic en **File Protection**.

Paso 2 En la página **File Protection**, modifique la política. Para obtener más información, consulte **Tabla 7-7**.

Tabla 7-7 Descripción del parámetro

Parámetro	Descripción
File Privilege Escalation	● Detecta la escalada de privilegios. –  : habilitar –  : deshabilitar ● **Ignored File Paths**: ruta de acceso del archivo ignorado.
File Integrity	● Detecta la integridad de los archivos clave. –  : habilitar –  : deshabilitar ● **Full Scan Interval (s)**: intervalo entre dos detecciones completas. El rango de valores es de 3,600 a 86,400s. ● **File Paths**: Configure las rutas de archivo.

Parámetro	Descripción
Important File Directory Change	● Detecta el cambio de directorio de archivos clave. –  : habilitar –  : deshabilitar ● **Enable Audit**: habilita la función de detección de auditoría. Si la función está habilitada y el uso de inotify excede el límite, no se pueden detectar algunos cambios en el directorio de archivos. –  : habilitar –  : deshabilitar ● **Session IP Whitelist**: Si el proceso de archivos pertenece a las sesiones de las direcciones IP enumeradas, no se aplica ninguna auditoría. ● **Unmonitored File Types**: Tipos de archivo que no necesitan ser monitoreados. ● **Unmonitored File Paths**: Rutas de archivos que no necesitan ser supervisadas. ● **Monitoring Login Keys**: permite la función de monitorización de claves de inicio de sesión. –  : habilitar –  : deshabilitar

Paso 3 Haga clic en **OK**.

----Fin

Comprobación de seguridad de inicio de sesión

Paso 1 Haga clic en **Login Security Check**.

Paso 2 En la página mostrada, modifique la configuración según sea necesario. Para obtener más información, consulte **Tabla 7-8**.

Tabla 7-8 Descripción del parámetro

Parámetro	Descripción
Block Attacking IP Address	Después de activar la función de bloqueo de direcciones IP atacantes, HSS bloquea los inicios de sesión de direcciones IP de fuerza bruta. El agente modifica las configuraciones del sistema para bloquear las direcciones IP de origen de los ataques de craqueo de cuentas.

Parámetro	Descripción
Lock Time (Min.)	Puede determinar cuántos minutos están bloqueados los ataques de fuerza bruta. El rango de valores es de 1 a 43,200 min.
Log Detection Period (s)	Intervalo para comprobar los registros. El rango de valores es de 5 a 3,600s.
Cracking Behavior Determination Threshold (s)	Este parámetro se utiliza junto con **Cracking Behavior Determination Threshold (Login Attempts)**. El rango de valores es de 1 a 10s. Por ejemplo, si este parámetro se establece en **30** y **Cracking Behavior Determination Threshold (Login Attempts)** se establece en **5**, el sistema determina que una cuenta está agrietada cuando la misma dirección IP no puede iniciar sesión en el sistema durante cinco veces en 30 segundos.
Cracking Behavior Determination Threshold (Login Attempts)	Este parámetro se utiliza junto con **Cracking Behavior Determination Threshold**. El intervalo de valores es de 1 a 36,000.
Threshold for slow brute force attack (second)	Este parámetro se utiliza junto con **Threshold for slow brute force attack (failed login attempt)**. El rango de valores es de 600 a 86,400s. Por ejemplo, si este parámetro se establece en **3,600** y **Threshold for slow brute force attack (failed login attempt)** se establece en **15**, el sistema determina que una cuenta está descifrada cuando la misma dirección IP no puede iniciar sesión en el sistema durante quince veces en 3,600 segundos.
Threshold for slow brute force attack (failed login attempt)	Este parámetro se utiliza junto con **Threshold for slow brute force attack (second)**. El rango de valores es de 6 a 100.
Alarm Consolidation Time (s)	El tiempo especificado durante el cual las alarmas se consolidan y notifican. El rango de valores es de 30 a 600s. Por ejemplo, si este parámetro se establece en **60**, las alarmas generadas en 60 segundos se consolidarán e informarán.
Cracking Behavior Determination Release Time (s)	Intervalo para borrar los registros de fallas de inicio de sesión generados debido a grietas. El rango de valores es de 60 a 86,400s.
MySQL Check Interval (s)	Intervalo para comprobar la base de datos MySQL. El rango de valores es de 60 a 86,400.
FTP Check Interval (s)	Intervalo para comprobar la conexión FTP. El rango de valores es de 60 a 86,400s.
SSH Check Interval (s)	Intervalo para las comprobaciones SSH. El rango de valores es de 60 a 86,400s.
Brute-force Prevention Whitelist	Las direcciones IP incluidas en la lista blanca no activarán alarmas de ataque de fuerza bruta ni serán bloqueadas.

Parámetro	Descripción
Check Whether the Audit Login Is Successful	● Después de habilitar esta función, HSS informa de los registros de éxito de inicio de sesión. –  : habilitar –  : deshabilitar
Classifying Login Success Events by Minute	Después de activar esta función, HSS informa los eventos de éxito de inicio de sesión por minuto. ●  : habilitar ●  : deshabilitar
Ignore Certificate Login Success	Después de activar esta función, HSS informa de que el inicio de sesión del certificado se ha realizado correctamente. ●  : habilitar ●  : deshabilitar
Ignore Local Logins	Una vez habilitada esta función, no se comprobarán los inicios de sesión locales. ●  : habilitar ●  : deshabilitar
IP Whitelisting	Una vez habilitada esta función, solo las direcciones IP de la lista blanca pueden iniciar sesión en hosts en la nube. ●  : habilitar ●  : deshabilitar
Clear Login Failure History After a Successful Login	Borra los registros de error de inicio de sesión anteriores después de un inicio de sesión exitoso. ●  : habilitar ●  : deshabilitar
Stop DenyHosts	Una vez activada esta función, las DenyHosts se desactivarán. ●  : habilitar ●  : deshabilitar
Allowed Login Software	Software de inicio de sesión permitido.

