Host Security Service

Preguntas frecuentes

Edición 01

Fecha 2023-07-13

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 Acerca de HSS

1.1 ¿Qué es Host Security Service?

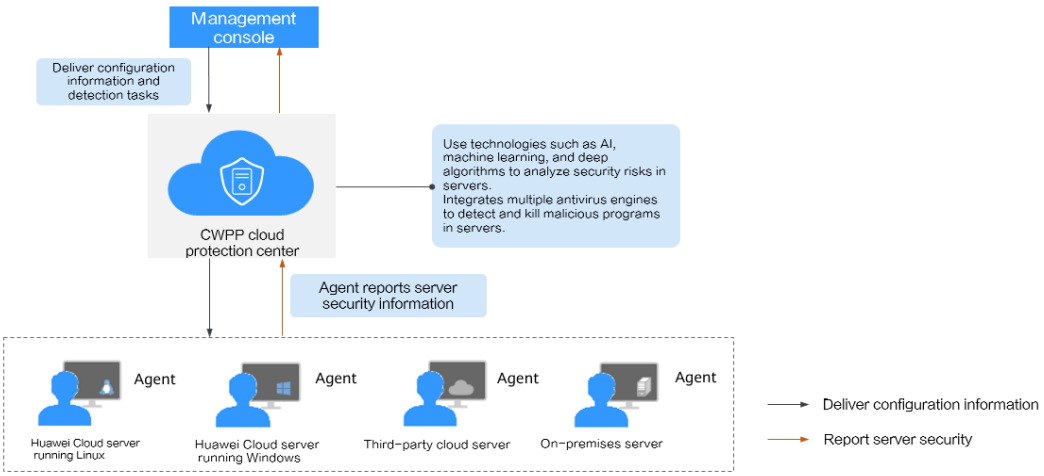
Host Security Service (HSS) le ayuda a identificar y gestionar los activos de sus servidores, eliminar riesgos y defenderse de intrusiones y manipulación de páginas web. También hay funciones avanzadas de protección y operaciones de seguridad disponibles para ayudarle a detectar y manejar fácilmente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

Cómo funciona HSS

Instale el agente HSS en sus servidores y podrá comprobar el estado de seguridad del servidor y los riesgos en una región en la consola HSS.

Figura 1-1 muestra los principios de trabajo de HSS.

Figura 1-1 Cómo funciona HSS



Las funciones y flujos de trabajo de los componentes HSS son las siguientes:

Tabla 1-1 Componentes

Componente	Descripción
Consola de gestión	Una plataforma de gestión visualizada, donde puede aplicar configuraciones de manera centralizada y ver el estado de defensa y los resultados de análisis de los servidores en una región.
Centro de protección en la nube de HSS	● Utiliza tecnologías como IA, aprendizaje automático y algoritmos profundos para analizar los riesgos de seguridad en los servidores. ● Integra múltiples motores antivirus para detectar y eliminar programas maliciosos en servidores. ● Recibe configuraciones y tareas de análisis enviadas desde la consola y las reenvía a los agentes de los servidores. ● Recibe la información del servidor reportada por los agentes, analiza los riesgos de seguridad y las excepciones en los servidores y muestra los resultados del análisis en la consola.
Agente	● Se comunica con el centro de protección en la nube HSS a través de HTTPS y WSS. El puerto 10180 se utiliza de forma predeterminada. ● Analiza todos los servidores a primera hora de la mañana, supervisa el estado de seguridad de los servidores e informa de la información recopilada del servidor (incluidas las configuraciones no conformes, configuraciones inseguras, trazas de intrusión, lista de software, lista de puertos y lista de procesos) al centro de protección de la nube. ● El agente bloquea los ataques al servidor en función de las políticas de seguridad que haya configurado. **NOTA** ● Si el agente no está instalado o es anormal, HSS no está disponible. ● Se puede instalar un agente en Huawei Cloud Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), servidores fuera de línea y servidores en la nube de terceros. ● Seleccione el agente y el comando de instalación adecuados para su sistema operativo. ● WTP, CGS y HSS comparten el mismo agente, por lo que solo necesita instalar el agente una vez en el mismo servidor.

1.2 ¿Qué es Container Security Service?

Container Security Service (CGS) analiza las vulnerabilidades y la información de configuración en las imágenes, lo que ayuda a las empresas a detectar riesgos de contenedores que no se pueden encontrar con software de seguridad convencional. CGS también proporciona funciones como la lista blanca de procesos de contenedores, la supervisión de archivos de contenedores, la recopilación de información de contenedores y la detección de escapes de contenedores para reducir los riesgos.

Arquitectura de despliegue

Figura 1-2 muestra la arquitectura de despliegue de CGS y **Tabla 1-2** describe sus componentes clave.

Figura 1-2 Arquitectura de despliegue de CGS

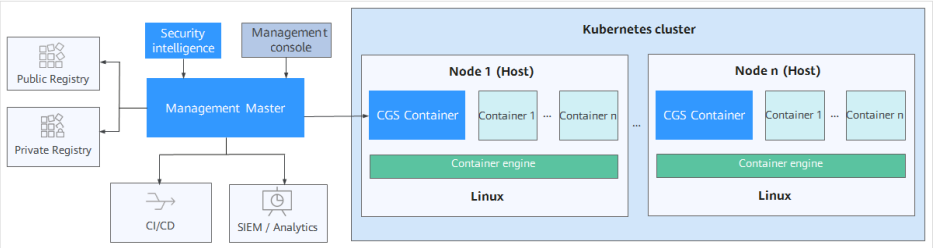


Tabla 1-2 Componentes clave de CGS

Componente	Descripción
Contenedor de CGS	Se ejecuta en cada nodo contenedor (host) para analizar todas las imágenes de contenedor en el nodo en busca de vulnerabilidades de imagen, implementar políticas de seguridad y recopilar excepciones.
Máster en Gestión	Gestiona y mantiene contenedores de CGS.
Inteligencia de seguridad	Proporciona una base de conocimientos de información de seguridad que contiene vulnerabilidades y bibliotecas de programas maliciosos, así como modelos de entrenamiento de IA de big data.
Consola de gestión	Proporciona una consola para que los usuarios utilicen CGS.

1.3 ¿Qué es Web Tamper Protection?

Web Tamper Protection (WTP) supervisa los directorios de sitios web en tiempo real, realiza copias de seguridad de los archivos y restaura los archivos manipulados mediante la copia de respaldo. WTP protege sus sitios web de troyanos, enlaces ilegales y manipulación.

Web Tamper Protection (WTP) puede detectar y evitar la manipulación de archivos en directorios específicos, incluidas páginas web, documentos e imágenes, y restaurarlos rápidamente utilizando archivos de copia de respaldo válidos.

Esta sección describe el proceso de operación y las principales funciones de WTP. Consulte **Figura 1-3** y **Tabla 1-3**.

Figura 1-3 Proceso de operación de WTP

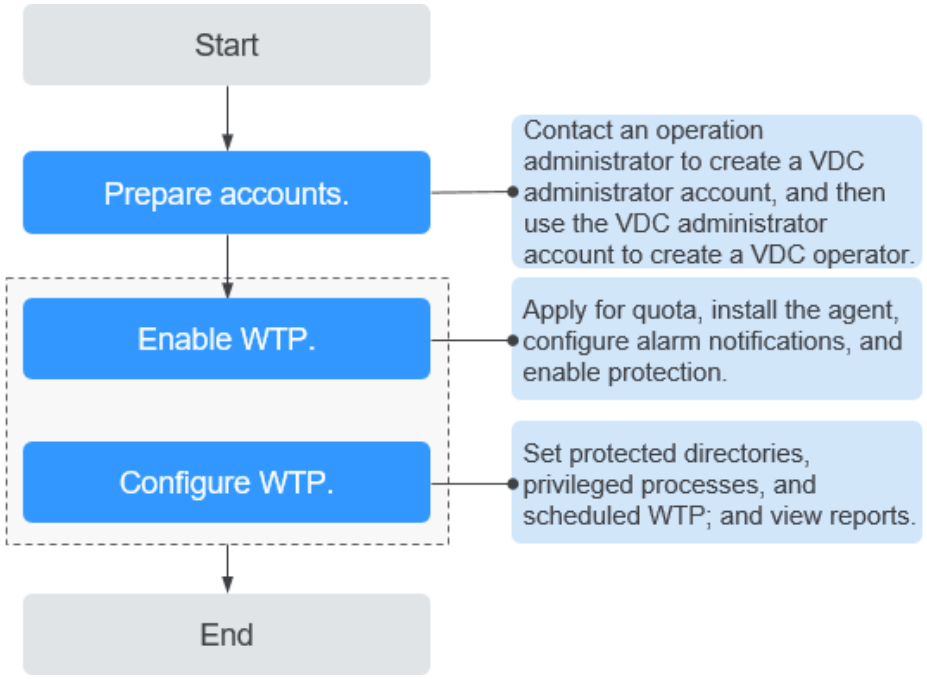


Tabla 1-3 Descripción del proceso de operación y función de WTP

Tipo	Operación	Descripción y referencia	Interfaz
Preparaciones	--	Si no hay una cuenta de operador VDC disponible, póngase en contacto con un administrador de operaciones para crear una cuenta de administrador VDC y, a continuación, utilice la cuenta de administrador VDC para crear un operador VDC.	Portal de operaciones de ManageOne: administrador de operaciones Portal de operación de ManageOne ● Administrador de VDC ● Administrador de agente
Primeros pasos con WTP	Solicitud de Cuota	Solicitar la cuota WTP.	Portal de operación de ManageOne ● Administrador de VDC ● Operador de VDC ● Administrador de agente

Tipo	Operación	Descripción y referencia	Interfaz
	Instalación de un agente	El agente es proporcionado por HSS. Ejecuta tareas de análisis para analizar todos los servidores, monitorea la seguridad del servidor e informa la información recopilada del servidor al centro de protección en la nube. Puede habilitar WTP solo después de que el agente esté instalado.	Portal de operación de ManageOne ● Administrador de VDC ● Operador de VDC ● Administrador de agente
	Parámetros necesarios para configurar las 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.	Portal de operación de ManageOne ● Administrador de VDC ● Operador de VDC ● Administrador de agente
	Habilitación de HSS	Asignar una cuota a un servidor y habilitar HSS para el servidor.	Portal de operación de ManageOne ● Administrador de VDC ● Operador de VDC ● Administrador de agente
Habilitar WTP	Adición de un directorio protegido	Agregar un directorio para ser protegido por WTP.	Portal de operación de ManageOne ● Administrador de VDC ● Operador de VDC ● Administrador de agente
	Crear copias de respaldo remotas	De forma predeterminada, HSS realiza una copia de respaldo de los archivos de los directorios protegidos 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.	Portal de operación de ManageOne ● Administrador de VDC ● Operador de VDC ● Administrador de agente

Tipo	Operación	Descripción y referencia	Interfaz
	Adición de un proceso privilegiado	Después de habilitar WTP, el contenido de los directorios protegidos es de solo lectura. Para permitir que ciertos procesos modifiquen archivos en los directorios, agréguelos a la lista de procesos con privilegios.	Portal de operación de ManageOne ● Administrador de VDC ● Operador de VDC ● Administrador de agente
	Establecer la protección de WTP programada	Puede programar la protección WTP para permitir actualizaciones de sitios web en períodos específicos.	Portal de operación de ManageOne ● Administrador de VDC ● Operador de VDC ● Administrador de agente
	Habilitación de WTP dinámico	WTP dinámico protege sus datos mientras Tomcat está en ejecución, detectando la manipulación de datos dinámicos en las bases de datos.	Portal de operación de ManageOne ● Administrador de VDC ● Operador de VDC ● Administrador de agente
	Ver informes de WTP	Después de que WTP esté habilitado, HSS comprobará inmediatamente los directorios protegidos que usted especificó. Puede comprobar los registros sobre la manipulación detectada.	Portal de operación de ManageOne ● Administrador de VDC ● Operador de VDC ● Administrador de agente

1.4 ¿Cuáles son las relaciones entre imágenes, contenedores y aplicaciones?

- Una imagen es un sistema especial de archivos. Proporciona programas, bibliotecas, recursos, archivos de configuración y otros archivos necesarios para un contenedor en ejecución. Una imagen también contiene algunos parámetros de configuración (como volúmenes anónimos, variables de entorno y usuarios) preparados para un contenedor en ejecución. Las imágenes no incluyen datos dinámicos y su contenido no puede cambiarse tras su creación.
- La relación entre la imagen y el contenedor es similar a la entre la clase y la instancia en el diseño del programa. Una imagen es estática, y un contenedor es la entidad para una

imagen en ejecución. Se puede crear, iniciar, detener, eliminar y suspender un contenedor.

- Se pueden iniciar varios contenedores para una imagen.
- Una aplicación puede incluir uno o un conjunto de contenedores.

1.5 ¿Dónde está disponible el HSS?

HSS está disponible en las siguientes regiones:

- CN South-Guangzhou
- CN-Hong Kong
- AP-Bangkok
- AP-Singapore

Puede acceder a servidores que no sean de Huawei Cloud solo en las siguientes regiones:

- CN South-Guangzhou
- CN-Hong Kong
- AP-Singapore

Tabla 1-4 Elegir una región para comprar HSS

Servidor	El HSS de la región se compra para
ECS BMS HECS	Regiones en las que se implementan sus ECS/BMS/HECS
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	

1.6 ¿Cómo uso HSS?

Realice los siguientes pasos para comenzar con HSS:

Paso 1 **Comprar HSS.**

Comprar cuotas de protección en la edición requerida.

Paso 2 **Instalar el agente**.

- Puede habilitar HSS solo después de instalar un agente HSS en el servidor.
- Las ediciones básica, empresarial y WTP utilizan el mismo agente.

Paso 3 **Habilitar notificaciones de alarma**.

Después de activar las notificaciones de alarma, puede recibir notificaciones de alarma enviadas por HSS para obtener información sobre los riesgos de seguridad que enfrenta el servidor. Sin esta función, debe iniciar sesión en la consola de gestión para ver las alarmas.

Paso 4 **Habilitar HSS**.

- Una vez instalado el agente, puede habilitar la protección para los servidores.
- Antes de habilitar HSS, 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.

Paso 5 **Vea los resultados de la detección** y maneje los riesgos relacionados.

----Fin

1.7 Is HSS in Conflict with Any Other Security Software?

HSS may conflict with DenyHosts, G01, or 360 Guard (server edition).

Conflicts Between the Agent and DenyHosts

For details, see **Is the Agent in Conflict with Any Other Security Software?**

Conflicts Between the Two-factor Authentication Function and G01 or 360 Guard (Server Edition)

On a Windows server where HSS is enabled, the two-factor authentication function may conflict with the login authentication function of G01 or 360 Guard (server edition). In this case, enable only one of the functions.

1.8 ¿Cuáles son las diferencias entre HSS, VSS y WAF?

HSS, Vulnerability Scan Service (VSS) y Web Application Firewall (WAF) son proporcionados por Huawei Cloud para ayudarlo a defender hosts, sitios web y aplicaciones web contra riesgos y amenazas, mejorando la seguridad del sistema. Se recomienda que los tres servicios se utilicen juntos.

Tabla 1-5 Diferencias entre HSS, VSS y WAF

Nombre del servicio	Categoría	Objeto protegido	Función
HSS	Seguridad del host	Hosts	● Gestión de activos ● Gestión de vulnerabilidades ● Detección de intrusiones ● Inspección de línea base ● Protección contra manipulación de la web
VSS	Seguridad de las aplicaciones	Sitios web	● Análisis de vulnerabilidades ● Comprobación de contenido web ● Control de estado del sitio web ● Comprobación de cumplimiento de referencia

Nombre del servicio	Categoría	Objeto protegido	Función
WAF	Seguridad de las aplicaciones	Aplicaciones web	● Protección básica de Web ● Protección contra ataques CC ● Protección precisa

1.9 ¿Qué es el agente de HSS?

El agente HSS se utiliza para escanear todos los servidores y contenedores, monitorear su estado en tiempo real y recopilar su información e informar al centro de protección en la nube.

Existen diferentes versiones de agentes para los sistemas operativos Linux y Windows. Las funciones de protección HSS estarán disponibles después de **instalar el agente** y activar la **protección HSS**.

Funciones del Agente

- El agente ejecuta tareas de análisis todos los días a primera hora de la mañana para analizar todos los servidores y contenedores, supervisa su seguridad e informa la información recopilada de ellos al centro de protección en la nube.
- El agente bloquea los ataques dirigidos a servidores y contenedores según las políticas de seguridad que haya configurado.

NOTA

- Si el agente no está instalado o es anormal, HSS no está disponible.
- El agente se puede instalar en Elastic Cloud Servers (ECSs) de Huawei Cloud, Bare Metal Servers (BMSs), servidores fuera de línea y servidores en la nube de terceros.
- WTP, CGS y HSS comparten el mismo agente, por lo que solo necesita instalar el agente una vez en el mismo servidor.

Procesos del agente Linux

El proceso del agente debe ser ejecutado por el usuario **root**.

El agente contiene los siguientes procesos:

Tabla 1-6 Procesos del agente Linux

Nombre del proceso del agente	Función	Ruta
hostguard	Detecta problemas de seguridad, protege el sistema y supervisa el agente.	/usr/local/hostguard/bin/hostguard
upgrade	Actualiza el agente.	/usr/local/hostguard/bin/upgrade

1.10 ¿Puedo actualizar mi HSS a una edición superior?

Sí.

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.

Actualización a la edición Enterprise/Premium

Para actualizar una cuota, su **Usage Status** debe ser **Idle**.

- **Actualización de una cuota inactivo**

  Actualice la cuota en la pestaña **Quotas** de la página **Servers & Quota**. Para obtener más información, consulte **Actualización de la edición**.

- **Actualización de una cuota en uso**

  a. Desvincule la cuota del servidor que protege. Para obtener más información, consulte **Desvincular una cuota de un servidor**.

  b. Compruebe el estado de la cuota. Se espera que cambie a **Idle**.

  c. Actualice la cuota. Para obtener más información, consulte **Actualización a la edición Enterprise/Premium**.

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.