Parámetro	Descripción
Supported Database Software	Software de base de datos compatible.
Supported FTP Software	Software FTP soportado.

Paso 3 Haga clic en **OK**.

----Fin

Detección de archivos maliciosos

Paso 1 Haga clic en **Malicious File Detection**.

Paso 2 En la página mostrada, modifique la política. Para obtener más información, consulte **Tabla 7-9**.

Tabla 7-9 Descripción del parámetro

Parámetro	Descripción
Whitelist Paths in Reverse Shell Check	Ruta del archivo de proceso que se ignorará en la detección de shell inversa
Reverse Shell Scanning Interval (s):	Período de escaneo de shell inverso. El rango de valores es de 30 a 86,400.
Audit detection enhancement	Mejora la detección de auditoría. Se recomienda activar esta función.
Max. open files per process	Número máximo de archivos que un proceso puede abrir. El rango de valores es de 10 a 300,000.
Detect Reverse Shells	● Detecta shells inversos. Se recomienda habilitar esta opción. –  : habilitar –  : deshabilitar
Abnormal Shell Detection	● Detecta proyectiles anormales. Se recomienda habilitar esta opción. –  : habilitar –  : deshabilitar

Paso 3 Haga clic en **OK**.

----Fin

Comportamiento de procesos anormales

Paso 1 Haga clic en **Abnormal Process behaviors**.

Paso 2 En el área mostrada, modifique la configuración según sea necesario. Para obtener más información, consulte **Tabla 7-10**.

Tabla 7-10 Descripción del parámetro

Parámetro	Descripción
Detection and Scanning Cycle (Seconds)	Intervalo para comprobar los programas en ejecución en el host. El rango de valores es de 30 a 1,800.
IP Address Blacklist	Introduzca direcciones IP negras. Cada dirección IP ocupa una línea. Ejemplos: 192.1.2.3 192.168.4.5
Ignored File Paths	Ruta de acceso del archivo que no es necesario comprobar.
High CPU Check Threshold (%)	El intervalo de valores es del 80 al 400%.
Check Strings File Maximum Size (MB)	Comprueba el tamaño máximo de los archivos de cadenas.
Strings Check Keywords	Introduzca una palabra clave en cada línea (hasta 50 caracteres). No se permiten líneas que contengan sólo espacios.
Threshold for Score Reporting	Umbral de informe de puntuación. El rango de valores es de 10 a 100.

Paso 3 Haga clic en **OK**.

----Fin

Detección de escalada de privilegios de root

Paso 1 Haga clic en **Root privilege escalation**.

Paso 2 En el área mostrada, modifique la configuración según sea necesario. Para obtener más información, consulte **Tabla 7-11**.

Tabla 7-11 Descripción del parámetro

Parámetro	Descripción
Ignored Process File Path	Ruta del archivo de proceso ignorada

Parámetro	Descripción
Scanning Interval (s)	Intervalo para comprobar archivos de proceso. El rango de valores es de 5 a 3,600s.
SUID Process Privilege Escalation	Detecta la escalada de privilegios de proceso SUID. Se recomienda habilitar esta opción. ●  : habilitar ●  : deshabilitar

Paso 3 Haga clic en **OK**.

----Fin

Proceso en tiempo real

Paso 1 Haga clic en **Real-time Process**.

Paso 2 En la página mostrada, modifique la configuración según sea necesario. Para obtener más información, consulte **Tabla 7-12**.

Tabla 7-12 Parámetros para la configuración de políticas de procesos en tiempo real

Parámetro	Descripción
Full Process Report Interval (s)	Intervalo para reportar todo el proceso. El rango de valores es de 3,600 a 86,400.
High-Risk Commands	Comandos de alto riesgo que contienen palabras clave durante la detección.
Lista blanca (No grabar registros)	Agregue rutas de acceso o nombres de programa permitidos o ignorados durante la detección.

Paso 3 Haga clic en **OK**.

----Fin

8 Informe de seguridad

8.1 Comprobación de un informe de seguridad

Puede suscribirse a informes **diarios**, semanales, mensuales y **personalizados**, que se almacenan durante seis meses. Los informes muestran las tendencias de seguridad del servidor y los principales eventos y riesgos de seguridad.

NOTA

- Si ha habilitado la función de proyecto de empresa, puede seleccionar su proyecto de empresa en la lista desplegable **Enterprise project** y suscribirse al informe de seguridad del proyecto. También puede seleccionar **All projects** y suscribirse al informe de seguridad de los servidores de todos los proyectos de esta región.
- Después de suscribirse a un informe, estará disponible para su revisión y descarga al día siguiente.

Descripción general del informe de seguridad

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, elija **Reports**. Se muestra la página de descripción general del informe de seguridad.

Puede utilizar plantillas de informe de seguridad predeterminadas directamente, que son **default monthly security report** y **default weekly security report**.

Paso 4 Haga clic en **Download** para ir a la página de vista previa. Puede consultar la información del informe de destino y descargarlo.