1. Compre WTP en la consola HSS. Para obtener más información, consulte **Compra de una cuota de HSS**.
2. Desvincule un servidor de su cuota existente. Para obtener más información, consulte **Desvincular una cuota de un servidor**.
3. Vincule el servidor a WTP. Para obtener más información, consulte **Actualización a la edición WTP**.

2 Preguntas Frecuentes de Agentes

2.1 ¿Está el agente en conflicto con cualquier otro software de seguridad?

Sí, puede estar en conflicto con DenyHosts.

- Síntoma: La dirección IP del host de inicio de sesión se identifica como una dirección IP de ataque, pero no se puede desbloquear.
- Causa: HSS y DenyHosts bloquean posibles direcciones IP de ataque, pero HSS no puede desbloquear las direcciones IP bloqueadas por DenyHosts.
- Método de manejo: Detener DenyHosts.
- Procedimiento

  a. Inicie sesión como usuario **root** a ECS.

  b. Ejecute el siguiente comando para comprobar si se ha instalado DenyHosts:

  ps -ef | grep denyhosts.py

  Si se muestra información similar a la siguiente, se ha instalado DenyHosts:

  ```
  [root@hss-test ~]# ps -ef | grep denyhosts.py
  root      64498      1  0 17:48 ?        00:00:00 python denyhosts.py --daemon
  ```

  c. Ejecute el siguiente comando para detener DenyHosts:

  kill -9 'cat /var/lock/denyhosts'

  d. Ejecute el siguiente comando para cancelar el inicio automático de DenyHosts al iniciar el host:

  chkconfig --del denyhosts;

2.2 ¿Cómo instalo el agente?

- For details about how to install the Linux agent, see **Installing an Agent on the Linux OS**.
- Para obtener más información acerca de cómo instalar el agente de Windows, consulte **Instalación de un agente en el sistema operativo de Windows**.

2.3 ¿Cómo desinstalo el agente?

Hay dos métodos de desinstalación disponibles: desinstalación con un solo clic y desinstalación local manual.

Escenario

- El agente se instaló usando un paquete incorrecto y es necesario desinstalarlo.
- El agente se instaló con comandos incorrectos y es necesario desinstalarlo.
- Si el agente no se actualiza, desinstale el agente.

Prerrequisitos

Agent Status del servidor es **Online**.

Desinstalar el agente en la consola con un solo clic

Puede desinstalar un agente HSS desde la consola HSS.

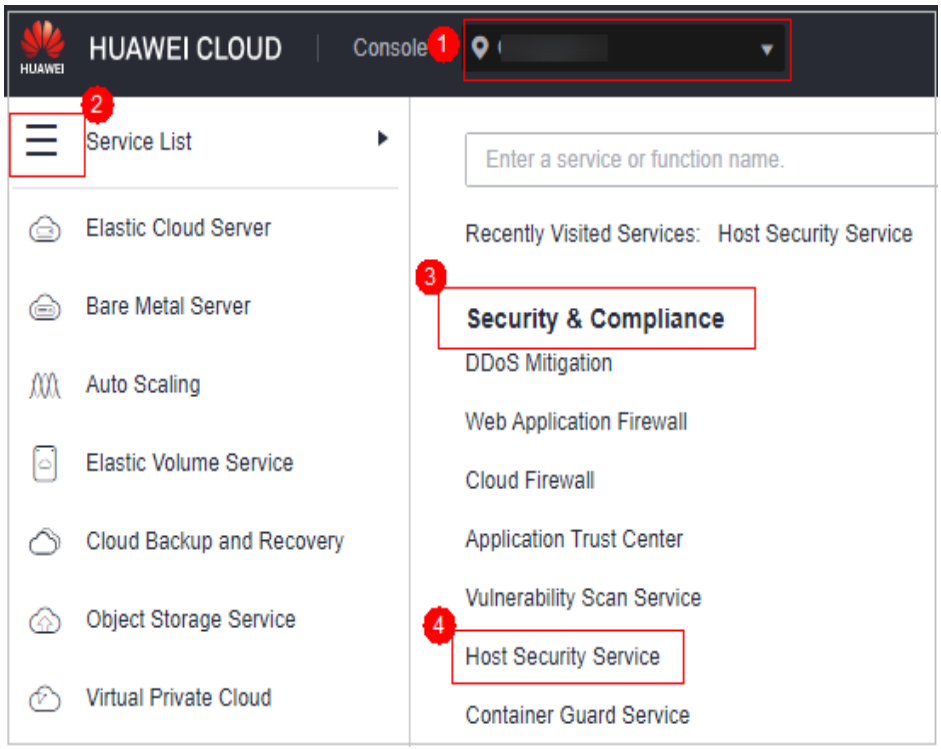
NOTA

Después de desinstalar el agente de un servidor, HSS no proporcionará ninguna protección para el 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)**.

Figura 2-1 Acceso a HSS



Paso 3 En el cuadro de diálogo que se muestra, haga clic en **Try the new edition** para cambiar a la consola HSS (Nueva).

NOTA

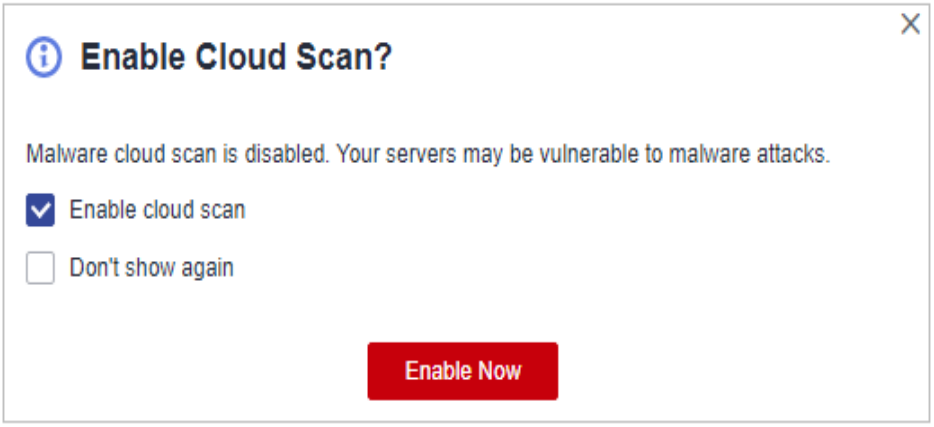
- Actualmente, HSS está disponible en las siguientes regiones: CN South-Guangzhou, CN-Hong Kong, AP-Bangkok, and AP-Singapore.
- En la consola HSS (Nueva), puede hacer clic en **Back to Old Console** en la esquina superior izquierda para cambiar a la consola HSS (Antigua).

- Si el análisis en la nube no está habilitado o accede a la consola HSS (Nuevo) por primera vez, se muestra el cuadro de diálogo **Enable Cloud Scan?**. Se recomienda seleccionar **Enable cloud scan**.

  NOTA

  – La función de escaneo en la nube es gratuita.
  – Una vez activada la función de análisis en la nube, se escanearán todos los servidores HSS. Algunas ediciones de cuota de HSS solo pueden admitir capacidades de análisis limitadas. Por lo tanto, se recomienda comprar la edición empresarial o superior para disfrutar de todas las capacidades de la función de escaneo en la nube.

Figura 2-2 Habilitar el análisis en la nube



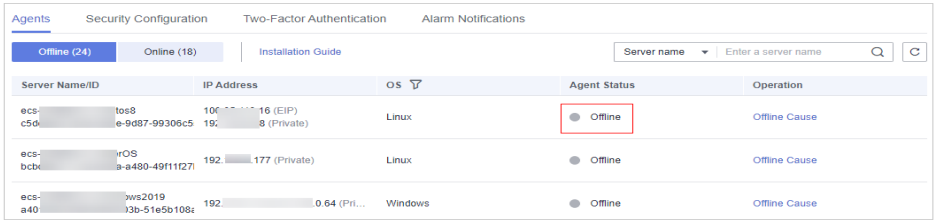
Paso 4 En el panel de navegación, elija **Installation and Configuration**.

Paso 5 En la página mostrada, haga clic en la pestaña **Agents** y haga clic en **Online**. En la fila que contiene el servidor deseado, haga clic en **Uninstall Agent** en la columna **Operation**.

Paso 6 En el cuadro de diálogo que se muestra, haga clic en **OK**.

En la lista de servidores, si **Agent Status** del servidor es **Offline**, su agente se desinstala correctamente.

Figura 2-3 Agente desinstalado



----Fin

Desinstalar el agente del servidor

Puede desinstalar manualmente un agente HSS en un servidor cuando ya no utilice HSS o necesite reinstalar el agente.

NOTA

Después de desinstalar el agente de un servidor, HSS no proporcionará ninguna protección para el servidor.

- **Desinstalar el agente de Linux**
  a. Inicie sesión en el servidor desde el que desea desinstalar el agente. A continuación, ejecute el comando **su - root** para cambiar a usuario **root**.
  b. En cualquier directorio, ejecute el siguiente comando para desinstalar el agente:
     i. Si el agente se instaló con un paquete.rpm, ejecute el comando **rpm -e --nodeps hostguard**.
     ii. Si el agente se instaló con el paquete a .deb, ejecute el comando **dpkg -P hostguard**.

     Si se muestra la siguiente información, se desinstala el agente:

     ```
     Stopping Hostguard...
     Hostguard stopped
     Hostguard uninstalled.
     ```

- **Desinstalar el agente de Windows**
  a. Inicie sesión en el servidor desde el que desea desinstalar un agente HSS.
  b. Haga clic en **Start** y seleccione **Control Panel** > **Programs**. A continuación, seleccione **HostGuard** y haga clic en **Uninstall**.

     NOTA

     - Alternativamente, vaya al directorio de instalación y haga doble clic en **unins000.exe**.
     - Si ha creado una carpeta para almacenar el acceso directo del agente en el menú **Start** al instalar el agente, también puede elegir **Start** > **HostGuard** > **Uninstall HostGuard** para desinstalar HostGuard.

  c. En el cuadro de diálogo **Uninstall HostGuard**, haga clic en **Yes**.
  d. Una vez completada la desinstalación, haga clic en **OK**.

2.4 ¿Qué debo hacer si falló la instalación del agente?

Si ha utilizado HSS de una versión anterior e instalado el agente en la nueva versión HSS, pero la página sigue mostrando que el agente no está instalado, consulte **¿Qué puedo hacer si el estado del agente sigue "No instalado" después de la instalación?**

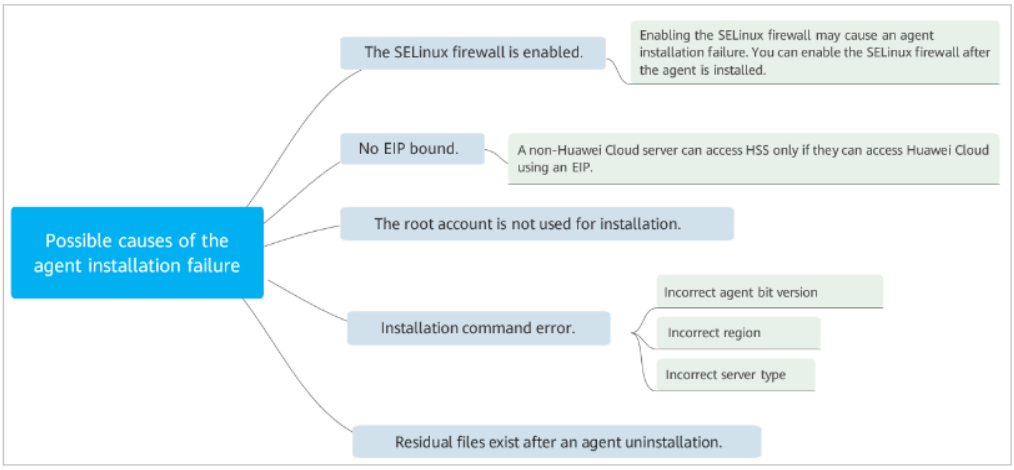
Si es la primera vez que instala el agente y la instalación ha fallado, rectifique el error según si se instala mediante scripts o comandos.

Error al instalar el agente ejecutando los comandos de instalación

Síntomas

El agente no se puede instalar mediante la ejecución de comandos. La página de lista de servidores de la consola aún indica que el agente no está instalado.

Causas posibles



Solución

Paso 1 Compruebe si el firewall SELinux del servidor está deshabilitado.

- En caso afirmativo, vaya a **Paso 2**.
- Si no lo es, desactívelo e instale de nuevo el agente.

Paso 2 Compruebe si hay una EIP enlazado al servidor.

- En caso afirmativo, vaya a **Paso 3**.
- Si no lo hay, vincule un EIP al servidor y vuelva a instalar el agente.

Paso 3 Compruebe si el comando de instalación es adecuado para la región del servidor y el sistema operativo.

1. Cambie a la región del servidor.
2. Copie los comandos de instalación adecuados para su sistema operativo de servidor.
   - Ejecute comandos de instalación de 32 bits en un servidor de 32-bit.
   - Ejecute comandos de instalación de 64 bits en un servidor de 64-bit.

- Si lo ha hecho, vaya a **Paso 4**.
- Si los comandos que utilizó son incorrectos, vuelva a instalar el agente con los correctos.

Paso 4 Compruebe si la instalación fue realizada por usuario **root**.

- Si lo ha hecho, vaya a **Paso 5**.
- Si no es así, instale el agente de nuevo como usuario **root**.

Paso 5 **Desinstale el agente** como usuario **root** e instálelo por la fuerza.

- Si la instalación se realiza correctamente, no se requiere ninguna otra acción.
- Si la instalación falla, póngase en contacto con el soporte técnico.

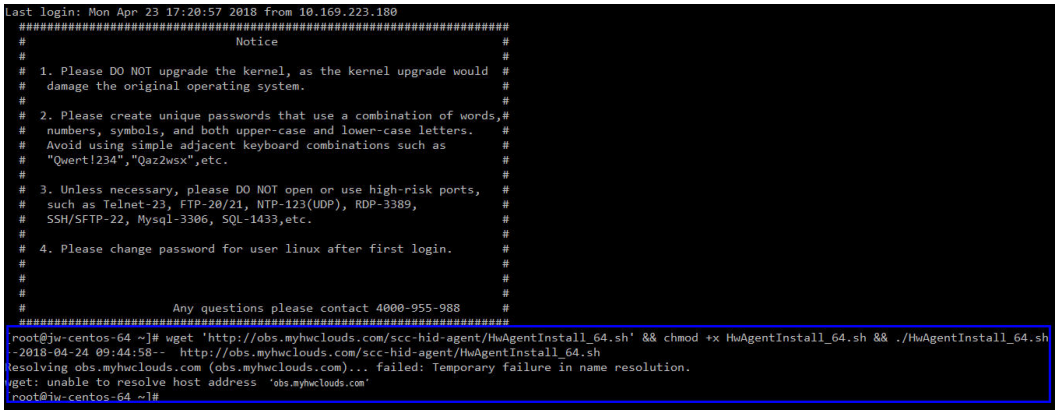
----Fin

Error al instalar el agente al ejecutar el script

Síntomas

Se notifica un error durante la instalación del agente. Se muestra el siguiente mensaje de error cuando se instala el agente mediante un script:

Figura 2-4 Mensaje de error



Causas posibles

La dirección DNS no está configurada correctamente. El nombre de dominio **obs.myhuaweicloud.com** no se puede resolver.

Solución

Realice los siguientes pasos para configurar correctamente DNS y reintentar la instalación:

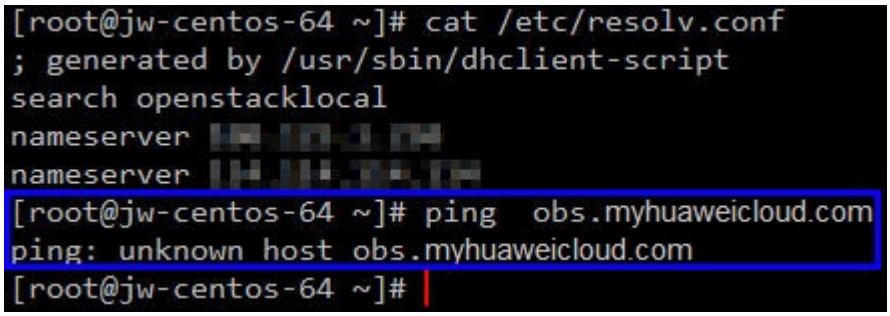
Paso 1 Ejecute el comando **cat /etc/resolv.conf** para ver el archivo **resolv.conf**.

cat /etc/resolv.conf

Paso 2 Ejecute el comando **ping** *Domain_name*. Si se muestra la salida del comando en **Figura 2-5**, vaya al **Paso 3**.

ping obs.myhuaweicloud.com

Figura 2-5 Error al hacer ping al nombre de dominio



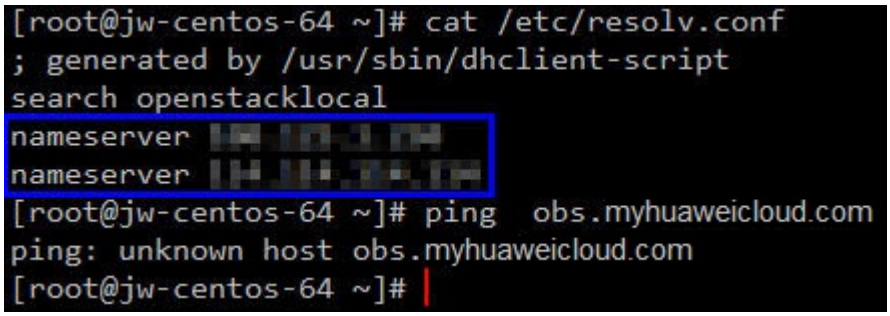
Paso 3 Ejecute el siguiente comando para abrir el archivo **resolv.conf**:

vi /etc/resolv.conf

Reemplace las direcciones IP resaltadas en **Figura 2-6** con direcciones IP de DNS comunes.

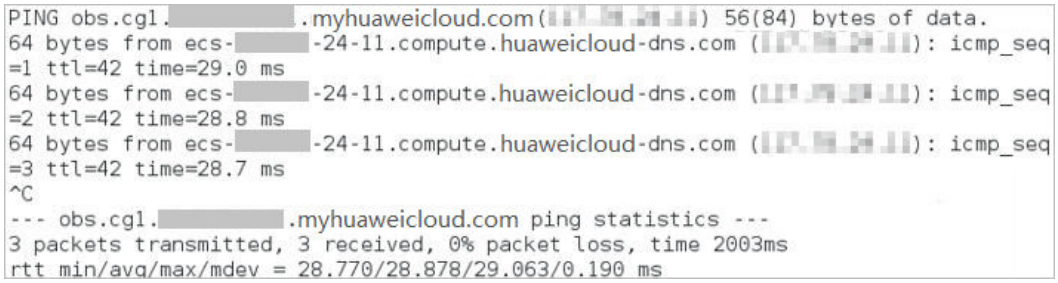
```
nameserver Common_DNS_IP_address_1
nameserver Common_DNS_IP_address_2
```


Figura 2-6 La parte que se va a sustituir



Paso 4 Después de la modificación, vuelva a ejecutar el comando **ping obs.myhuaweicloud.com**. Si se muestra información similar a la siguiente, el nombre de dominio se hace ping correctamente.

Figura 2-7 Mensaje que indica que el nombre de dominio se puede hacer ping



Paso 5 Ejecute el script de instalación.

----Fin

2.5 ¿Cómo puedo arreglar un agente anormal?

Su agente es probablemente anormal si está en estado **Not installed** o **Offline**. Los estados de agente y su significado son los siguientes:

- **Uninstalled**: No se ha instalado ningún agente en el servidor o el agente se ha instalado pero no se ha iniciado.
- **Offline**: La comunicación entre el agente y el servidor es anormal. El agente en el servidor se ha eliminado, o un servidor que no es de Huawei Cloud está desconectado.
- **Online**: El agente en el servidor se está ejecutando correctamente.

Causas posibles

- La red presenta fallas.

  El agente o el centro de protección en la nube es anormal. Por ejemplo, la NIC está defectuosa, la dirección IP cambia o el ancho de banda es bajo.
- El proceso del agente es anormal.
- No se ha actualizado el estado del agente. Después de instalar el agente, la consola tarda unos 2 minutos en actualizar su estado.

Solución

Paso 1 Solucionar problemas de red (si los hay).

Asegúrese de que las configuraciones salientes del grupo de seguridad de su servidor permiten el acceso al puerto 10180 en el segmento de red 100.125.0.0/16.

Después de que la red se recupere,

- Si el estado del agente es de **Online**, no se requiere ninguna acción adicional.
- Si el estado del agente es **Not installed** o **Offline**, vaya a **Paso 2**.

Paso 2 Inicie sesión en el servidor y reinicie el agente. El estado del agente **Not installed** o **Offline** indica que el proceso del agente es probablemente anormal.

- Linux

  Ejecute el siguiente comando en la CLI como usuario **root** para reiniciar el agente:

  service hostguard restart

  Si se muestra la siguiente información, el reinicio se realiza correctamente:

```
root@HSS-Ubuntu32:~#service hostguard restart
Stopping Hostguard...
Hostguard stopped
Hostguard restarting...
Hostguard is running
```

Después de reiniciar el proceso, espere aproximadamente 2 minutos.

- Si el estado del agente es de **Online**, no se requiere ninguna acción adicional.
- Si el estado del agente sigue siendo **Not installed** o **Offline**, desinstale el agente e instálelo de nuevo.

----Fin

2.6 ¿Cuál es la ruta de instalación predeterminada del agente?

Las rutas de instalación del agente en servidores que ejecutan el sistema operativo Linux o Windows no se pueden personalizar. **Tabla 2-1** describe las rutas predeterminadas.

Tabla 2-1 Rutas de instalación del agente predeterminadas

Sistema operativo	Ruta de instalación predeterminada
Linux	/usr/local/hostguard/
Windows	C:\Program Files (x86)\HostGuard

2.7 ¿Cuántos recursos de CPU y memoria están ocupados por el agente cuando realiza escaneos?

HSS utiliza agentes ligeros, que ocupan solo unos pocos recursos y no afectan a sus servicios.

El uso de CPU y memoria es como sigue.

Uso máximo de CPU

Un agente en ejecución ocupa un máximo del 20% de una vCPU. El uso real depende de las especificaciones de su servidor. Para obtener más información, consulte **Uso de recursos de diferentes especificaciones mientras el agente se está ejecutando**.

Si el uso de la CPU alcanza el 20% de una vCPU, el agente reducirá automáticamente el uso de la CPU y dedicará más tiempo a los análisis. Esto no afecta a sus servicios.

NOTA

El agente está programado para escanear sus servidores de 00:00 a 04:00 todos los días, evitando sus horas de servicio ocupado.

Uso máximo de memoria

Un agente en ejecución ocupa aproximadamente 500 MB de memoria.

Si el uso de memoria alcanza los 500 MB, el agente se reiniciará automáticamente en 5 minutos.

Uso de recursos de diferentes especificaciones mientras el agente se está ejecutando

En la siguiente tabla se describe el uso de CPU y memoria de diferentes especificaciones cuando el agente se está ejecutando.

Tabla 2-2 Uso de recursos del agente

vCPUs	Máx. Uso de CPU del agente	Máx. Uso de memoria
1 vCPU	20%	500MB
2 vCPUs	10%	500MB
4 vCPUs	5%	500MB
8 vCPUs	2.5%	500MB
12 vCPUs	About 1.67%	500MB
16 vCPUs	About 1.25%	500MB
24 vCPUs	About 0.84%	500MB
32 vCPUs	About 0.63%	500MB
48 vCPUs	About 0.42%	500MB
60 vCPUs	About 0.34%	500MB
64 vCPUs	About 0.32%	500MB

2.8 ¿WTP y HSS usan el mismo agente?

Sí.

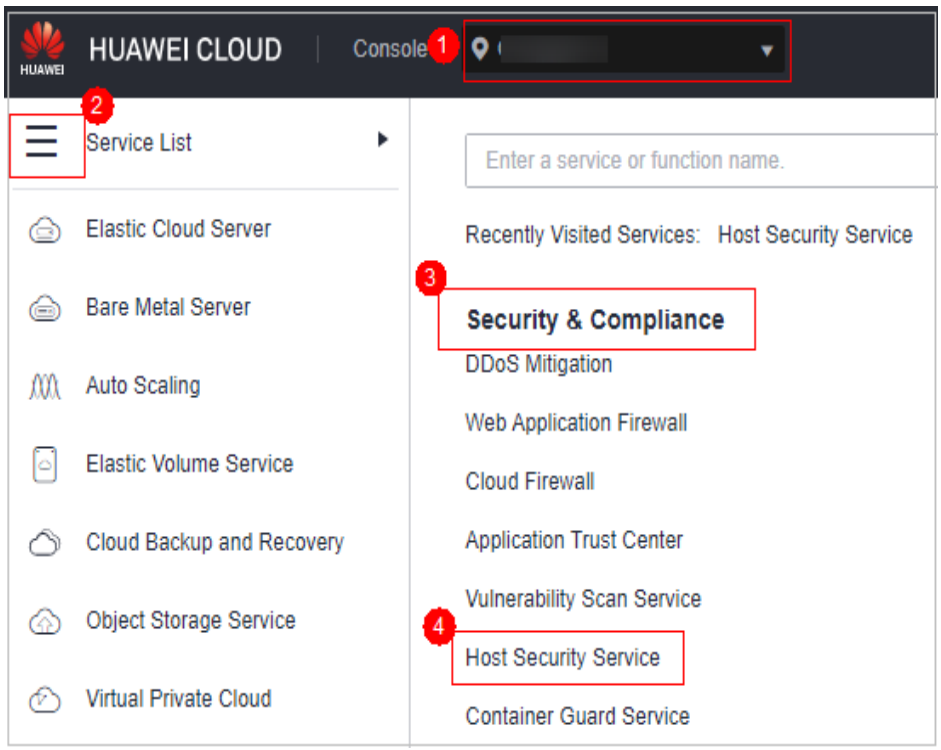
Todas las ediciones HSS pueden utilizar el mismo agente instalado en un servidor.

2.9 ¿Cómo puedo ver los servidores donde no se han instalado agentes?

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 2-8 Acceso a HSS



Paso 3 En el cuadro de diálogo que se muestra, haga clic en **Try the new edition** para cambiar a la consola HSS (Nueva).

NOTA

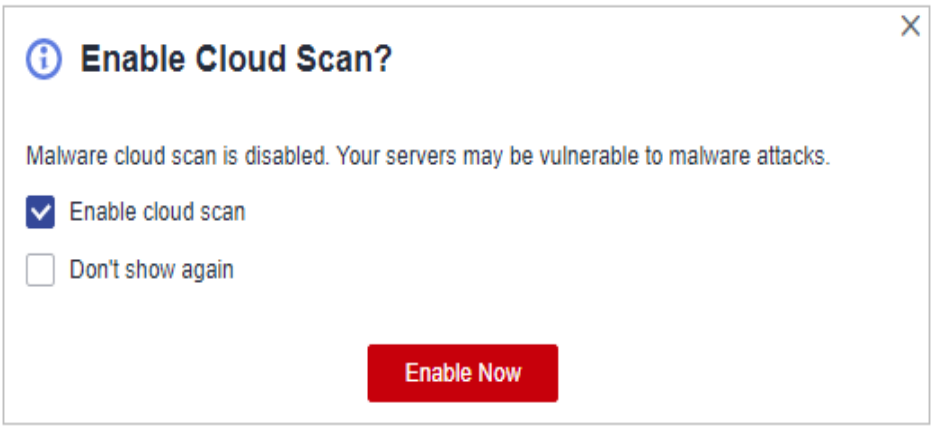
- Actualmente, HSS está disponible en las siguientes regiones: CN South-Guangzhou, CN-Hong Kong, AP-Bangkok, and AP-Singapore.
- En la consola HSS (Nueva), puede hacer clic en **Back to Old Console** en la esquina superior izquierda para cambiar a la consola HSS (Antigua).

- Si el análisis en la nube no está habilitado o accede a la consola HSS (Nuevo) por primera vez, se muestra el cuadro de diálogo **Enable Cloud Scan?**. Se recomienda seleccionar **Enable cloud scan**.

NOTA

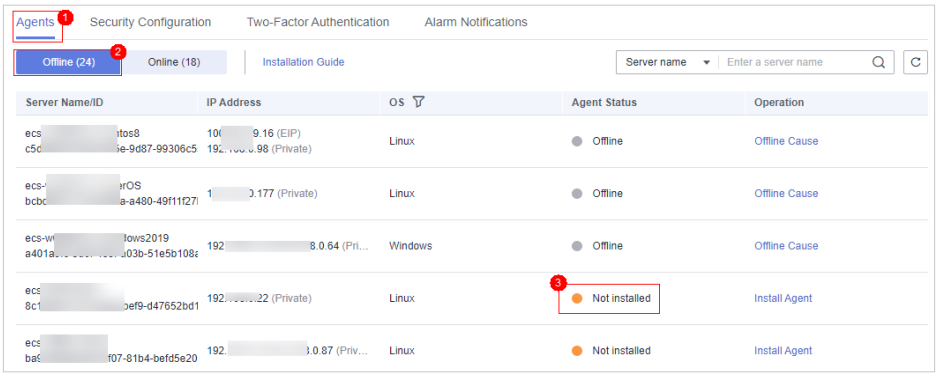
- La función de escaneo en la nube es gratuita.
- Una vez activada la función de análisis en la nube, se escanearán todos los servidores HSS. Algunas ediciones de cuota de HSS solo pueden admitir capacidades de análisis limitadas. Por lo tanto, se recomienda comprar la edición empresarial o superior para disfrutar de todas las capacidades de la función de escaneo en la nube.

Figura 2-9 Habilitar el análisis en la nube



Paso 4 En la página **Installation & Configuration**, haga clic en la pestaña **Agents** y haga clic en **Offline**. Vea los servidores donde el agente no está instalado.

Figura 2-10 Servidores donde el agente no está instalado



Los posibles estados de agente son:

- **Not installed**: El agente no se ha instalado ni se ha iniciado correctamente.
- **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.

  Haga clic en **Offline Cause** para ver las posibles causas.

----Fin

2.10 ¿Qué puedo hacer si el estado del agente sigue "No instalado" después de la instalación?

Precauciones

En un servidor, solo necesita instalar el agente una vez.

Después de la instalación, se recomienda reiniciar los servidores antes de habilitar HSS y cuotas de enlace.

Causa posible

Ahora están en uso las consolas de HSS (Nuevo) y HSS (Antigua). Los estados de agente y protección de un servidor solo se pueden mostrar correctamente en una de las consolas.

Por ejemplo, si ha instalado el agente en el servidor A en la consola antigua e intenta volver a instalarlo en la nueva consola, aparecerá un mensaje indicando que la instalación se ha realizado correctamente, pero el estado de instalación en la nueva consola seguirá siendo **Not installed**.

Solución

Utilice solo una consola. No cambie entre las consolas antiguas y nuevas.

Puede **actualizar el agente** para utilizar HSS (Nuevo). La actualización es gratuita y no afecta a los servicios.

NOTA

HSS (Nuevo) proporciona una protección contra ransomware más fuerte y capacidades adicionales de protección de aplicaciones, que no están disponibles en la versión anterior. Se recomienda utilizar la nueva versión.

3 Defensa de ataque de fuerza bruta

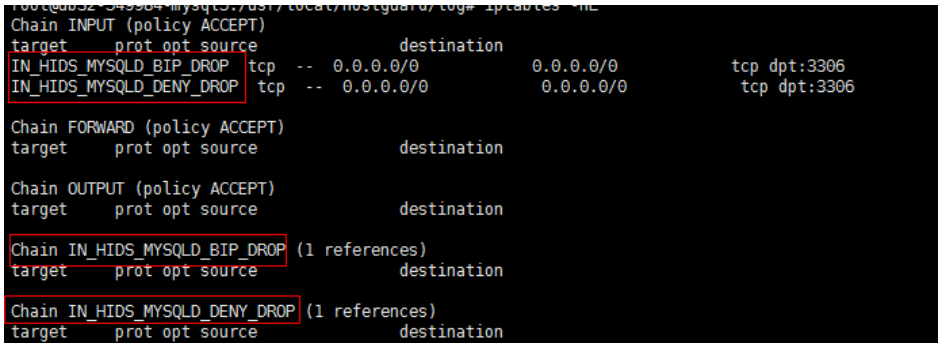
3.1 ¿Cómo Intercepta HSS los Ataques de Fuerza Bruta?

Alcance de protección

HSS puede bloquear ataques en MySQL, SQL Server 2012, VSFTP, SSH y RDP.

Si MySQL o VSFTP está instalado en su servidor, después de que HSS esté habilitado, el agente agregará reglas a iptables para evitar ataques de fuerza bruta de MySQL y VSFTP. Al detectar un ataque de fuerza bruta, HSS agregará la dirección IP de origen a la lista de bloqueo. Las reglas agregadas se resaltan a continuación.

Figura 3-1 Reglas agregadas



AVISO

Las reglas iptables existentes se utilizan para bloquear ataques de fuerza bruta. Se aconseja que los conserve. Si se eliminan, HSS no podrá proteger MySQL o VSFTP de ataques de fuerza bruta.

Cómo se interceptan los ataques de fuerza bruta

Los ataques de fuerza bruta son un tipo de ataques de intrusión comunes. Los atacantes envían muchas contraseñas de servidor hasta que finalmente adivinan correctamente y obtienen control sobre un servidor.

HSS utiliza algoritmos de detección de fuerza bruta y una lista negra de direcciones IP para prevenir eficazmente los ataques de fuerza bruta y bloquear las direcciones IP atacantes. La duración de bloqueo para ataques SSH sospechosos es de 12 horas y para otros ataques sospechosos es de 24 horas. **Si una dirección IP bloqueada no realiza ataques de fuerza bruta en la duración de bloqueo predeterminada, se desbloqueará automáticamente**. HSS admite **2FA** para autenticar la identidad del usuario, evitando eficazmente que los atacantes pirateen cuentas.

Puede **establecer direcciones IP de inicio de sesión comunes** y **listas blancas de direcciones IP de SSH** que no se bloquearán.

NOTA

Si HSS detecta ataques de craqueo de cuentas en servidores que usan Kunpeng EulerOS (EulerOS con ARM), no bloquea las direcciones IP de origen y solo genera alarmas. La lista blanca de direcciones IP de inicio de sesión SSH no tiene efecto para dichos servidores.

Políticas de alarma

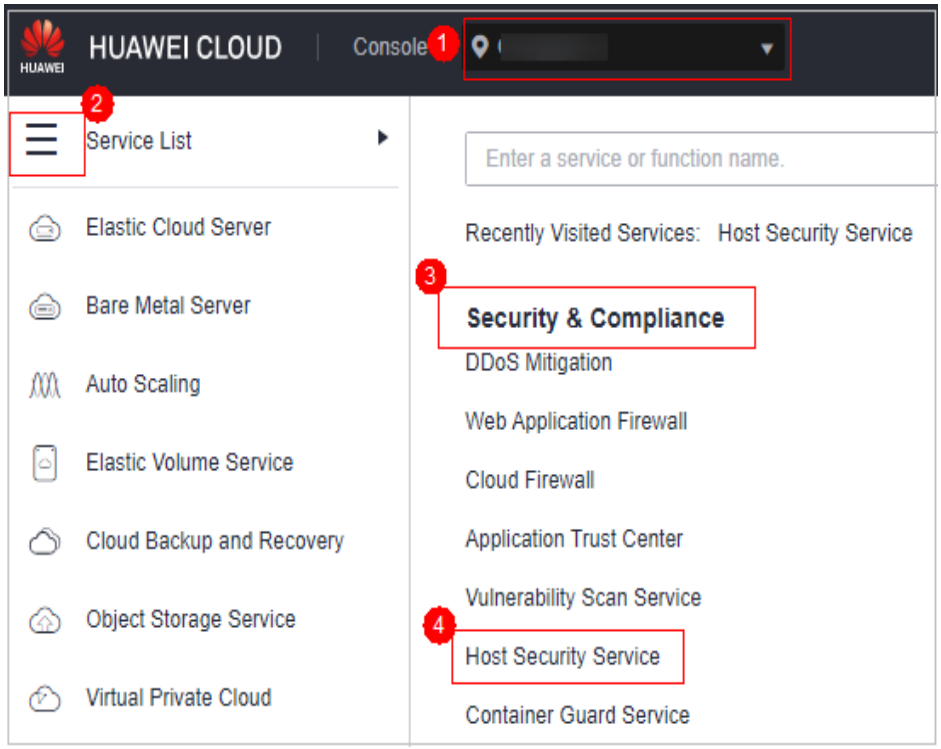
- Si un hacker rompe con éxito la contraseña e inicia sesión en un servidor, se enviará inmediatamente una alarma en tiempo real a los destinatarios especificados.
- Si se detecta un ataque de fuerza bruta y riesgos de piratería de cuentas, se enviará inmediatamente una alarma en tiempo real a los destinatarios especificados.
- Si se detecta un ataque de fuerza bruta y falla, y no se detectan configuraciones inseguras (como contraseñas débiles) en el servidor, no se enviarán alarmas en tiempo real. HSS resumirá todos los ataques en un día en su informe diario de alarma. También puede ver los ataques de bloqueo en la página **Intrusions** de la consola de HSS.