----Fin

Comprobación del historial de informes

El historial del informe almacena los detalles de envío del informe.

Paso 1 En la parte central superior de la página de descripción general del informe de seguridad, haga clic en **Report History** para comprobar los registros de envío del informe.

Paso 2 Compruebe el historial de informes en la página mostrada, como se muestra en la siguiente imagen. Para obtener más información, consulte los parámetros relacionados que se enumeran a continuación.

Tabla 8-1 Descripción del parámetro

Parámetro	Descripción
Report Name	Nombre de un informe enviado.
Statistical Period	Periodo estadístico de un informe enviado.
Report Type	Tipo de período estadístico de un informe enviado. ● Reportes semanales ● Reportes mensuales
Sent	Hora en que se envía el informe.

Paso 3 Haga clic en **Download** en la columna **Operation** para comprobar los informes históricos. También puede obtener una vista previa y descargar los informes.

----Fin

8.2 Suscribirse a un informe de seguridad

Esta sección proporciona instrucciones para que pueda suscribirse rápidamente a informes de seguridad semanales o mensuales utilizando plantillas preestablecidas en la consola. Para obtener información sobre cómo personalizar un informe de seguridad, consulte **Creación de un informe de seguridad**.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, elija **Reports**. Se muestra la página de descripción general del informe de seguridad.

Puede utilizar plantillas de informe de seguridad predeterminadas directamente, que son **default monthly security report** y **default weekly security report**.

Paso 4 Puede activar la suscripción al informe de seguridad mensual o semanal haciendo clic en el icono de conmutador correspondiente  . Para obtener más información sobre cómo editar un informe, consulte **Edición de un informe**.

----Fin

8.3 Creación de un informe de seguridad

Si el tipo y el contenido de la plantilla de informe existente no pueden cumplir los requisitos para suscribirse a informes de seguridad, puede personalizar el informe consultando esta sección.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en ☰, y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, elija **Reports**. Se muestra la página de descripción general del informe de seguridad.

Puede utilizar plantillas de informe de seguridad predeterminadas directamente, que son **default monthly security report** y **default weekly security report**.

Paso 4 Crear un informe.

- Cree un informe de seguridad mensual o semanal basado en plantillas.
  - Haga clic en **Copy** resaltado en el cuadro rojo, como se muestra en la imagen siguiente, para acceder a la página de configuración de información básica.
- Personalizar un informe
  - Haga clic en **Create Report** para acceder a la página de configuración de información básica.

Paso 5 Edite la información básica de un informe. Para obtener más información, consulte **Tabla 8-2**.

Tabla 8-2 Descripción del parámetro

Parámetro	Descripción	Valor de ejemplo
Report Name	Nombre de informe predeterminado	ecs security report
Report Type	Periodo estadístico tipo de informe: ● **Daily**: 00:00 a 24:00 todos los días ● **Weekly Reports**: 00:00 el lunes a 24:00 el domingo ● **Monthly Reports**: 00:00 en el primer día de cada mes a 24:00 en el último día ● **Custom**: período estadístico personalizado, que varía de un día a tres meses	**Monthly Reports**
Schedule Delivery	Hora en que se envía automáticamente un informe	-

Parámetro	Descripción	Valor de ejemplo
Send Report To	Modo para enviar los informes de seguridad generados: ● **Recipients specified in Message Center**: si utiliza la configuración del Centro de mensajes, las notificaciones de alarma se enviarán a los destinatarios especificados en el tipo de mensaje **Security events**. Debe iniciar sesión en la consola y comprobar el buzón en la esquina superior derecha. ● **Recipients specified in SMN topic**: Si utiliza la configuración del tema SMN, puede crear un tema y especificar destinatarios para HSS.	Message Center Settings

Paso 6 Después de confirmar que la información es correcta, haga clic en **Next** en la esquina inferior derecha de la página para configurar el informe.

Paso 7 Seleccione los elementos de informe que se generarán en el panel izquierdo. Puede obtener una vista previa de los elementos del informe en el panel derecho. Después de confirmar los elementos del informe, haga clic en **Save** y habilite la suscripción al informe de seguridad.

----Fin

8.4 Gestión de un informe de seguridad

Esta sección proporciona instrucciones para modificar, cancelar o deshabilitar un informe suscrito.

Edición de un informe

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, elija **Reports**. Se muestra la página de descripción general del informe de seguridad.

- Puede utilizar plantillas de informe de seguridad predeterminadas directamente, que son **default monthly security report** y **default weekly security report**.

Paso 4 Haga clic en **Edit** en la esquina inferior derecha del informe de destino.

Paso 5 Edite la información básica de un informe. Para obtener más información, consulte **Tabla 8-3**.

Tabla 8-3 Descripción del parámetro

Parámetro	Descripción	Valor de ejemplo
Report Name	Nombre predeterminado del informe.	**default monthly security report**

Parámetro	Descripción	Valor de ejemplo
Report Type	Nombre del tipo de período estadístico de un informe, que no se puede editar.	**Monthly Reports**
Schedule Delivery	Hora en que se envía automáticamente un informe.	-
Send Report To	Modo para enviar los informes de seguridad generados: ● **Recipients specified in Message Center**: si utiliza la configuración del Centro de mensajes, las notificaciones de alarma se enviarán a los destinatarios especificados en el tipo de mensaje **Security events**. Debe iniciar sesión en la consola y comprobar el buzón en la esquina superior derecha. ● **Recipients specified in SMN topic**: Si utiliza la configuración del tema SMN, puede crear un tema y especificar destinatarios para HSS.	Message Center Settings

Paso 6 Confirme la información y haga clic en **Next** en la esquina inferior derecha de la página para configurar el informe.

Paso 7 Seleccione o anule la selección de los elementos de informe que se van a generar en el panel izquierdo. Puede obtener una vista previa de los elementos del informe en el panel derecho. Después de confirmar los elementos del informe, haga clic en **Save**. El informe se ha cambiado correctamente.

----Fin

Cancelar la suscripción de un informe

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, elija **Reports**. Se muestra la página de descripción general del informe de seguridad.

- Puede utilizar plantillas de informe de seguridad predeterminadas directamente, que son **default monthly security report** y **default weekly security report**.

Paso 4 Desactiva el informe de destino, como se muestra en  .

----Fin

Eliminación de un informe

NOTA

Las plantillas de informe de seguridad predeterminadas **default monthly security report** and **default weekly security report** no se pueden eliminar.

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación de la izquierda, elija **Reports**. Se muestra la página de descripción general del informe de seguridad.

- Puede utilizar plantillas de informe de seguridad predeterminadas directamente, que son **default monthly security report** y **default weekly security report**.

Paso 4 Haga clic en **Delete** en la esquina inferior derecha del informe de destino para eliminar el informe.

----Fin

9 Instalación & Configuración

9.1 Gestión de Agentes

9.1.1 Comprobación de agentes

Puede ordenar los servidores, comprobar si el agente está instalado en ellos y puede instalar o desinstalar el agente. En la consola, puede encontrar las instrucciones de instalación del agente y el enlace al paquete del agente.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en  , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Installation & Configuration**. Haga clic en la pestaña **Agents**.

Paso 4 Haga clic en **Offline** para comprobar los servidores donde el agente no está instalado o está sin conexión. Haga clic en **Online** para comprobar los servidores donde está conectado el agente.

Paso 5 (Opcional) Haga clic en **Installation Guide** para consultar la guía para instalar el agente.

----Fin

9.1.2 Instalación de un agente

Instalar el agente en un servidor. Solo entonces el servidor puede ser protegido por HSS.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Installation & Configuration**. Haga clic en la pestaña **Agents**.

Paso 4 Haga clic en **Offline** para comprobar los servidores donde el agente no está instalado o está sin conexión. La tabla siguiente describe los parámetros.

Tabla 9-1 Parámetros del agente sin conexión

Parámetro	Descripción
Server Name/ID	Nombre e ID del servidor
IP Address	EIP o dirección IP privada de un servidor
OS	Sistema operativo del servidor. Su valor puede ser: ● **Linux** ● **Windows**
Agent Status	Estado del agente de un servidor. Su valor puede ser: ● **Offline** ● **Not installed**

Paso 5 Haga clic en **View Cause** en la columna **Operation** de un servidor para comprobar por qué un agente está sin conexión.

Paso 6 Haga clic en **Install Agent** en la columna **Operation**. Descargue el paquete de agente adecuado para su arquitectura de servidor y sistema operativo. Para obtener más información sobre cómo instalar el agente en un servidor Linux, consulte **Instalación de un agente en el sistema operativo Linux**. Para obtener más información acerca de cómo instalar el agente en un servidor Windows, consulte **Instalación de un agente en el sistema operativo Windows**.

----Fin

9.1.3 Desinstalación de un agente

Puede desinstalar el agente de un servidor. El servidor no estará protegido por HSS después de desinstalar el agente.

Procedimiento

Paso 1 **Iniciar sesión en la consola de gestión**.

Paso 2 En la esquina superior izquierda de la página, seleccione una región, haga clic en , y elija **Security & Compliance** > **Host Security Service (New)**.

Paso 3 En el panel de navegación, elija **Installation & Configuration**. Haga clic en la pestaña **Agents**.

Paso 4 Haga clic en **Offline** para comprobar los servidores donde está conectado el agente. La tabla siguiente describe los parámetros.

Tabla 9-2 Parámetros del agente en línea

Parámetro	Descripción
Server Name/ID	Nombre e ID del servidor
IP Address	EIP o dirección IP privada de un servidor
OS	Sistema operativo del servidor. Su valor puede ser: ● **Linux** ● **Windows**
Agent Status	Estado del agente de un servidor. Su valor puede ser: ● **Offline** ● **Online**

Paso 5 Haga clic en **Uninstall Agent** en la columna **Operation** de un servidor. En el cuadro de diálogo que aparece, confirme la información de desinstalación y haga clic en **OK**.

----Fin

9.2 Configuraciones de seguridad

Puede agregar ubicaciones de inicio de sesión comunes, direcciones IP comunes y direcciones IP de lista blanca, y habilitar el aislamiento y la eliminación de programas maliciosos para mejorar la seguridad del servidor.

Para más detalles, consulte **Configuración de seguridad**.

10 Auditoría

10.1 Operaciones de HSS respaldadas por CTS

Cloud Trace Service (CTS) registra todas las operaciones en HSS, incluidas las solicitudes iniciadas desde la consola de gestión o las API abiertas y las respuestas a las solicitudes, para que los inquilinos puedan consultar, auditar y rastrear.

Tabla 10-1 enumera las operaciones de HSS registradas por CTS.