Consulta de los resultados de detección de agrietamiento de fuerza bruta

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 3-2 Acceso a HSS



Paso 3 En el cuadro de diálogo que se muestra, haga clic en **Try the new edition** para cambiar a la consola HSS (Nueva).

NOTA

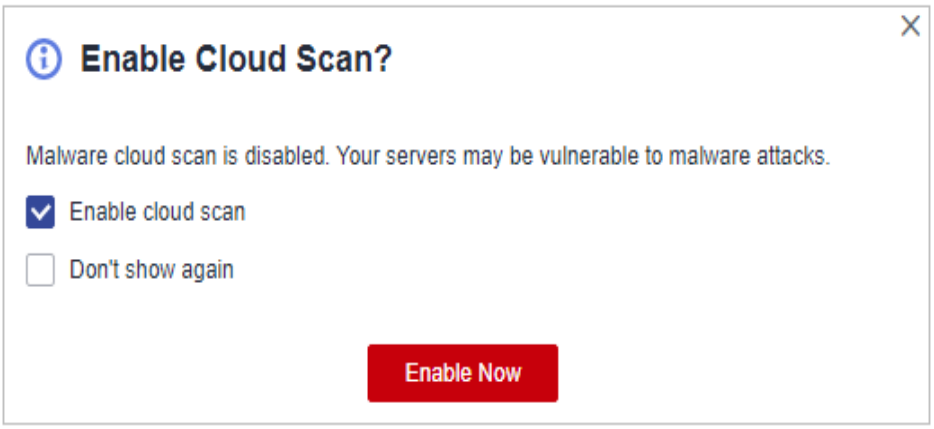
- Actualmente, HSS está disponible en las siguientes regiones: CN South-Guangzhou, CN-Hong Kong, AP-Bangkok, and AP-Singapore.
- En la consola HSS (Nueva), puede hacer clic en **Back to Old Console** en la esquina superior izquierda para cambiar a la consola HSS (Antigua).

- Si el análisis en la nube no está habilitado o accede a la consola HSS (Nuevo) por primera vez, se muestra el cuadro de diálogo **Enable Cloud Scan?**. Se recomienda seleccionar **Enable cloud scan**.

  NOTA

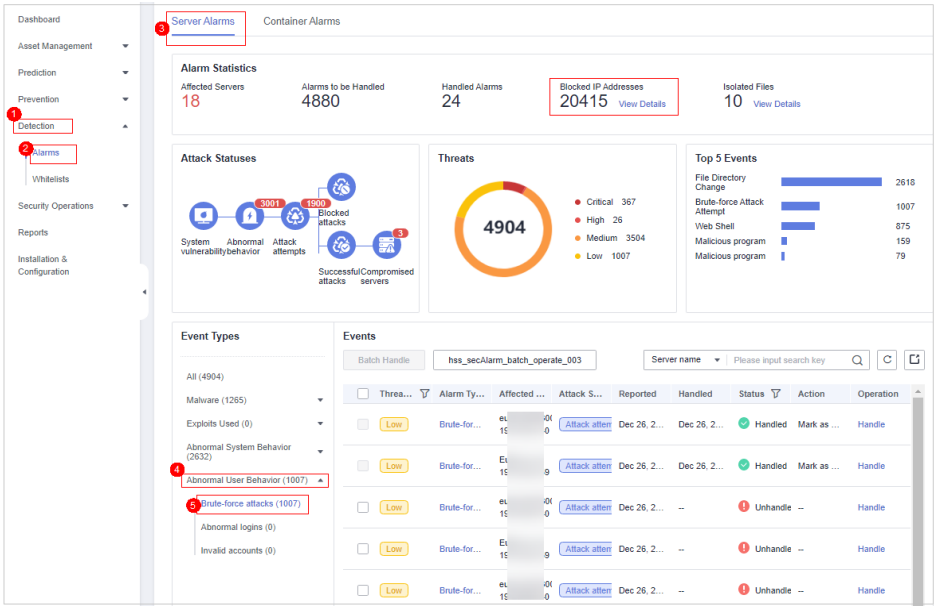
  – La función de escaneo en la nube es gratuita.
  – Una vez activada la función de análisis en la nube, se escanearán todos los servidores HSS. Algunas ediciones de cuota de HSS solo pueden admitir capacidades de análisis limitadas. Por lo tanto, se recomienda comprar la edición empresarial o superior para disfrutar de todas las capacidades de la función de escaneo en la nube.

Figura 3-3 Habilitar el análisis en la nube



Paso 4 En la tabla que se muestra después de hacer clic en **Brute-force attacks**, puede ver los ataques bloqueados en servidores protegidos.

Figura 3-4 Ataques de fuerza bruta



Paso 5 Haga clic en **View Details** en **Blocked IP Addresses** para comprobar las direcciones IP de origen, los tipos de ataque, el número de ataques interceptados, la hora de la primera y última intercepción y el estado de intercepción.

- **Blocked** indica que el ataque de fuerza bruta ha sido bloqueado por HSS.
- **Canceled** indica que ha desbloqueado la dirección IP de origen del ataque de fuerza bruta.

  NOTA

  De forma predeterminada, los atacantes SSH sospechosos están bloqueados durante 12 horas. Otros tipos de atacantes sospechosos están bloqueados durante 24 horas. Si una dirección IP bloqueada no realiza ataques de fuerza bruta en la duración de bloqueo predeterminada, se desbloqueará automáticamente.

----Fin

Gestión de direcciones IP bloqueadas

- Si un servidor es atacado con frecuencia, se recomienda corregir sus vulnerabilidades de manera oportuna y eliminar los riesgos.

  Se recomienda habilitar **2FA** y configurar **direcciones IP de inicio de sesión comunes** y la **lista blanca IP de inicio de sesión SSH**.

- Si una dirección IP válida está bloqueada por error (por ejemplo, después de que el personal de O&M introduzca contraseñas incorrectas varias veces), **desbloquee manualmente la dirección IP**.

AVISO

Si desbloqueó manualmente una dirección IP, pero los intentos de contraseña incorrectos de esta dirección IP alcanzan de nuevo el umbral, esta dirección IP se bloqueará de nuevo.

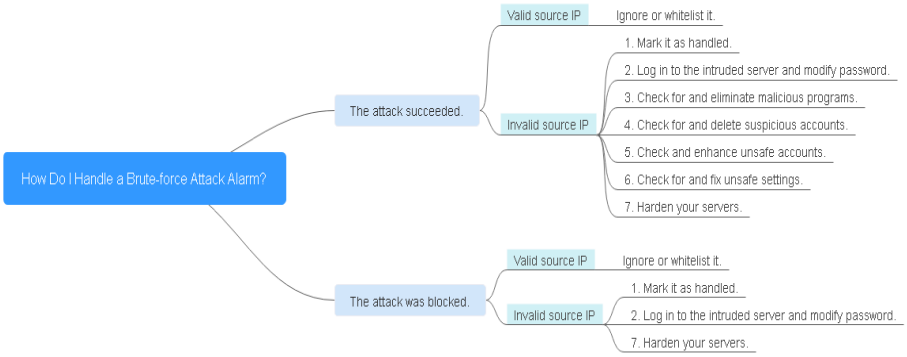
3.2 ¿Cómo manejo una alarma de ataque de fuerza bruta?

- Si un ataque de fuerza bruta tuvo éxito, tome medidas inmediatas para evitar que los atacantes realicen otras acciones, como la violación de datos, la realización de ataques DDoS o la implantación de ransomware, mineros o troyanos.
- Si se bloqueó un ataque de fuerza bruta, tome medidas inmediatas para mejorar sus servidores.

Mapa mental para la resolución de problemas

El siguiente mapa mental describe cómo manejar una alarma de ataque de fuerza bruta.

Figura 3-5 Mapa mental para la resolución de problemas



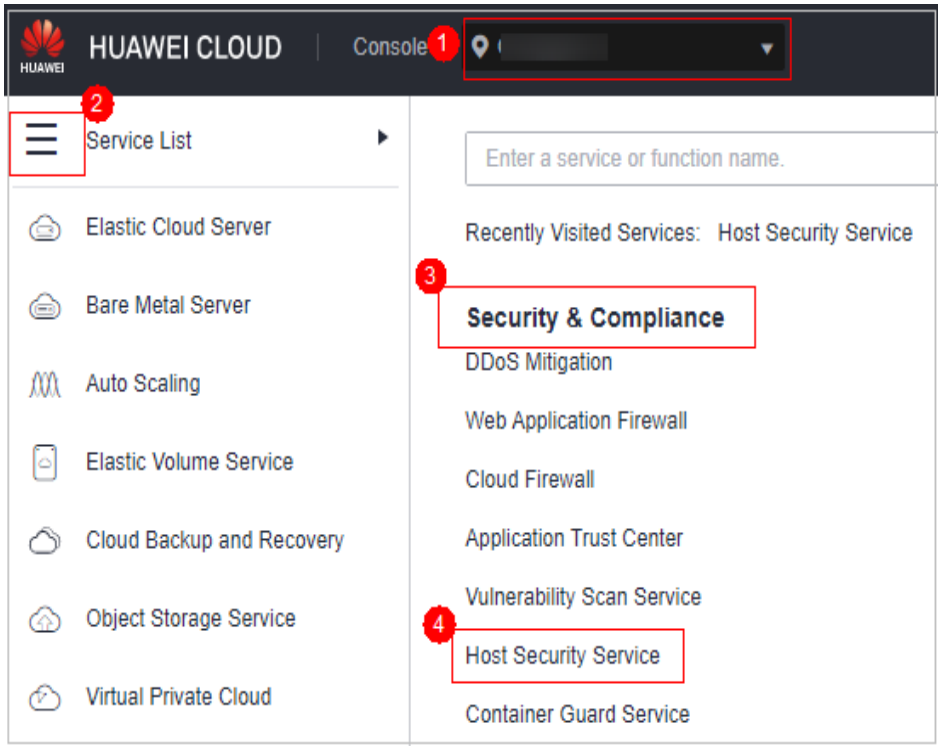
Manejo de la alarma de un ataque de fuerza bruta exitoso

Si recibió una notificación de alarma que indica que su cuenta ha sido descifrada, se le aconseja que endurezca sus servidores lo antes posible.

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 3-6 Acceso a HSS



Paso 3 En el cuadro de diálogo que se muestra, haga clic en **Try the new edition** para cambiar a la consola HSS (Nueva).

NOTA

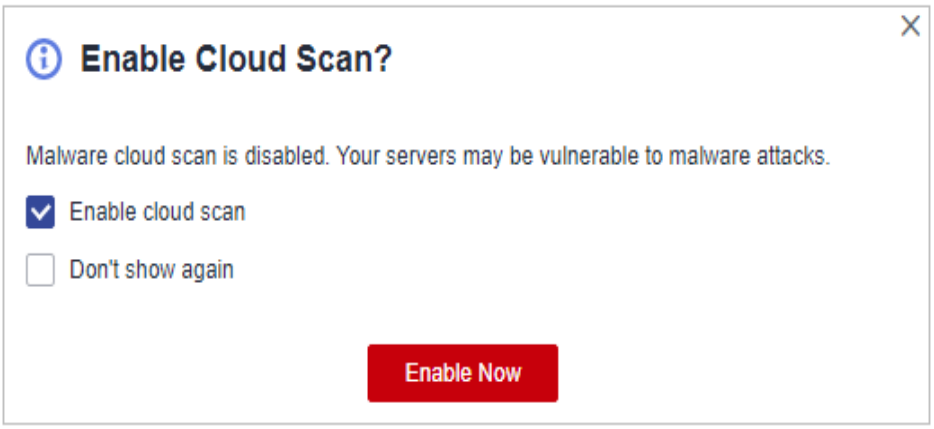
- Actualmente, HSS está disponible en las siguientes regiones: CN South-Guangzhou, CN-Hong Kong, AP-Bangkok, and AP-Singapore.
- En la consola HSS (Nueva), puede hacer clic en **Back to Old Console** en la esquina superior izquierda para cambiar a la consola HSS (Antigua).

- Si el análisis en la nube no está habilitado o accede a la consola HSS (Nuevo) por primera vez, se muestra el cuadro de diálogo **Enable Cloud Scan?**. Se recomienda seleccionar **Enable cloud scan**.

  NOTA

  – La función de escaneo en la nube es gratuita.
  – Una vez activada la función de análisis en la nube, se escanearán todos los servidores HSS. Algunas ediciones de cuota de HSS solo pueden admitir capacidades de análisis limitadas. Por lo tanto, se recomienda comprar la edición empresarial o superior para disfrutar de todas las capacidades de la función de escaneo en la nube.

Figura 3-7 Habilitar el análisis en la nube



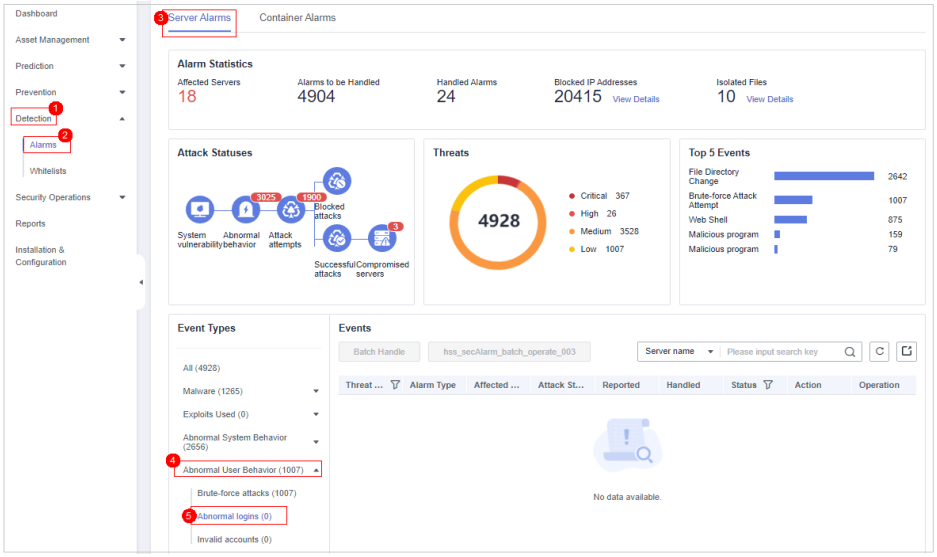
Paso 4 Compruebe si la dirección IP que activó la alarma es válida.

Elija **Detection** > **Alarms**. En el área **Event Types**, seleccione **Abnormal User Behavior** > **Abnormal logins** y compruebe la dirección IP de inicio de sesión.

- Si la dirección IP es de un usuario normal (por ejemplo, quien ha introducido una contraseña incorrecta varias veces pero ha iniciado sesión antes de que se bloquee su cuenta) su servidor no está entrometido. En este caso, puede hacer clic en **Handle** e ignorar el evento.
- Si la dirección IP no es válida, es posible que su servidor haya sido intrusado.

  En este caso, marque este evento como controlado, inicie sesión en el servidor intruso y cambie su contraseña a una más fuerte. Para más detalles, consulte **¿Cómo configuro una contraseña segura?**

Figura 3-8 Inicios de sesión anormales



Paso 5 Comprobar y eliminar programas maliciosos.

Elija **Malware** > **Malicious programs** y compruebe los eventos de alarma.

- Si encuentra programas maliciosos implantados en sus servidores, localícelos según sus rutas de proceso, los usuarios que los ejecutan y el tiempo de inicio.

Para eliminar un programa malicioso en un evento de alarma, haga clic en **Handle** en la fila de este evento y seleccione **Isolate and kill**.

- Si ha confirmado que todas las alarmas de programas maliciosos son falsas, vaya al **Paso 8**.

Paso 6 **Compruebe si hay registros de cambios de cuenta sospechosos.**

Seleccione **Asset Management** > **Asset Fingerprints** y haga clic en la pestaña **Account Information**. Detectar registros de cambios de cuenta sospechosos para evitar que los atacantes creen cuentas o aumenten los permisos de cuenta (por ejemplo, agregar permisos de inicio de sesión a una cuenta). Para más información, consulte **Comprobación del historial de operaciones** .

Paso 7 **Verificar y manejar cuentas inválidas.**

Elija **Detection** > **Alarms**. Elija **Abnormal User Behavior** > **Invalid accounts** para ver y manejar las alarmas de cuenta no válidas. Para obtener más información, consulte **Manejo de alarmas de servidor**

Paso 8 Compruebe y corrija la configuración insegura.

Compruebe y corrija políticas débiles de complejidad de contraseñas y configuraciones de software inseguras en sus servidores. Para obtener más información, consulte **Sugerencias sobre la corrección de configuraciones inseguras**.

Paso 9 Endurece sus servidores.

- Para obtener más información, consulte **Reforzamiento de la seguridad para inicios de sesión SSH en ECS de Linux**.

----Fin

Manejar la alarma de un ataque de fuerza bruta bloqueado

Compruebe si las direcciones IP bloqueadas pueden ser confiables. HSS bloqueará una dirección IP si tiene cinco o más intentos de ataque de fuerza bruta detectados en 30 segundos, o 15 o más intentos de ataque de fuerza bruta detectados en 3,600 segundos.

Restricciones y limitaciones

- Linux

  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.

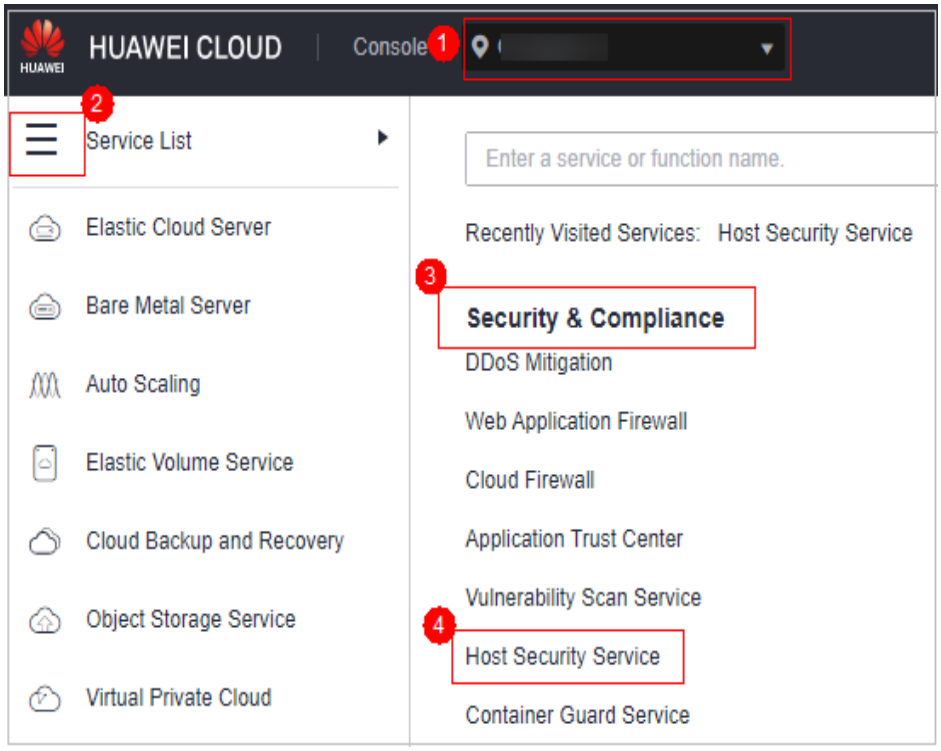
- Windows
  - Autorice el firewall de Windows cuando habilite la protección para un servidor Windows. No deshabilite el firewall de Windows durante el período de servicio del HSS. Si el firewall de Windows está deshabilitado, HSS no puede bloquear direcciones IP de ataque de fuerza bruta.
  - Si el firewall 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)**.

Figura 3-9 Acceso a HSS



Paso 3 En el cuadro de diálogo que se muestra, haga clic en **Try the new edition** para cambiar a la consola HSS (Nueva).

NOTA

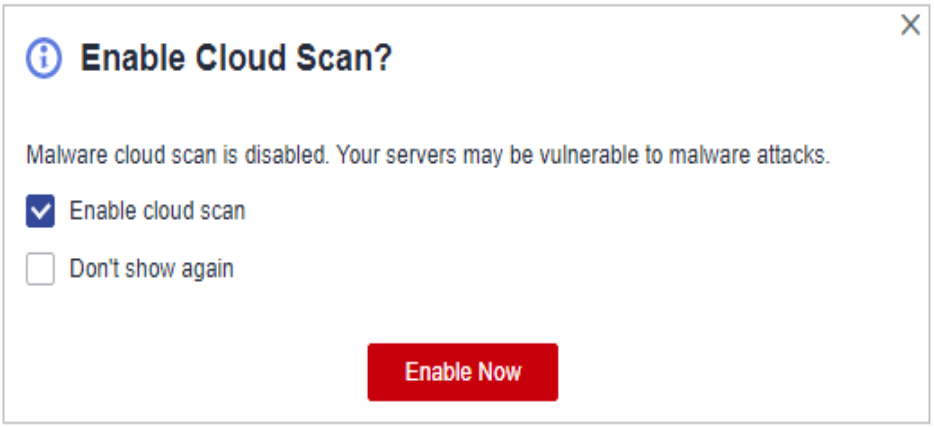
- Actualmente, HSS está disponible en las siguientes regiones: CN South-Guangzhou, CN-Hong Kong, AP-Bangkok, and AP-Singapore.
- En la consola HSS (Nueva), puede hacer clic en **Back to Old Console** en la esquina superior izquierda para cambiar a la consola HSS (Antigua).

- Si el análisis en la nube no está habilitado o accede a la consola HSS (Nuevo) por primera vez, se muestra el cuadro de diálogo **Enable Cloud Scan?**. Se recomienda seleccionar **Enable cloud scan**.

  NOTA

  – La función de escaneo en la nube es gratuita.
  – Una vez activada la función de análisis en la nube, se escanearán todos los servidores HSS. Algunas ediciones de cuota de HSS solo pueden admitir capacidades de análisis limitadas. Por lo tanto, se recomienda comprar la edición empresarial o superior para disfrutar de todas las capacidades de la función de escaneo en la nube.

Figura 3-10 Habilitar el análisis en la nube

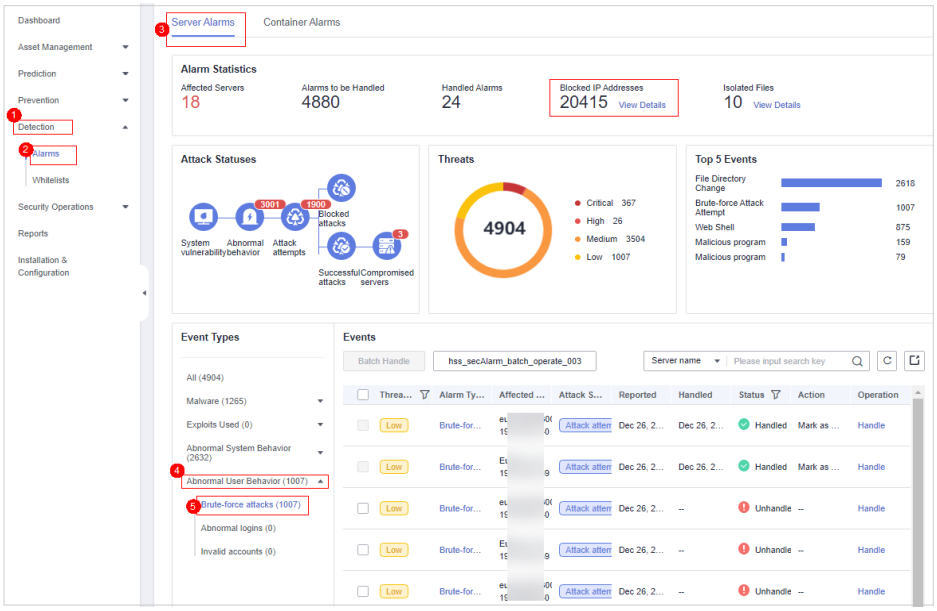


Paso 4 Elija **Detection** > **Alarms**. Elija **Abnormal User Behavior** > **Brute-force attacks** para ver los eventos de fuerza bruta de la cuenta.

Las alarmas de ataque de fuerza bruta se generarán si:

- El sistema utiliza contraseñas débiles, está bajo ataques de fuerza bruta y las direcciones IP de los atacantes están bloqueadas.
- Los usuarios no pueden iniciar sesión después de varios intentos de contraseña incorrectos y sus direcciones IP están bloqueadas.

Figura 3-11 Ataques de fuerza bruta



Paso 5 Compruebe si la dirección IP de inicio de sesión que activa la alarma es válida.

- Si la dirección IP es válida,
  - Para controlar una falsa alarma, haga clic en **Handle** en la fila del evento de alarma. Ignore o ponga en la lista blanca la dirección IP.

    Esto no desbloquea la dirección IP.
  - Para desbloquear la dirección IP, haga clic en **View Details** en **Blocked IP Addresses** y seleccione la dirección IP. Alternativamente, puede esperar a que se desbloquee automáticamente cuando expire su duración de bloqueo.

De forma predeterminada, los atacantes SSH sospechosos están bloqueados durante 12 horas. Otros tipos de atacantes sospechosos están bloqueados durante 24 horas.

- Si la dirección IP de origen es inválida o desconocida,

  Marque este evento como manejado.

  Inicie sesión inmediatamente en su servidor y cambie su contraseña por una más segura. También puede mejorar la defensa contra ataques de fuerza bruta siguiendo las instrucciones proporcionadas en **¿Cómo puedo defenderme de los ataques de fuerza bruta?**

----Fin

Enlaces útiles

- **¿Cómo Intercepta HSS los Ataques de Fuerza Bruta?**
- **¿Cómo desbloqueo una dirección IP?**

3.3 ¿Cómo puedo defenderme de los ataques de fuerza bruta?

Impacto de los ataques de fuerza bruta

Los intrusos que descifran cuentas de servidor pueden explotar los permisos para robar o manipular datos en servidores, interrumpiendo los servicios empresariales y causando grandes pérdidas.

Medidas preventivas

- Configurar la lista blanca de inicio de sesión SSH.

  La lista blanca de inicio de sesión SSH permite inicios de sesión solo desde direcciones IP de la lista blanca, lo que evita eficazmente la vulneración de la cuenta. Para obtener más información, consulte **Configuración de una lista blanca de direcciones IP de inicio de sesión de SSH**.

- Habilitar 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.

  Elija **Installation & Configuration**. En la pestaña **Two-Factor Authentication**, seleccione servidores y haga clic en **Enable 2FA**. Para obtener más información, consulte **Habilitar 2FA**.

- Utilice puertos no predeterminados.

  Cambie los puertos de gestión remota predeterminados 22 y 3389 a otros puertos.

- Configure las reglas de grupo de seguridad para evitar que las direcciones IP atacantes accedan a los puertos de servicio.

  NOTA

  Se recomienda permitir que solo las direcciones IP especificadas accedan a los puertos de gestión remota abiertos (por ejemplo, para el inicio de sesión en SSH y en el escritorio remoto).

  HSS **intercepta los ataques de fuerza bruta** en las cuentas del servidor en tiempo real y bloquea las direcciones IP de origen de los ataques. Puede **configurar reglas de grupo** para controlar el acceso a los servidores.

Para un puerto utilizado para el inicio de sesión remoto, puede establecer direcciones IP que tienen permiso para iniciar sesión remotamente en sus ECS.

Para permitir que la dirección IP **192.168.20.2** acceda de forma remota a ECS de Linux en un grupo de seguridad a través del protocolo SSH y el puerto 22, puede configurar la siguiente regla de grupo de seguridad.

Tabla 3-1 Configuración de direcciones IP para conectarse remotamente a ECS

Dirección	Protocolo/Aplicación	Puerto	Origen
Inbound	SSH	22	Por ejemplo, 192.168.20.2/32

- Establezca una contraseña segura.

  Comprobación de la política de contraseñas y **Detección de contraseñas débiles** puede encontrar cuentas que utilizan contraseñas débiles en sus servidores. Puede ver y manejar los riesgos de contraseña en la consola.

3.4 ¿Cómo lo hago si la función de prevención de craqueo de cuentas no tiene efecto en algunas cuentas de Linux?

Causas posibles

El servicio SSHD en el sistema de host no depende de **libwrap.so**.

NOTA

Como biblioteca de software libre, libwrap implementa la función universal de TCP Wrapper. Cualquier daemon que contenga **libwrap.so** puede usar las reglas de los archivos **/etc/hosts.allow** y **/etc/hosts.deny** para realizar un control de acceso sencillo en el host.

Solución

Inicie sesión en el servidor e instale el agente HSS. Ejecute el siguiente comando:

sh /usr/local/hostguard/conf/config_ssh_xinetd.sh.

Versiones de imágenes afectadas

- Las siguientes son imágenes de Gentoo que tienen el problema:
  - Gentoo Linux 17.0 64bit (40 GB)
  - Gentoo Linux 13.0 64bit (40 GB)
- Las siguientes son imágenes de OpenSUSE que tienen el problema:
  - OpenSUSE 42.2 64bit (40 GB)
  - OpenSUSE 13.2 64bit (40 GB)

3.5 ¿Cómo desbloqueo una dirección IP?

HSS bloqueará una dirección IP si tiene cinco o más intentos de ataque de fuerza bruta detectados en 30 segundos, o 15 o más intentos de ataque de fuerza bruta detectados en 3600 segundos. Si una dirección IP normal está bloqueada por error (por ejemplo, después de que el personal de O&M introduzca contraseñas incorrectas varias veces), puede desbloquear la dirección IP.

Si desbloqueó manualmente una dirección IP, pero los intentos de contraseña incorrectos de esta dirección IP alcanzan de nuevo el umbral, esta dirección IP se bloqueará de nuevo.

NOTA

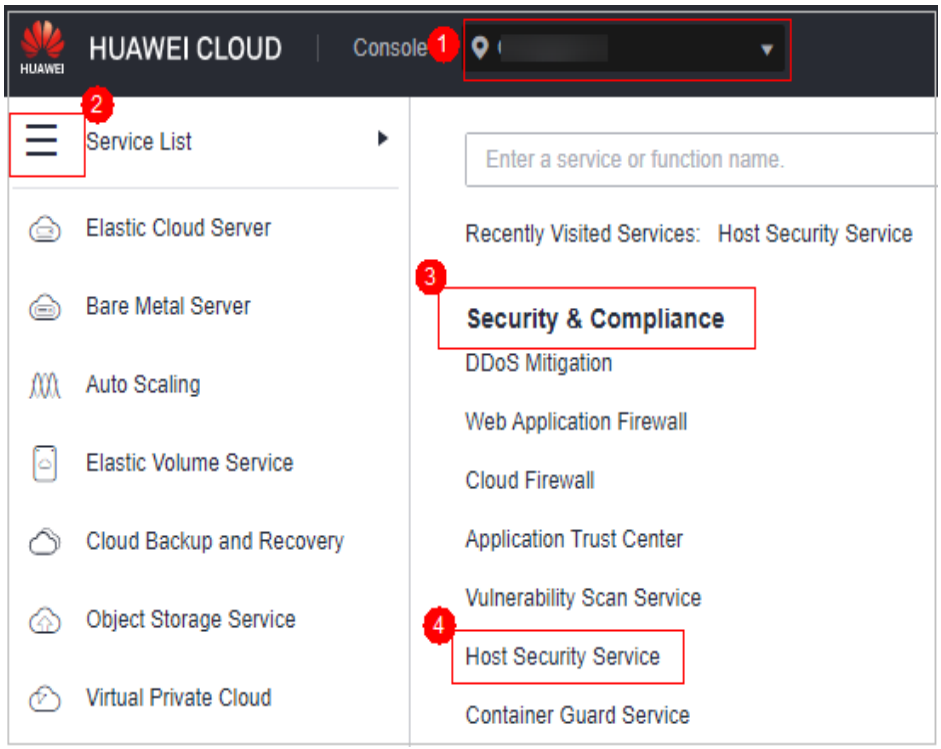
- De forma predeterminada, los atacantes SSH sospechosos están bloqueados durante 12 horas. Otros tipos de atacantes sospechosos están bloqueados durante 24 horas.
- Si una dirección IP bloqueada no realiza ataques de fuerza bruta en la duración de bloqueo predeterminada, se desbloqueará automáticamente.

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)**.

Figura 3-12 Acceso a HSS



Paso 3 En el cuadro de diálogo que se muestra, haga clic en **Try the new edition** para cambiar a la consola HSS (Nueva).

NOTA

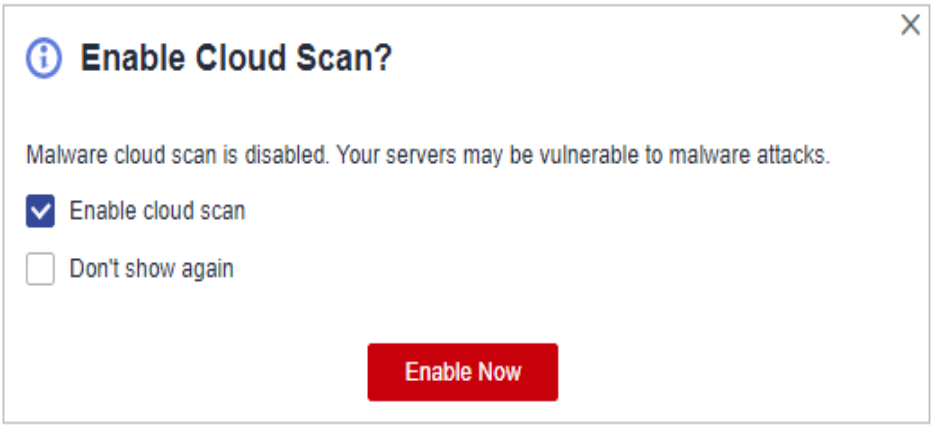
- Actualmente, HSS está disponible en las siguientes regiones: CN South-Guangzhou, CN-Hong Kong, AP-Bangkok, and AP-Singapore.
- En la consola HSS (Nueva), puede hacer clic en **Back to Old Console** en la esquina superior izquierda para cambiar a la consola HSS (Antigua).

- Si el análisis en la nube no está habilitado o accede a la consola HSS (Nuevo) por primera vez, se muestra el cuadro de diálogo **Enable Cloud Scan?**. Se recomienda seleccionar **Enable cloud scan**.

  NOTA

  – La función de escaneo en la nube es gratuita.
  – Una vez activada la función de análisis en la nube, se escanearán todos los servidores HSS. Algunas ediciones de cuota de HSS solo pueden admitir capacidades de análisis limitadas. Por lo tanto, se recomienda comprar la edición empresarial o superior para disfrutar de todas las capacidades de la función de escaneo en la nube.

Figura 3-13 Habilitar el análisis en la nube



Paso 4 En el árbol de navegación de la izquierda, elija **Detection** > **Alarms** y haga clic en **Server Alarms**.

Paso 5 En el área **Alarm Statistics**, haga clic en **View Details** en **Blocked IP Addresses**.

Figura 3-14 Direcciones IP bloqueadas

Paso 6 En la lista de direcciones IP bloqueadas, seleccione una dirección IP y haga clic en **Unblock**.

Figura 3-15 Desbloquear una dirección IP

----Fin

4 Contraseñas débiles y cuentas inseguras

4.1 ¿Cómo manejo una alarma de contraseña débil?