Tabla 10-1 Operaciones de HSS que pueden ser registradas por CTS

Operación	Tipo de recurso	Nombre del rastro
Dejar de ignorar un puerto	hss	notIgnorePortStatus
Ignorar un puerto	hss	ignorePortStatus
Dejar de ignorar los elementos de comprobación de configuración	hss	notIgnoreCheckRuleStat
Ignorar elementos de comprobación de configuración	hss	ignoreCheckRuleStat
Realizar una comprobación de línea de base de nuevo	hss	runBaselineDetect
Desvinculación de cuota	hss	cancelHostsQuota
Deshabilitar la protección del contenedor	hss	closeContainerProtectStatus
Habilitación de la protección del contenedor	hss	openContainerProtectStatus
Desbloquear una dirección IP	hss	changeBlockedIp
Manejo de un evento	hss	changeEvent
Cancelar el aislamiento de un archivo	hss	changeIsolatedFile

Operación	Tipo de recurso	Nombre del rastro
Eliminacción de una alarma de la lista blanca	hss	removeAlarmWhiteList
Configuración de la lista blanca de inicio de sesión	hss	addLoginWhiteList
Eliminar información de inicio de sesión de la lista blanca de inicio de sesión	hss	removeLoginWhiteList
Adición de un grupo de servidores	hss	addHostsGroup
Adición de servidores a un grupo	hss	associateHostsGroup
Modificación de un grupo de servidores	HSS	changeHostsGroup
Eliminación de un grupo de servidores	HSS	deleteHostsGroup
Deshabilitación de HSS	hss	closeHostsProtectStatus
Habilitación de HSS	hss	openHostsProtectStatus
Desinstalación de un agente	hss	uninstallAgents
Escanear una imagen	hss	runImageScan
Sincronización de la lista de imágenes de SWR	hss	runImageSynchronizeTask
Actualización y escaneo de una imagen de SWR	hss	runSwrImageScan
Realizar una comprobación de seguridad de nuevo	hss	resetRiskScore
Agregar un grupo de políticas	hss	addPolicyGroup
Eliminación de un grupo de políticas	hss	deletePolicyGroup
Aplicación de un grupo de política	hss	deployPolicyGroup
Modificación de una política	hss	modifyPolicyDetail
Modificación de un grupo de políticas	hss	modifyPolicyGroup
Deshabilitación del aislamiento y la matanza automáticas	hss	closeAutoKillVirusStatus
Enabling automatic isolation and killing	hss	openAutoKillVirusStatus
Configurar direcciones IP de inicio de sesión comunes	hss	modifyLoginCommonIp

Operación	Tipo de recurso	Nombre del rastro
Configurar ubicaciones de inicio de sesión comunes	hss	modifyLoginCommonLocation
Configuración de la lista blanca de inicio de sesión SSH	hss	modifyLoginWhiteIp
Arreglar una vulnerabilidad	hss	changeVulStatus
Adición de un directorio protegido	hss	addHostProtectDirInfo
Adición de un proceso privilegiado	hss	addPrivilegedProcessInfo
Adición de una configuración de protección programada	hss	addTimingOffConfigInfo
Eliminación de un servidor de copia de respaldo remoto	hss	deleteBackupHostInfo
Eliminación de un directorio protegido	hss	deleteHostProtectDirInfo
Eliminación de un proceso privilegiado	hss	deletePrivilegedProcessInfo
Eliminación de la configuración de protección programada	hss	deleteTimingOffConfigInfo
Configuración del período de protección programado	hss	setDateOffConfigInfo
Modificación del estado de un directorio protegido	hss	setProtectDirSwitchInfo
Activación o desactivación de WTP dinámico	hss	setRaspSwitch
Configuración de un servidor de backup remoto	hss	setRemoteBackupInfo
Activación o desactivación de la protección programada	hss	setTimingOffSwitchInfo
Deshabilitación de WTP	hss	closeWtpProtectionStatusInfo
Habilitación de WTP	hss	openWtpProtectionStatusInfo
Modificación de un servidor de copia de respaldo remoto	hss	updateBackupHostInfo
Modificación de un directorio protegido	hss	updateHostProtectDirInfo
Modificación de un proceso privilegiado	hss	updatePrivilegedProcessInfo

Operación	Tipo de recurso	Nombre del rastro
Modificación del directorio bin de Tomcat	hss	updateRaspPathInfo
Modificación del período de protección programado	hss	updateTimingOffConfigInfo

10.2 Consulta de registros de auditoría

Después de habilitar CTS, el sistema inicia las operaciones de grabación en HSS. Los registros de operación de los últimos siete días se pueden ver en la consola CTS.

Consulta de un seguimiento HSS en la consola CTS

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en la parte superior de la página y elija **Cloud Trace Service** en **Management & Deployment**. Se muestra la consola CTS.

Paso 3 Elija **Trace List** en el panel de navegación.

Paso 4 Haga clic en **Filter** y especifique los criterios de filtrado según sea necesario. Los cuatro filtros siguientes están disponibles:

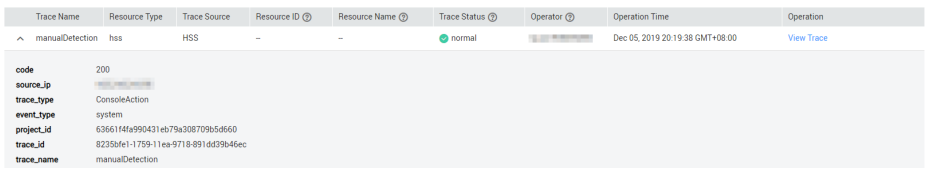
- **Trace Type**, **Trace Source**, **Resource Type**, y **Search By**.