Los servidores que usan contraseñas débiles están expuestos a intrusiones. Si se informa de una alarma de contraseña débil, se le aconseja cambiar la contraseña alarmada inmediatamente.

Causas

- Si se usan contraseñas simples y coinciden con las de la biblioteca de contraseñas débiles, se generará una alarma de contraseñas débiles.
- Una contraseña utilizada por varias cuentas de miembros se considerará como una contraseña débil y desencadenará una alarma.

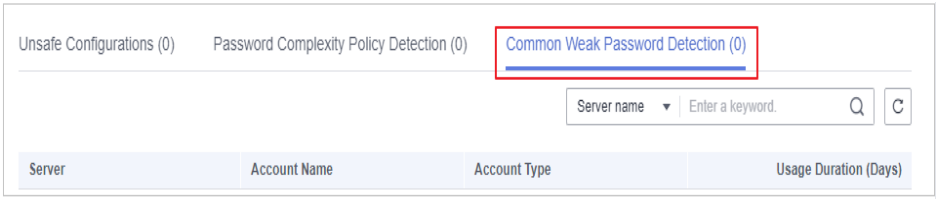
Comprobación y cambio de contraseñas débiles

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 **Prediction** > **Baseline Checks** y haga clic en la pestaña **Common Weak Password Detection**.

Figura 4-1 Contraseñas débiles comunes



Paso 4 Compruebe el servidor, el nombre de la cuenta, el tipo de cuenta y la duración de uso de la contraseña débil. Inicie sesión en el servidor y cambie la contraseña.

----Fin

Cambiar una contraseña débil

Sistema	Procedimiento	Observaciones
Windows OS	Para cambiar la contraseña en Windows 10, realice los siguientes pasos: 1. Inicie sesión en el Windows OS. 2. Haga clic en  en la esquina inferior izquierda y haga clic en  . 3. En la ventana **Windows Settings**, haga clic en **Accounts**. 4. Elija **Sign-in options** en el árbol de navegación. 5. En la pestaña **Sign-in options**, haga clic en **Change** en **Password**.	Ninguna
Linux OS	Inicie sesión en el servidor Linux y ejecute el siguiente comando: **passswd [<*user*>]**	Si no especifica ningún nombre de usuario, está cambiando la contraseña del usuario actual. Después de ejecutar el comando, introduzca la nueva contraseña como se le solicite. **NOTA** Reemplace <*user*> con el nombre de usuario.

Sistema	Procedimiento	Observaciones
Base de datos de MySQL	1. Inicie sesión en la base de datos de MySQL. 2. Ejecute el siguiente comando para comprobar la contraseña del usuario de la base de datos: **SELECT user, host, authentication_string From user;** Este comando es probablemente inválido en ciertas versiones de MySQL. En este caso, ejecute el siguiente comando: **SELECT user, host password From user;** 3. Ejecute el siguiente comando para cambiar la contraseña: **SET PASSWORD FOR'*Username*'@'*Host*'=PASSWORD('*New_password*');** 4. Ejecute el siguiente comando para actualizar la configuración de contraseña: **flush privileges;**	Ninguna
Base de datos de Redis	1. Abra el archivo **redis.conf** de configuración de la base de datos de Redis. 2. Ejecute el siguiente comando para cambiar la contraseña: **requirepass <*password*>;**	● Si ya hay una contraseña, el comando la cambiará por la nueva contraseña. ● Si no se ha establecido una contraseña, el comando establecerá la contraseña. **NOTA** Reemplace <*password*> con la nueva contraseña.
Tomcat	1. Abra el archivo de configuración **conf/tomcat-user.xml** en el directorio raíz de Tomcat. 2. Cambie el valor de **password** en el nodo **user** a una contraseña segura.	Ninguna

4.2 ¿Cómo configuro una contraseña segura?

Cumplir con las siguientes reglas:

- Utilice una contraseña de alta complejidad.

  La contraseña debe cumplir los siguientes requisitos:

a. Contiene al menos ocho caracteres.
b. Contiene al menos tres tipos de los siguientes caracteres:
   i. Letras mayúsculas (A-Z)
   ii. Letras minúsculas (a-z)
   iii. Digitales (0-9)
   iv. Caracteres especiales
c. La contraseña no puede ser igual al nombre de usuario ni al nombre de usuario al revés.

- No utilice contraseñas débiles comunes que sean fáciles de descifrar, que incluye:
  - Cumpleaños, nombre, tarjeta de identificación, número de teléfono móvil, dirección de correo electrónico, ID de usuario, hora o fecha
  - Dígitos y letras consecutivos, caracteres de teclado adyacentes o contraseñas en tablas de arco iris
  - Frases
  - Palabras comunes, como nombres de empresas, **admin** y **root**
- No utilice contraseñas vacías o predeterminadas.
- No vuelva a utilizar las últimas cinco contraseñas que utilizó.
- Utilice diferentes contraseñas para diferentes sitios web y cuentas.
- No utilice el mismo par de nombre de usuario y contraseña para varios sistemas.
- Cambie su contraseña al menos una vez cada 90 días.
- Si una cuenta tiene una contraseña inicial, forzar al usuario a cambiar la contraseña en el primer inicio de sesión o dentro de un período de tiempo limitado.
- Se recomienda establecer una política de bloqueo para todas las cuentas. Si las fallas consecutivas de inicio de sesión de una cuenta superan cinco veces, la cuenta se bloqueará y se desbloqueará automáticamente en 30 minutos.
- Se recomienda establecer una política de cierre de sesión. Las cuentas que hayan estado inactivas durante más de 10 minutos se cerrarán o bloquearán automáticamente.
- Se recomienda forzar a los usuarios a cambiar las contraseñas iniciales de sus cuentas en su primer inicio de sesión.
- Se recomienda conservar los registros de inicio de sesión de la cuenta durante al menos 180 días. Los registros no pueden contener contraseñas de usuario.

4.3 ¿Por qué se siguen reportando las débiles alarmas de contraseña después de deshabilitar la débil política de contraseñas?

Si tiene contraseñas mejoradas antes de deshabilitar la política de contraseñas débiles, la alarma de contraseñas débiles no se volverá a informar.

Si no mejora las contraseñas antes de deshabilitar la política de contraseñas débiles, la alarma notificada persistirá y se conservará durante 30 días.

- Para mejorar la seguridad del servidor, se recomienda modificar las cuentas con contraseñas débiles de manera oportuna, como las cuentas de SSH.

- Para proteger los datos internos de su servidor, se recomienda modificar las cuentas de software que utilizan contraseñas débiles, como las cuentas de MySQL y las cuentas de 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 y no deshabilita el análisis de contraseña débil, HSS comprobará automáticamente la configuración al día siguiente por la mañana temprano.

5 Intrusiones

5.1 ¿Qué hago si mis servidores están sujetos a un ataque minero?

Tomar medidas inmediatas para contener el ataque, evitando que los mineros ocupen la CPU o afecten a otras aplicaciones. Si un servidor es intrusado por un programa de minería, el programa de minería puede penetrar en la intranet y persistir en el servidor intruso.

También debe endurecer sus servidores para bloquear mejor las intrusiones.

Procedimiento de resolución de problemas

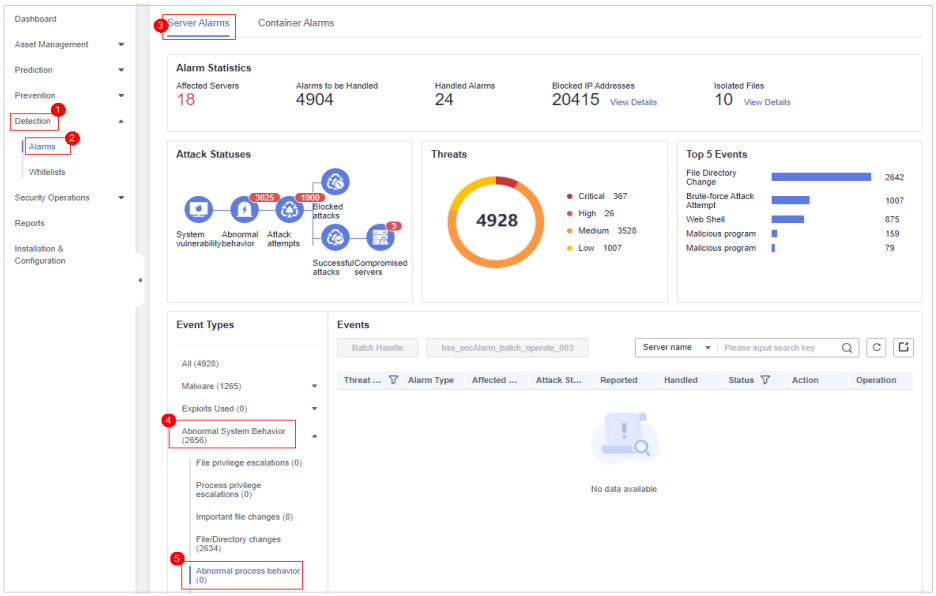
Paso 1 **Iniciar sesión en la consola de gestión**.

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 Comprueba los eventos de **Abnormal process behavior**.

Elija **Detection** > **Alarms** y haga clic en **Server Alarms**. Elija **Abnormal System Behavior** > **Abnormal process behavior** para ver y manejar las alarmas de comportamiento anormal del proceso. Haga clic en **Handle** en la columna **Operation** de un evento.

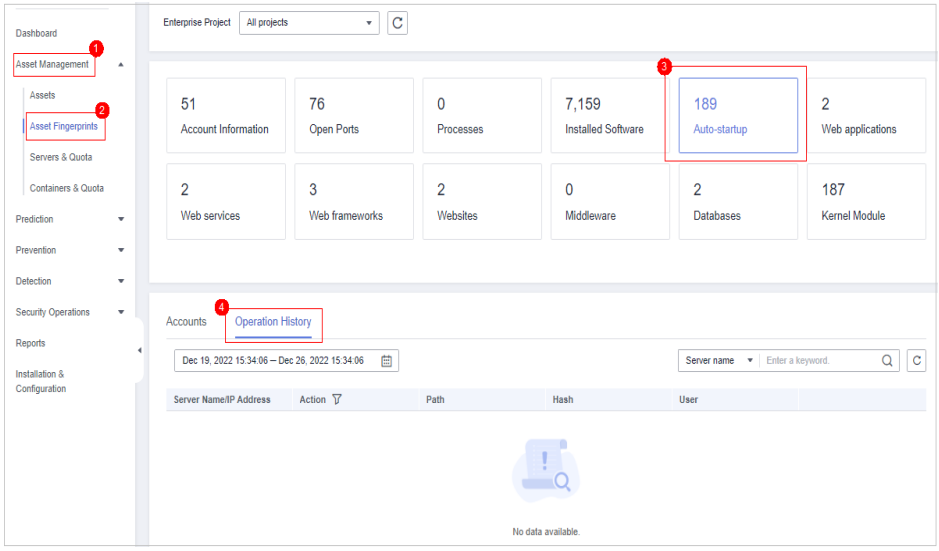
Figura 5-1 Manejo de comportamientos anormales del proceso



Paso 4 Compruebe los elementos de inicio automático. Algunos de sus elementos de inicio automático probablemente fueron creados por atacantes para iniciar programas de minería al reiniciar el servidor.

Elija **Asset Management** > **Asset Fingerprints**, haga clic en **Auto-startup**, y seleccione **Operation History** para ver el historial de cambios.

Figura 5-2 Comprobación de elementos de inicio automático



----Fin

Servidores de endurecimiento

Después de eliminar los programas mineros, endurecer sus servidores para defenderse mejor contra las intrusiones.

Linux servers

1. Permita que HSS analice automáticamente sus servidores y aplicaciones a primera hora de la mañana todos los días para ayudarle a detectar y eliminar los riesgos de seguridad.
2. Establezca contraseñas más seguras para todas las cuentas (incluidas las cuentas de sistema y aplicación), o cambie el modo de inicio de sesión a inicio de sesión basado en clave.
   a. Establezca la contraseña de seguridad. Para obtener más información, consulte **¿Cómo configuro una contraseña segura?**.
   b. Utilice una clave para iniciar sesión en el servidor. Para obtener más información, consulte **Uso de una clave privada para iniciar sesión en el ECS de Linux**.
3. Controle estrictamente el uso de las cuentas de administrador del sistema. Conceda solo los permisos mínimos requeridos para aplicaciones y middleware y controle estrictamente su uso.
4. Configurar reglas de acceso en grupos de seguridad. Abra solo los puertos necesarios. Para puertos especiales (como los puertos de inicio de sesión remoto), solo permita el acceso desde direcciones IP especificadas o utilice hosts VPN o bastion para establecer sus propios canales de comunicación. Para obtener más información, consulte **Reglas de grupo de seguridad**.

Windows servers

Utilice HSS para verificar y eliminar los riesgos de seguridad de forma integral. Mejore la seguridad de su cuenta, contraseña y autorización.

- **Endurecimiento de seguridad de cuenta**

Cuenta	Descripción	Procedimiento
Asegurar la seguridad predeterminada de la cuenta.	• Deshabilitar usuario **Guest**. • Desactivar y eliminar cuentas innecesarias. (Se recomienda desactivar las cuentas inactivas durante tres meses antes de eliminarlas.)	1. Abra **Control Panel**. 2. Haga clic en **Administrative Tools**. Abra **Computer Management**. 3. Seleccione **System Tools** > **Local Users and Groups** > **Users**. 4. Haga doble clic en **Guest**. En la ventana **Guest Properties**, seleccione **Account is disabled**. 5. Haga clic en **OK**.
Asignar cuentas con solo los permisos necesarios a los usuarios.	Crear usuarios y grupos de usuarios de tipos específicos. Ejemplo: administradores, usuarios de bases de datos, usuarios de auditoría	1. Abra **Control Panel**. 2. Haga clic en **Administrative Tools**. Abra **Computer Management**. 3. Elija **System Tools** > **Local Users and Groups**. Cree usuarios y grupos según sea necesario.

Cuenta	Descripción	Procedimiento
Comprobar y eliminar periódicamente cuentas innecesarias.	Eliminar o bloquear periódicamente cuentas innecesarias.	1. Abra **Control Panel**. 2. Haga clic en **Administrative Tools**. Abra **Computer Management**. 3. Elija **System Tools** > **Local Users and Groups**. 4. Elija **Users** o **User Groups** y elimine usuarios innecesarios o grupos de usuarios.
No mostrar el último nombre de usuario.	Prohibir que la página de inicio de sesión muestre el último usuario registrado.	1. Abra **Control Panel**. 2. Haga clic en **Administrative Tools**. Abra **Local Security Policy**. 3. Elija **Local Policies** > **Security Options**. 4. Haga doble clic en **Interactive logon: Do not display last user name**. 5. En el cuadro de diálogo que aparece, seleccione **Enable** y haga clic en **OK**.

- **Endurecimiento de seguridad de contraseña**

Configuración	Descripción	Procedimiento
Complejidad	De acuerdo con los requisitos establecidos en **¿Cómo configuro una contraseña segura?**	1. Abra **Control Panel**. 2. Haga clic en **Administrative Tools**. Abra **Local Security Policy**. 3. Elija **Account Policies** > **Password Policy**. 4. Habilite la política **Password must meet complexity requirements**.
Maximum Password Age (Duración máxima de la contraseña)	En el modo de autenticación de contraseña estática, forzar a los usuarios a cambiar sus contraseñas cada 90 días o a intervalos más cortos.	1. Abra **Control Panel**. 2. Haga clic en **Administrative Tools**. Abra **Local Security Policy**. 3. Elija **Account Policies** > **Password Policy**. 4. Establezca **Maximum password age** en 90 días o menos.
Política de bloqueo de cuenta	En el modo de autenticación de contraseña estática, bloquee una cuenta de usuario si la autenticación del usuario falla durante 10 veces consecutivas.	1. Abra **Control Panel**. 2. Haga clic en **Administrative Tools**. Abra **Local Security Policy**. 3. Elija **Account Policies** > **Account Lockout Policy**. 4. Establezca **Account lockout threshold** en **10** o más pequeño.

- **Endurecimiento de seguridad de autorización**

Autorización	Descripción	Procedimiento
Apagados remotos	Asignar el permiso **Force shutdown from a remote system** sólo al grupo **Administrators**.	1. Abra **Control Panel**. 2. Haga clic en **Administrative Tools**. Abra **Local Security Policy**. 3. Elija **Local Policies** > **User Rights Assignment**. 4. Asignar el permiso **Force shutdown from a remote system** sólo al grupo **Administrators**.
Apagado local	Asignar el permiso **Shut down the system** sólo al grupo **Administrators**.	1. Abra **Control Panel**. 2. Haga clic en **Administrative Tools**. Abra **Local Security Policy**. 3. Elija **Local Policies** > **User Rights Assignment**. 4. Asignar el permiso **Shut down the system** sólo al grupo **Administrators**.
Asignación de derechos de usuario	Asigne el permiso **Take ownership of files or other objects** sólo al grupo **Administrators**.	1. Abra **Control Panel**. 2. Haga clic en **Administrative Tools**. Abra **Local Security Policy**. 3. Elija **Local Policies** > **User Rights Assignment**. 4. Asignar el permiso **Shut down the system** sólo al grupo **Administrators**.
Inicio de sesión	Autorizar a los usuarios a iniciar sesión en el equipo localmente.	1. Abra **Control Panel**. 2. Haga clic en **Administrative Tools**. Abra **Local Security Policy**. 3. Elija **Local Policies** > **User Rights Assignment**. 4. Asigne el permiso **Allow log on locally** a los usuarios que desea autorizar.
Acceso desde la red	Permitir que solo los usuarios autorizados accedan a este equipo desde la red (por ejemplo, mediante uso compartido de red). No se permite el acceso desde otras terminales.	1. Abra **Control Panel**. 2. Haga clic en **Administrative Tools**. Abra **Local Security Policy**. 3. Elija **Local Policies** > **User Rights Assignment**. 4. Asigne el permiso **Access this computer from the network** a los usuarios que desea autorizar.

5.2 ¿Por qué un proceso todavía está aislado después de que fue incluido en la lista blanca?

Después de agregar un proceso a la lista blanca, ya no activará ciertas alarmas, pero su aislamiento no se cancelará automáticamente.

Aislamiento y eliminación de un programa malicioso

- Elija **Installation & Configuration** y haga clic en la pestaña **Security Configuration**. Haga clic en la pestaña **Isolation and Killing of Malicious Programs** y habilite esta función.
- Elija **Detection** > **Alarms**. En el área **Events**, aísle y elimine manualmente los programas maliciosos.

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.

Cancelación del aislamiento de archivos

- Elija **Detection** > **Events**. En el área **Alarm Statistics**, haga clic en **View Details** en **Isolated Files** y busque el servidor de destino y haga clic en **Restore** en la columna **Operation**.

Después de cancelar el aislamiento, se restaurarán los permisos de lectura/escritura de los archivos, pero los procesos terminados no se iniciarán automáticamente.

5.3 ¿Qué hago si se detecta un proceso de minería en un servidor?

Se recomienda:

1. Hacer copias de respaldo de los datos y deshabilitar los puertos innecesarios.
2. Establecer una contraseña de servidor más segura.
3. Habilitar HSS. Sus servidores estarán protegidos de los procesos de minería por sus funciones de detección de intrusos, como la prevención de agrietamiento de cuentas, la detección remota de inicio de sesión, la detección de programas maliciosos y la detección de shell web; así como la eliminación de programas maliciosos y funciones de fijación de vulnerabilidades.

5.4 ¿Qué debo hacer si encuentro que mis servidores atacan a otros?

Si sus servidores están lanzando ataques, pueden estar infectados con troyanos. Se recomienda reinstalar el sistema operativo y establecer contraseñas seguras para endurecer los servidores y aplicaciones como phpStudy y Redis. Las contramedidas son las siguientes:

- Establezca contraseñas seguras para todas las cuentas. No utilice contraseñas predeterminadas u otras contraseñas que sean fáciles de adivinar.

- Configurar políticas de grupo de seguridad. Establezca direcciones IP de acceso fijo para puertos de servicio no público para evitar su exposición a Internet.
- Actualice el sistema y las aplicaciones, instalando los parches más recientes de manera oportuna.
- Haga copias de respaldo de los datos con regularidad.
- Elimine o cambie el nombre de la carpeta **phpmyadmin**.

5.5 ¿Por qué no se detectan algunos ataques a servidores?

- No se pueden detectar las intrusiones en sus servidores antes de que HSS esté habilitado.
- Si ha adquirido HSS, recuerde habilitarlo para detectar intrusiones.
- No se pueden detectar ataques web, porque HSS principalmente defiende sus servidores. Para proteger sitios web, puede consultar el Arquitecto de soluciones de seguridad o utilizar otros servicios seguros (como Web Application Firewall y Anti-DDoS).

5.6 ¿Puedo desbloquear una dirección IP bloqueada por HSS y cómo?

Si puede desbloquear una dirección IP depende de por qué se bloqueó. Una dirección IP se bloqueará si se considera como la fuente de un ataque de fuerza bruta, listada en la lista negra de IP común, o no en la lista blanca de IP que establezca.

Comprobación de ataques de craqueo de cuenta

- HSS bloquea las direcciones IP atacantes para evitar intrusiones. La duración de bloqueo para ataques SSH sospechosos es de 12 horas y para otros ataques sospechosos es de 24 horas. Si una dirección IP bloqueada no realiza ataques de fuerza bruta en la duración de bloqueo predeterminada, se desbloqueará automáticamente.
- Si está seguro de que se puede confiar en una dirección IP de origen, puede desbloquearla manualmente. Seleccione **Detection** > **Alarms**, haga clic en **View Details** en **Blocked IP Addresses**, y desbloquee la dirección IP en el panel desplegable que se muestra.

  Si desbloqueó manualmente una dirección IP, pero los intentos de contraseña incorrectos de esta dirección IP superan de nuevo el umbral, esta dirección IP se bloqueará de nuevo.

Dirección IP en la lista negra de IP común

No puede desbloquear manualmente dichas direcciones IP.

Dirección IP que no está en la lista blanca de IP de inicio de sesión de SSH

Si ha configurado la **lista blanca de IP de inicio de sesión de SSH**, se bloquearán las direcciones IP que no estén en la lista blanca. Para desbloquear una dirección IP, agréguela a la lista blanca.

5.7 ¿Por qué una dirección IP bloqueada se desbloquea automáticamente?

Si una dirección IP bloqueada no realiza ataques de fuerza bruta en las próximas 24 horas, la dirección IP se desbloqueará automáticamente.

6 Inicios de sesión anormales

6.1 ¿Por qué sigo recibiendo alarmas de inicio de sesión remoto después de configurar la lista blanca de IP de inicio de sesión?

Incluso las direcciones IP de la lista blanca pueden activar ciertas alarmas. La lista blanca de direcciones IP de inicio de sesión SSH, la lista blanca de inicio de sesión y las funciones de inicio de sesión remoto se centran en diferentes aspectos de la seguridad, como se describe en **Tabla 6-1**.

Tabla 6-1 Funciones

Función	Descripción	Cómo enmascarar la alarma
Lista blanca de direcciones IP de inicio de sesión SSH	Solo las direcciones IP de esta lista blanca pueden iniciar sesión en servidores especificados a través de SSH. **AVISO** Para evitar problemas de conexión, asegúrese de que no se han perdido las direcciones IP necesarias antes de habilitar esta función.	-
Lista blanca de inicio de sesión	Para reducir las falsas alarmas de ataque de fuerza bruta, agregue direcciones IP de inicio de sesión de confianza y sus direcciones IP de servidor de destino a esta lista blanca.	Elija **Detection** > **Whitelists**. Haga clic en la pestaña **Login Whitelist** y agregue direcciones IP. HSS no generará alarmas de fuerza bruta para estas direcciones IP.

Función	Descripción	Cómo enmascarar la alarma
Inicio de sesión remoto	Los inicios de sesión no desde **Common Login Locations** y **Common Login IP Addresses** activarán alarmas de inicio de sesión remoto. Se le informará de las nuevas direcciones IP que inician sesión en sus servidores.	Elija **Installation & Configuration** y haga clic en **Security Configuration**. Agregue información de inicio de sesión en las pestañas **Common Login Locations** y **Common Login IP Addresses**. Los inicios de sesión incluidos en la lista blanca ya no activarán alarmas remotas.

6.2 ¿Cómo puedo comprobar la dirección IP del usuario de un inicio de sesión remoto?

Políticas de alarma

La función de detección de inicio de sesión remoto comprueba los inicios de sesión remotos en sus servidores en tiempo real. HSS genera una alarma si detecta inicios de sesión desde ubicaciones distintas de las **ubicaciones de inicio de sesión comunes que establezca**.

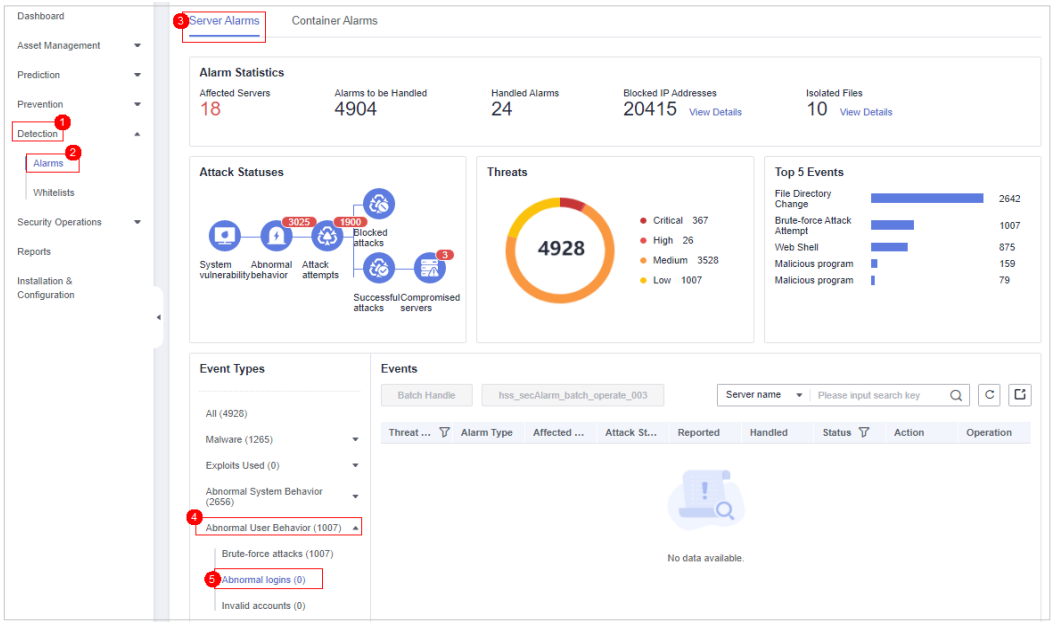
Consulta de registros de inicio de sesión remoto en la consola

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**.

Paso 3 Como se muestra en la **Figura 6-1**, compruebe el **Abnormal logins**. Haga clic en **Remote Login** y haga clic en el nombre de la alarma para ver los detalles.

Figura 6-1 Inicio de sesión anormal



----Fin

Consulta local de registros de inicio de sesión remoto

Para servidores Linux, puede ver los registros de los directorios **/var/log/secure** y **/var/log/message** o ejecutar el comando **last** para comprobar si hay registros de inicio de sesión anormales.

6.3 ¿Qué puedo hacer si se informa de una alarma que indica un inicio de sesión exitoso?

- Esta alarma no indica necesariamente un problema de seguridad. Si ha seleccionado **Successful Logins** en el área **Real-Time Alarm Notifications** HSS enviará alarmas cuando detecte cualquier inicio de sesión exitoso.
- Si todas las cuentas de sus ECS son gestionadas por un único administrador, estas alarmas les ayudan a monitorear cómodamente las cuentas del sistema.
- Si las cuentas del sistema son gestionadas por varios administradores, o diferentes servidores son gestionados por diferentes administradores, demasiadas alarmas interrumpirán al personal de O&M. En este caso, se recomienda desactivar el elemento de alarma.
- Las alarmas de este evento no necesariamente indican ataques. Los inicios de sesión desde direcciones IP válidas no son ataques.

7 Configuración insegura

7.1 ¿Cómo instalo un PAM y configuro una política de complejidad de contraseña adecuada en un sistema operativo Linux?

Instalación de un PAM

La política de complejidad de contraseñas no se puede comprobar si no se está ejecutando un módulo de autenticación conectable (PAM) en el sistema.

Para Debian o Ubuntu, ejecute el comando **apt-get install libpam-cracklib** como administrador para instalar un PAM.

NOTA

Un PAM se instala y se ejecuta por defecto en CentOS, Fedora y EulerOS.

Configuración de una política de complejidad de contraseñas

Una política de complejidad de contraseña adecuada sería: la contraseña debe contener al menos ocho caracteres y debe contener letras mayúsculas, minúsculas, números y caracteres especiales.

NOTA

Las configuraciones anteriores son requisitos básicos de seguridad. Para obtener más configuraciones de seguridad, ejecute los siguientes comandos para obtener información de ayuda en sistemas operativos Linux:

- Para CentOS, Fedora y EulerOS basados en Red Hat 7.0, ejecute:
  man pam_pwquality
- Para otros sistemas operativos Linux, ejecute:
  man pam_cracklib

- CentOS, Fedora y EulerOS
  a. Ejecute el siguiente comando para editar el archivo **/etc/pam.d/system-auth**:
     vi /etc/pam.d/system-auth

b. Encuentre la siguiente información en el archivo:
   - Para CentOS, Fedora y EulerOS basados en Red Hat 7.0:

     password requisite pam_pwquality.so try_first_pass retry=3 type=
   - Para otros sistemas CentOS, Fedora y EulerOS:

     password requisite pam_cracklib.so try_first_pass retry=3 type=

c. Agregue los siguientes parámetros y sus valores: **minlen**, **dcredit**, **ucredit**, **lcredit** y **ocredit**. Si el archivo ya tiene estos parámetros, cambie sus valores. Para obtener más información, consulte **Tabla 7-1**.

   Ejemplo:

   password requisite pam_cracklib.so try_first_pass retry=3 minlen=8 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 type=

   NOTA

   Establezca **dcredit**, **ucredit**, **lcredit** y **ocredit** en números negativos.

Tabla 7-1 Descripción de parámetro

Parámetro	Descripción	Ejemplo
minlen	Longitud mínima de una contraseña. Por ejemplo, si desea que la longitud mínima sea ocho, establezca el valor **minlen** en 8.	minlen=8
dcredit	Número de dígitos Un valor negativo (por ejemplo, **-N**) indica el número (por ejemplo, N) de dígitos requeridos en una contraseña. Un valor positivo indica que no hay límite.	dcredit=-1
ucredit	Número de letras mayúsculas Un valor negativo (por ejemplo, **-N**) indica el número (por ejemplo, N) de letras mayúsculas requeridas en una contraseña. Un valor positivo indica que no hay límite.	ucredit=-1
lcredit	Número de letras minúsculas Un valor negativo (por ejemplo, **-N**) indica el número (por ejemplo, N) de letras minúsculas requeridas en una contraseña.A positive value indicates that there is no limit.	lcredit=-1

Parámetro	Descripción	Ejemplo
ocredit	Número de caracteres especiales Un valor negativo (por ejemplo, **-N**) indica el número (por ejemplo, N) de caracteres especiales requeridos en una contraseña. Un valor positivo indica que no hay límite.	ocredit=-1

- Debian y Ubuntu
  a. Ejecute el siguiente comando para editar el archivo **/etc/pam.d/common-password**:

     vi /etc/pam.d/common-password
  b. Encuentre la siguiente información en el archivo:

     password requisite pam_cracklib.so retry=3 minlen=8 difok=3
  c. Agregue los siguientes parámetros y sus valores: **minlen**, **dcredit**, **ucredit**, **lcredit** y **ocredit**. Si el archivo ya tiene estos parámetros, cambie sus valores. Para obtener más información, consulte **Tabla 7-1**.

     Ejemplo:

     password requisite pam_cracklib.so retry=3 minlen=8 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 difok=3

7.2 ¿Cómo configuro una política de complejidad de contraseña adecuada en un sistema operativo Windows?

Una política de complejidad de contraseña adecuada sería: ocho caracteres para la longitud de una contraseña y al menos tres tipos de los siguientes caracteres utilizados: letras mayúsculas, letras minúsculas, dígitos y caracteres especiales.

Realice los siguientes pasos para establecer una política de seguridad local:

Paso 1 Inicie sesión en el sistema operativo como usuario **Administrator**. Elija **Start** > **Control Panel** > **System and Security** > **Administrative Tools**. En la carpeta **Administrative Tools**, haga doble clic en **Local Security Policy**.

NOTA

También puede hacer clic en **Start** y escribir **secpol.msc** en el cuadro **Search programs and files**.

Paso 2 Elija **Account Policies** > **Password Policy** y realice las siguientes operaciones.

- Haga doble clic en **Password must meet complexity requirements**, seleccione **Enable** y haga clic en **OK** para habilitar la política.
- Haga doble clic en **Minimum password length** y escriba la longitud (superior o igual a **8**) y haga clic en **OK** para establecer la política.

Paso 3 Ejecute el comando **gpupdate** para actualizar la configuración del sistema. Después de la actualización exitosa, la configuración tendrá efecto en el sistema.

----Fin

8 Gestión de vulnerabilidades

8.1 ¿Cómo soluciono las vulnerabilidades?

Procedimiento

Paso 1 **Comprobar los resultados de detección de vulnerabilidades**.

Paso 2 Basado en las soluciones proporcionadas, **corrija vulnerabilidades** una por una en orden descendente por gravedad.

- Reinicie el sistema operativo Windows después de corregir sus vulnerabilidades.
- Reinicie el sistema operativo Linux después de corregir las vulnerabilidades del kernel.

Paso 3 HSS escanea todos los servidores Linux, servidores Windows y servidores Web-CMS en busca de vulnerabilidades cada mañana temprano. Después de corregir las vulnerabilidades, se recomienda realizar una comprobación inmediatamente para verificar el resultado.

----Fin

8.2 ¿Qué hago si todavía existe una alarma después de haber solucionado una vulnerabilidad?

Realice las siguientes operaciones para localizar la causa y solucionar los problemas.

NOTA

Para obtener más información sobre cómo corregir vulnerabilidades, consulte **Solucionar vulnerabilidades y verificar el resultado**.

Posibles causas y soluciones en un servidor Linux

- No se han configurado fuentes de yum.

  En este caso, configure una fuente yum adecuada para su sistema operativo Linux y corrija la vulnerabilidad de nuevo.
- La fuente yum no tiene el último paquete de actualización del software correspondiente.

Cambie a la fuente yum que tiene el paquete requerido y corrija la vulnerabilidad de nuevo.

- El entorno de intranet no se puede conectar a Internet.

  Los servidores necesitan acceder a Internet y utilizar fuentes externas de yum para corregir vulnerabilidades. Si sus servidores no pueden acceder a Internet o las fuentes de imagen externas no pueden proporcionar servicios estables, puede utilizar la fuente de imagen.

- La versión antigua del kernel permanece.

  Las versiones antiguas del núcleo a menudo permanecen en los servidores después de la actualización. Puede ejecutar los **comandos de verificación** para comprobar si la versión actual del núcleo cumple con los requisitos de corrección de vulnerabilidades. Si lo hace, ignore la vulnerabilidad en la pestaña **Linux Vulnerabilities** de la página **Vulnerabilities**. No se recomienda eliminar el núcleo antiguo.

Tabla 8-1 Comandos de verificación

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

8.3 ¿Por qué no existe un servidor mostrado en la información de vulnerabilidad?

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.

8.4 ¿Necesito reiniciar un servidor después de corregir sus vulnerabilidades?

- En un servidor de Windows, debe reiniciarlo después de corregir sus vulnerabilidades.
- En un servidor de Linux, debe reiniciarlo después de corregir una vulnerabilidad del kernel. El reinicio no es necesario para otras correcciones de vulnerabilidades.

9 Otros

9.1 ¿Qué son las Regiones y las AZ?