  Seleccione el filtro de la lista desplegable.
  - Establezca **Trace Type** en **Management**.
  - Establezca **Trace Source** en **HSS**.
  - Cuando selecciona **Trace name** para **Search By** también debe seleccionar un nombre de seguimiento específico. Cuando selecciona **Resource ID** para **Search By** también debe seleccionar o ingresar un ID de recurso específico. Cuando selecciona **Resource name** para **Search By**, también debe seleccionar o ingresar un nombre de recurso específico.
- **Operator**: Seleccione un operador específico (un usuario que no sea inquilino).
- **Trace Rating**: las opciones disponibles incluyen **all trace status**, **normal**, **warning**, y **incident**. Solo se puede habilitar una de ellas.
- **Time Range**: En la esquina superior derecha de la página, puede consultar trazas en la última hora, el último día, la última semana o dentro de un período personalizado.

Paso 5 Haga clic en **Query**.

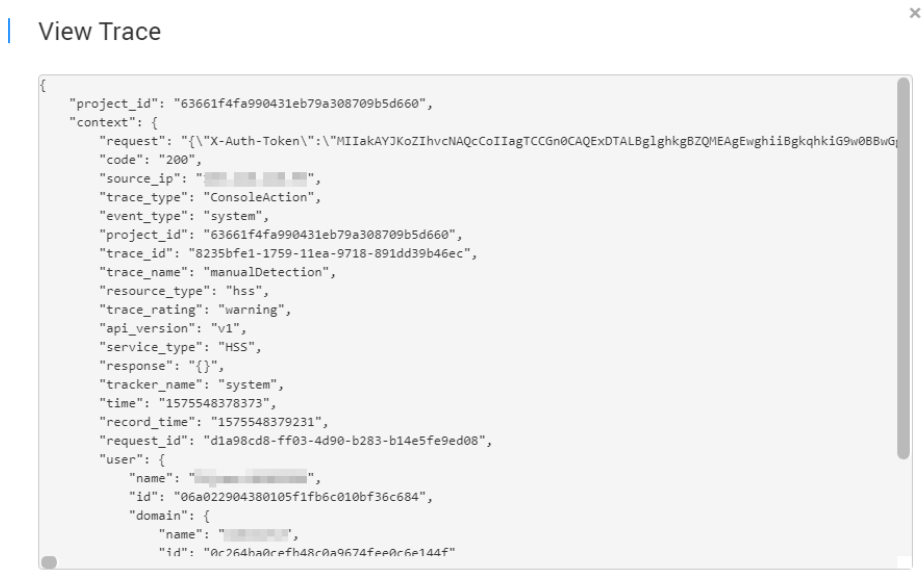
Paso 6 Haga clic en la izquierda de una traza para ampliar sus detalles, como se muestra en **Figura 10-1**.

Figura 10-1 Ampliación de los detalles de rastro



Paso 7 Haga clic en **View Trace** en la columna **Operation**. En el cuadro de diálogo **View Trace** que se muestra en **Figura 10-2**, se muestran los detalles de la estructura de trazado.

Figura 10-2 Consulta de una seguimiento



----Fin

11 Gestión de permisos

11.1 Creación de un usuario y concesión de permisos

En esta sección se describe la gestión detallada de permisos de IAM para sus recursos de HSS. Con **IAM**, usted puede:

- Crear usuarios de IAM para empleados en función de la estructura organizativa de su empresa. Cada usuario de IAM tiene sus propias credenciales de seguridad, lo que proporciona acceso a los recursos de HSS.
- Conceder sólo los permisos necesarios para que los usuarios realicen una tarea específica.
- Confíe una cuenta de Huawei cloud o un servicio en la nube para realizar operaciones profesionales y eficientes en sus recursos HSS.

Si su cuenta de Huawei Cloud no requiere usuarios individuales de IAM, omita este capítulo.

En esta sección se describe el procedimiento para conceder permisos (ver **Figura 11-1**).

Prerrequisitos

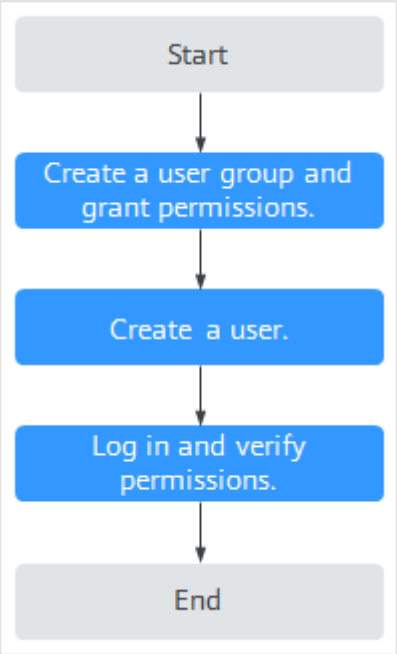
Antes de autorizar permisos para un grupo de usuarios, debe saber qué permisos HSS se pueden agregar al grupo de usuarios. **Tabla 11-1** describe los detalles de la política.

Tabla 11-1 Permisos definidos por el sistema admitidos por HSS

Nombre de rol/política	Descripción	Tipo	Dependencia
HSS Administrator	Administrador de HSS, que tiene todos los permisos de HSS.	Rol definido por el sistema	• Depende del rol de **Tenant Guest**. Tenant Guest: Un rol global, que debe asignarse en el proyecto global. • Para adquirir cuotas de protección HSS, debe tener los roles de **ECS ReadOnlyAccess** y **BSS Administrator** – **ECS ReadOnlyAccess**: permiso de acceso de solo lectura para el ECS. Esta es una política del sistema. – **BSS Administrator**: un rol de sistema, que es el administrador del centro de facturación (BSS) y tiene todos los permisos para el servicio.
HSS FullAccess	Todos los permisos de HSS	System-defined policy	Para adquirir cuotas de protección HSS, debe tener la función de **BSS Administrator**. **BSS Administrator**: un rol de sistema, que es el administrador del centro de facturación (BSS) y tiene todos los permisos para el servicio.
HSS ReadOnlyAccess	Permisos de sólo lectura para HSS	System-defined policy	Ninguno

Proceso de Autorización

Figura 11-1 Proceso de concesión de permisos



1. **Cree un grupo de usuarios y asigne permisos**. En la consola de IAM, conceda el permiso de **HSS Administrator**.
2. **Crear un usuario y agréguelo al grupo**. En la consola de IAM, agregue el usuario al grupo creado en **1**.
3. **Iniciar sesión** y verificar los permisos.

   Inicie sesión en la consola HSS como el usuario creado y compruebe que el usuario solo tiene permisos de lectura para HSS.

   En **Service List** en la consola de Huawei Cloud, seleccione cualquier otro servicio (por ejemplo, solo existe la política de **HSS Administrator**). Si se muestra un mensaje que indica que el permiso es insuficiente, el permiso **HSS Administrator** tiene efecto.

11.2 Políticas personalizadas de HSS

Se pueden crear políticas personalizadas para complementar las políticas definidas por el sistema de HSS. Para ver las acciones admitidas para las directivas personalizadas, consulte **Acciones de HSS**.

Puede crear políticas personalizadas mediante uno de los métodos siguientes:

- Editor visual: Seleccione servicios en la nube, acciones, recursos y condiciones de solicitud. No es necesario tener conocimiento de la sintaxis de la política.
- JSON: Cree una política en formato JSON o edite las cadenas JSON de una política existente.

Para obtener más información, consulte **Creación de una política personalizada**. La siguiente sección contiene ejemplos de políticas personalizadas comunes de HSS.

Ejemplo de políticas personalizadas

- Ejemplo 1: Permitir a los usuarios consultar la lista de servidores protegidos

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "hss:hosts:list"
                                                        ]
                }
        ]
}
```

- Ejemplo 2: Denegar la desinstalación del agente

  Una política de denegación debe usarse junto con otras políticas. Si las directivas asignadas a un usuario contienen tanto "Allow" como "Deny", los permisos "Deny" tienen prioridad sobre los permisos "Allow".

  Se puede utilizar el siguiente método si necesita asignar permisos de la política **HSS Administrator** a un usuario, pero también prohibir que el usuario elimine pares de claves (**hss:agent:uninstall**). Cree una política personalizada con la acción de eliminar pares de claves, establezca su **Effect** en **Deny** y asigne esta política y las políticas de **HSS Administrator** al grupo al que pertenece el usuario. Entonces el usuario puede realizar todas las operaciones en HSS excepto desinstalarlo. A continuación se muestra una política de ejemplo que niega la desinstalación del agente.

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Deny",
                        "Action": [

"hss:agent:uninstall"
                        ]
                },
        ]
}
```

- Políticas de acción múltiple

  Una política personalizada puede contener las acciones de varios servicios que son del tipo de proyecto. La siguiente es una política con varias sentencias:

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "hss:hosts:list"
                        ]
                },
               {
                        "Effect": "Allow",
                        "Action": [
                                "hss:hosts:switchVersion",
                                "hss:hosts:manualDetect",
                                "hss:manualDetectStatus:get"
                        ]
                }
        ]
}
```


11.3 Acciones de HSS

En esta sección se describe la gestión detallada de permisos para las instancias HSS. Si su cuenta de Huawei Cloud no necesita usuarios individuales de IAM, puede omitir esta sección.

De forma predeterminada, los nuevos usuarios de IAM no tienen ningún permiso asignado. Debe agregar un usuario a uno o más grupos y asignar políticas o roles a estos grupos. A continuación, el usuario hereda los permisos de los grupos de los que es miembro. Este proceso se llama autorización. Después de la autorización, el usuario puede realizar operaciones específicas en los servicios en la nube en función de los permisos.

Puede conceder permisos a los usuarios mediante **roles** y **políticas**. Los roles son proporcionados por IAM para definir permisos basados en servicios dependiendo de las responsabilidades del trabajo del usuario. IAM utiliza políticas para realizar una autorización detallada. Una política define los permisos necesarios para realizar operaciones en recursos específicos de la nube bajo ciertas condiciones.

Acciones admitidas

HSS proporciona políticas definidas por el sistema que se pueden usar directamente en IAM. También puede crear directivas personalizadas y utilizarlas para complementar las directivas definidas por el sistema, implementando un control de acceso más refinado. Los siguientes son conceptos relacionados:

- Permisos: Permitir o denegar ciertas operaciones.
- Acciones: Operaciones específicas que están permitidas o denegadas.
- Acciones dependientes: Al asignar permisos para una acción, también debe asignar permisos para las acciones dependientes.

HSS admite las siguientes acciones que se pueden definir en políticas personalizadas:

Acciones

Permiso	Acción	Acción relacionada
Consultar la lista de servidores protegidos	hss:hosts:list	vpc:ports:get vpc:publicIps:list ecs:cloudServers:list
Habilitar o deshabilitar la protección en servidores	hss:hosts:switchVersion	-
Escaneo manual	hss:hosts:manualDetect	-
Comprobar el estado de un análisis manual	hss:manualDetectStatus:get	-
Consultar informes de análisis de contraseñas débiles	hss:weakPwds:list	-

Permiso	Acción	Acción relacionada
Consultar informes de protección contra agrietamiento de cuentas	hss:accountCracks:list	-
Desbloquear una dirección IP que se bloqueó durante la prevención de craqueo de cuentas	hss:accountCracks:unblock	-
Consultar resultados de análisis de programas maliciosos	hss:maliciousPrograms:list	-
Consultar resultados de análisis de inicio de sesión remoto	hss:abnorLogins:list	-
Consultar informes de cambios de archivos importantes	hss:keyfiles:list	-
Consultar la lista de puertos abiertos	hss:ports:list	-
Consultar la lista de vulnerabilidades	hss:vuls:list	-
Realizar operaciones por lotes en vulnerabilidades	hss:vuls:operate	-
Consultar la lista de cuentas	hss:accounts:list	-
Consultar la lista de software	hss:softwares:list	-
Consultar la lista de rutas web	hss:webdirs:list	-
Consultar la lista de procesos	hss:processes:list	-
Consultar informes de análisis de configuración	hss:configDetects:list	-
Consultar resultados de análisis de shell web	hss:webshells:list	-
Consultar informes de análisis de cuentas riesgosas	hss:riskyAccounts:list	-
Obtener estadísticas de riesgo del servidor	hss:riskyDashboard:get	-

Permiso	Acción	Acción relacionada
Consultar informes de análisis de políticas de complejidad de contraseñas	hss:complexityPolicys:list	-
Realizar operaciones por lotes en programas maliciosos	hss:maliciousPrograms:operate	-
Realizar operaciones por lotes en puertos abiertos	hss:ports:operate	-
Realizar operaciones en la configuración insegura detectada	hss:configDetects:operate	-
Realizar operaciones por lotes en shells web	hss:webshells:operate	-
Configurar ubicaciones de inicio de sesión comunes	hss:commonLocations:set	-
Consultar ubicaciones de inicio de sesión comunes	hss:commonLocations:list	-
Configurar direcciones IP de inicio de sesión comunes	hss:commonIPs:set	-
Consultar direcciones IP comunes de inicio de sesión	hss:commonIPs:list	-
Configurar la lista blanca de direcciones IP de inicio de sesión	hss:whiteIps:set	-
Consultar la lista blanca de direcciones IP de inicio de sesión	hss:whiteIps:list	-
Configurar contraseñas débiles	hss:weakPwds:set	-
Consultar contraseñas débiles	hss:weakPwds:get	-
Configurar rutas web	hss:webDirs:set	-
Consultar rutas de acceso web	hss:webDirs:get	-

Permiso	Acción	Acción relacionada
Obtener la lista de servidores donde 2FA está habilitado	hss:twofactorAuth:list	-
Habilitar 2FA	hss:twofactorAuth:set	-
Habilitar o deshabilitar el aislamiento automático y la eliminación de programas maliciosos	hss:automaticKillMp:set	-
Consultar los programas que han sido aislados y eliminados automáticamente	hss:automaticKillMp:get	-
Consultar la dirección de descarga del agente	hss:installAgent:get	-
Desinstalar un agente	hss:agent:uninstall	-
Consultar alarmas HSS	hss:alertConfig:get	-
Configurar alarmas HSS	hss:alertConfig:set	-
Consultar la lista WTP	hss:wtpHosts:list	vpc:ports:get vpc:publicIps:list ecs:cloudServers:list
Habilitar o deshabilitar WTP	hss:wtpProtect:switch	-
Configurar servidores de backup	hss:wtpBackup:set	-
Consultar servidores de copia de respaldo	hss:wtpBackup:get	-
Configurar directorios protegidos	hss:wtpDirectorys:set	-
Consultar la lista de directorios protegidos	hss:wtpDirectorys:list	-
Consultar registros WTP	hss:wtpReports:list	-
Configurar procesos privilegiados	hss:wtpPrivilegedProcess:set	-
Consultar la lista de procesos privilegiados	hss:wtpPrivilegedProcesses:list	-
Configurar un modo de protección	hss:wtpProtectMode:set	-

Permiso	Acción	Acción relacionada
Consultar el modo de protección	hss:wtpProtectMode:get	-
Configurar un sistema de archivos protegido	hss:wtpFilesystems:set	-
Consultar la lista del sistema de archivos protegido	hss:wtpFilesystems:list	-
Configurar la protección programada	hss:wtpScheduledProtections:set	-
Consultar Protección programada	hss:wtpScheduledProtections:get	-
Configurar alarmas WTP	hss:wtpAlertConfig:set	-
Consultar alarmas WTP	hss:wtpAlertConfig:get	-
Consultar estadísticas WTP	hss:wtpDashboard:get	-
Grupo de políticas de consulta	hss:policy:get	-
Configurar un grupo de políticas	hss:policy:set	-
Consultar la lista de intrusos detectados	hss:event:get	-
Realizar operaciones en intrusiones	hss:event:set	-
Consultar grupos de servidores	hss:hostGroup:get	-
Configurar grupos de servidores	hss:hostGroup:set	-
Supervisar la integridad de los archivos	hss:keyfiles:set	-
Consultar informes de cambios de archivos importantes	hss:keyfiles:list	-
Consultar la lista de inicio automático	hss:launch:list	-