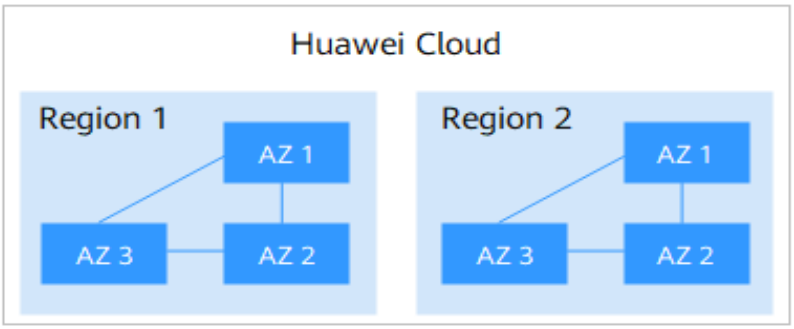
Conceptos

Una región y una zona de disponibilidad (AZ) identifican la ubicación de un centro de datos. Puede crear recursos en una región específica y AZ.

- **Regiones** se definen en términos de ubicación geográfica y latencia de red. Cada región tiene sus propios servicios públicos compartidos (ECS, EVS, OBS, VPC, EIP e IMS). Las regiones son comunes o dedicadas. Una región común proporciona servicios en la nube comunes disponibles para todos los tenants. Una región dedicada proporciona servicios de un tipo específico o solo para tenants específicos.
- Una **AZ** contiene uno o más centros de datos físicos. Cada AZ tiene instalaciones independientes de refrigeración, extinción de incendios, antihumedad y electricidad. La computación, la red, el almacenamiento y otros recursos en una AZ se dividen lógicamente en múltiples clústeres. Las AZs de una región están interconectadas a través de fibra óptica de alta velocidad, por lo que los sistemas implementados en las AZ pueden lograr una mayor disponibilidad.

Figura 9-1 muestra la relación entre las regiones y las zonas de disponibilidad.

Figura 9-1 Región y AZ



Huawei Cloud ofrece servicios en muchas regiones de todo el mundo. Puede seleccionar una región y una AZ según sea necesario.

¿Qué región debo elegir?

Al seleccionar una región, tenga en cuenta lo siguiente:

- Localización

  Se recomienda seleccionar una región más cercana a sus usuarios objetivo. Esto reduce la latencia de la red y mejora la velocidad de acceso. Sin embargo, las regiones de China continental proporcionan la misma infraestructura, calidad de red BGP y operaciones y configuraciones de recursos. Por lo tanto, si sus usuarios objetivo se encuentran en China continental, no es necesario tener en cuenta las diferencias de latencia de la red al seleccionar una región.

  - Si sus usuarios objetivo se encuentran en Asia Pacífico (excepto China continental), seleccione la región **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore**.
  - Si usted o sus usuarios objetivo están en África, seleccione la región de **AF-Johannesburg**.
  - Si usted o sus usuarios objetivo están en Europa, seleccione la región **EU-Paris**.
- Precio del recurso

  Los precios de los recursos pueden variar en diferentes regiones. Para obtener más información, consulte **Detalles de precios del producto**.

¿Qué zona de disponibilidad debo elegir?

Tenga en cuenta sus requisitos para DR y latencia de red al seleccionar un AZ:

- Para obtener una mayor capacidad de DR, despliegue recursos en diferentes zonas de disponibilidad en la misma región.
- Para reducir la latencia, despliegue recursos en la misma zona de disponibilidad.

Regiones y puntos de conexión

Antes de usar una API para llamar a recursos, especifique su región y punto de conexión. Para obtener más información, consulte **Regiones y puntos de conexión**.

9.2 ¿Qué debo hacer si la respuesta del teclado es lenta o si necesito ingresar dígitos consecutivos en el sistema operativo Windows chino?

Elija el método de entrada de inglés.

9.3 ¿Cómo uso la herramienta de conexión a escritorio remoto de Windows para conectarme a un servidor?

Procedimiento

Paso 1 En el equipo local, elija **Startup** > **Running** y, a continuación, ejecute el comando **mstsc** para iniciar la conexión a Escritorio remoto de Windows.

Paso 2 Haga clic en **Options** y, a continuación, haga clic en la pestaña **Local Resources**. En el área **Local devices and resources**, seleccione **Clipboard**.

Paso 3 Haga clic en la pestaña **General**. En **Computer**, introduzca la EIP del servidor en el que desea instalar un agente. En **User name**, escriba **Administrator**. A continuación, haga clic en **Connect**.

Paso 4 En el cuadro de diálogo que se muestra, escriba la contraseña de usuario del servidor y haga clic en **OK** para conectarse al servidor.

----Fin

9.4 ¿Cómo puedo comprobar los archivos de registro de HSS?

Ruta de log

En la siguiente tabla se describen los archivos de registro y sus rutas de acceso.

Sistema operativo	Directorio de log	Archivo de log
Linux	/var/log/hostguard/	● hostwatch.log ● hostguard.log ● upgrade.log ● hostguard-service.log ● config_tool.log ● ngine.log

Retención de log

Archivo de log	Descripción	Tamaño máximo	Archivo retenido	Período de retención
hostwatch.log	Registra logs generados durante la ejecución de procesos de daemon.	10M	Últimos cinco logs	Hasta que se desinstala el agente HSS
hostguard.log	Registra logs generados durante la ejecución de los procesos de trabajo.	10M	Últimos ocho archivos	
upgrade.log	Registra logs generados durante la actualización de la versión.	10M	Últimos cinco logs	

Archivo de log	Descripción	Tamaño máximo	Archivo retenido	Período de retención
hostguard-service.log	Registra logs (scripts) generados cuando se inicia el servicio.	100k	Últimos dos logs	
config_tool.log	Registra logs (programas) generados cuando se inicia el servicio.	10M	Últimos dos logs	
engine.log	Registra logs generados cuando sale el servicio.	10M	Últimos dos logs	

9.5 ¿Cómo puedo habilitar el registro de errores de inicio de sesión?

MySQL

La función de prevención de hackeo de cuentas para Linux soportan MySQL 5.6 y 5.7. Realice los siguientes pasos para habilitar el registro en caso de fallo de inicio de sesión:

Paso 1 Inicie sesión en el host como usuario **root**.

Paso 2 Ejecute el siguiente comando para consultar el valor **log_warnings**:

show global variables like 'log_warnings'

Paso 3 Ejecute el siguiente comando para cambiar el valor **log_warnings**:

set global log_warnings=2

Paso 4 Modifique el archivo de configuración.

- Para un sistema operativo Linux, modifique el archivo **my.conf** agregando **log_warnings=2** a **[MySQLd]**.

----Fin

vsftp

Esta sección muestra cómo habilitar el registro de errores de inicio de sesión de vsftp.

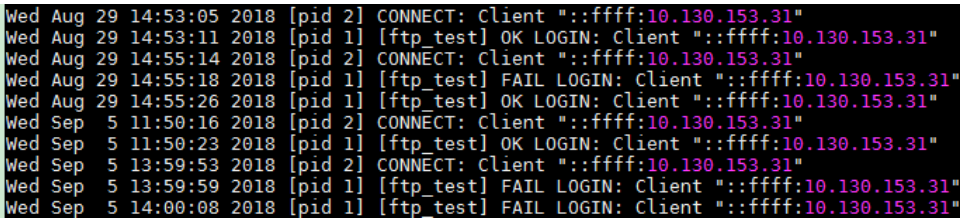
Paso 1 Modifique el archivo de configuración (por ejemplo, **/etc/vsftpd.conf**) y establezca los siguientes parámetros:

vsftpd_log_file=log/file/path

dual_log_enable=YES

Paso 2 Reinicie el servicio vsftp. Si la configuración es correcta, los registros de registro mostrados en los registros mostrados en **Figura 9-2** se devolverán cuando inicie sesión en vsftp.

Figura 9-2 Registros de logs



----Fin

10 Protección contra manipulación de la web

10.1 ¿Por qué necesito agregar un directorio protegido?

WTP protege archivos en directorios. Si no se especifica ningún directorio, WTP no puede surtir efecto incluso si está habilitado.

Para obtener más información, consulte **Habilitación de WTP**.

10.2 ¿Cómo modifico 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**.

Paso 3 En el panel de navegación, elija **Prevention** > **Web Tamper Protection**.

Paso 4 Busque el servidor de destino y haga clic en **Configure Protection** en la columna **Operation**.

Paso 5 Haga clic en **Settings**. En la página **Protected Directory Settings** de la derecha, seleccione el directorio que desea editar y haga clic en **Edit** en la columna **Operation**.

NOTA

- 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 En el cuadro de diálogo **Edit Protected Directory**, modifique la configuración y haga clic en **OK**.

----Fin

10.3 ¿Qué debo hacer si WTP no se puede habilitar?

Las causas de este problema varían según los escenarios.

Cuota insuficiente

- **Síntomas**

  La cuota de WTP en la región seleccionada es insuficiente.

- **Solución**

  Comprar cuota WTP en la región seleccionada.

El estado del agente es anormal

- **Síntomas**

  El estado del agente es **Offline** o **Not installed** en la **lista de servidores** en la página **Web Tamper Protection**.

- **Solución**

  Rectifique la falla siguiendo las instrucciones proporcionadas en **¿Cómo puedo arreglar un agente anormal?**. Asegúrese de que **Agent Status** en la lista de servidores esté **Online**.

Se ha habilitado el HSS Basic o Enterprise Edition

- **Síntomas**

  Protection Status está **Enabled** en la **lista de servidores** en la consola HSS.

- **Solución**

  Deshabilitar HSS y luego **habilitar WTP**.

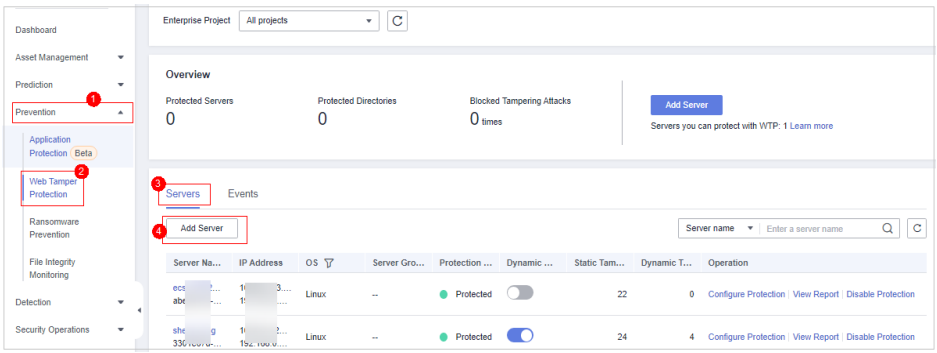
  NOTA

  Las ediciones HSS incluyen las ediciones básicas, empresariales, premium y WTP. Antes de habilitar WTP para un servidor, asegúrese de que se ha deshabilitado el HSS de edición básica, empresarial y premium para el servidor.

Se habilitó la protección en la página incorrecta

Para habilitar WTP, elija **Web Tamper Protection** > **Servers**.

Figura 10-1 Adición de servidores protegidos



NOTA

Si ha adquirido la edición WTP, puede utilizar todas las funciones de la edición Premium, y puede activar la protección del servidor solo en **Web Tamper Protection**. Después de habilitar WTP, también se habilita la protección del servidor de la edición Premium.

10.4 ¿Cómo modifico un archivo después de que WTP esté habilitado?

Los directorios protegidos son de solo lectura. Para modificar archivos o actualizar el sitio web, realizar cualquiera de las siguientes operaciones.

Desactivación temporal de WTP

Deshabilite WTP mientras modifica archivos en directorios protegidos.

Su sitio web no está protegido contra manipulaciones mientras WTP está deshabilitado. Habilítelo inmediatamente después de actualizar su sitio web.

Configuración de la protección programada

Puede establecer WTP estático periódico y actualizar sitios web mientras WTP está desactivado automáticamente.

Tenga cuidado al establecer los períodos para deshabilitar WTP, ya que los archivos no estarán protegidos en esos períodos.

10.5 ¿Qué puedo hacer si habilité el WTP dinámico pero su estado está habilitado pero no está en efecto?

WTP dinámico protege sus aplicaciones de Tomcat.

Para que esta función tenga efecto, asegúrese de que:

- Hay aplicaciones Tomcat ejecutándose en sus servidores.
- Sus servidores ejecutan el sistema operativo Linux.
- El archivo **setenv.sh** se ha generado automáticamente en el directorio **tomcat/bin** (normalmente 20 minutos después de habilitar WTP dinámico). Si el archivo existe, reinicie Tomcat para que el WTP dinámico surta efecto.

Si el estado del WTP dinámico es **Enabled but not in effect** después de habilitarlo, realice las siguientes operaciones:

- Compruebe si el archivo **setenv.sh** se ha generado en el directorio **tomcat/bin**.
- Si el archivo **setenv.sh** existe, compruebe si Tomcat se ha reiniciado.

10.6 ¿Cuáles son las diferencias entre las funciones de protección contra manipulaciones Web de HSS y WAF?

La función de protección contra manipulaciones web de HSS monitorea los directorios del sitio web en tiempo real, realiza copias de respaldo de los archivos y restaura los archivos

manipulados mediante la copia de respaldo, protegiendo los sitios web de la manipulación. Esta función es útil para los gobiernos, las instituciones educativas y las empresas.

WAF protege los datos del usuario en la capa de la aplicación. Soporta la configuración de caché en páginas web estáticas. Cuando un usuario accede a una página web, el sistema devuelve una página almacenada en caché al usuario y comprueba aleatoriamente si la página ha sido manipulada.

Diferencias entre las funciones de protección contra manipulaciones Web de HSS y WTP

La siguiente tabla describe las diferencias entre HSS y WAF.

Tabla 10-1 Diferencias entre las funciones de protección contra manipulaciones web de HSS y WAF

Elemento	HSS	WAF
Protección de página web estática	Bloquea los archivos en los directorios de controladores y archivos web para evitar que los atacantes los manipulen.	Almacena en caché las páginas web estáticas en los servidores.
Protección dinámica de páginas web	● WTP dinámico Protege sus datos mientras Tomcat está en ejecución, detectando la manipulación dinámica de datos en las bases de datos. ● Gestión de procesos privilegiados Permite a los procesos privilegiados modificar páginas web.	No
Copia de respaldo y restauración	● Copia de respaldo y restauración activas Si WTP detecta que un archivo en el directorio de protección está manipulado, inmediatamente utiliza el archivo de copia de respaldo en el host local para restaurar el archivo. ● 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.	No
Adecuado para:	Sitios web que tienen altos requisitos de seguridad y difíciles de recuperar manualmente	Sitios web que solo requieren protección en la capa de aplicación

Sugerencia de compra

Sitio web	Servicio
Sitios web comunes	Protección contra manipulaciones web de WAF + edición empresarial de HSS
Sitios web que requieren una fuerte protección y capacidades antimanipulación	Protección contra manipulaciones web de WAF + HSS WTP

11 Container Guard Service

11.1 ¿Cómo puedo habilitar la protección de nodos?

Cuando habilita la protección de nodos, el sistema instala automáticamente el complemento CGS en el nodo.

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 **Asset Management** > **Containers & Quota**.

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

Paso 5 En el cuadro de diálogo que se muestra, lea y seleccione **I have read and agree to the Container Guard Service Disclaimer**.

Paso 6 Haga clic en **OK** para habilitar la protección para el nodo. Si **Protection Status** del nodo es de **Protected**, se habilita la protección para el nodo.

NOTA

- Si habilita la protección para nodos que exceden la cuota de protección adquirida, los nodos en exceso se cobrarán según el pago por uso. Para obtener detalles sobre el modo de facturación de pago por uso de Host Security Service (HSS), consulte **¿Cuándo y cómo se cobrará CGS por uso?**
- Cuando habilita la protección de un nodo, el sistema instala automáticamente el complemento de protección CGS en el nodo.
- Una cuota HSS protege un nodo de clúster.

----Fin

11.2 How Do I Disable Node Protection?

Perform the following steps to disable protection, which will automatically uninstall the CGS plug-in from the cluster.

Paso 1 **Log in to the management console**.

Paso 2 In the upper part of the page, select a region, click , and choose **Security** > **Container Guard Service**.

Paso 3 Locate the row containing the target cluster and click **Disable Protection** in the **Operation** column.

NOTA

Click the name of a cluster to go to the node list page. You can also click **Disable Protection** on the top of the node list.

Paso 4 In the displayed dialog box, click **Yes**.

After protection is disabled, **Cluster Protection Status** of the cluster is **Disabled**, indicating that protection has been disabled for all available nodes in the cluster.

NOTA

Disabling protection will automatically uninstall the CGS plug-in from the cluster.

----Fin

11.3 How Often Is the CGS Vulnerability Library Updated?

CGS obtains official vulnerability updates in real time, adds new vulnerabilities to the vulnerability library in the early morning every day, and performs comprehensive scans and provides solutions. You can repair or adjust risky images based on service requirements.

- For details about how to check local image vulnerabilities and solutions, see **Managing Local Image Vulnerabilities**.
- For details about how to check private image vulnerabilities and solutions, see **Managing Private Image Vulnerabilities**.

11.4 ¿Qué es el mecanismo de procesamiento de registros de CGS?

CGS actualiza los registros en su archivo de registro cada 10 minutos. Si el archivo supera los 30 MB, CGS realizará una copia de respaldo de logs de 30 MB más recientes en un archivo de copia de respaldo y borrará el contenido del archivo de log.

El nombre del archivo de log de copia de respaldo es el nombre del archivo de registro más la extensión **.last**. Por ejemplo, el archivo de copia de respaldo de **shield.log** es **shield.log.last**.

11.5 ¿Cuál es la ruta de log de CGS?

Logs de CGS se almacenan en el directorio **/var/log/shield** de la máquina host.

Los archivos de log incluyen:

- **shield.log**: registra logs de ejecución de seguridad del contenedor y logs de errores.

- **message.log**: comunicación entre el agente y el servidor, como la entrega de políticas y la notificación de alarmas
- **defender_audit.log**: logs del sistema de auditoría. Este archivo almacena los mensajes de auditoría activados por las reglas de auditoría que se configuran manualmente pero que no se utilizan para HSS (si las hay).

11.6 ¿El escudo de CGS afecta a los servicios?

No. El escudo de CGS se instala como un complemento de daemonset y se ejecuta en cada nodo de un clúster en modo de contenedor. Cuando se inicia el complemento de escudo, solicita una cantidad fija de recursos (0.3 vCPU y 300 MB de memoria). Después de iniciar el complemento de escudo, monitorea los contenedores iniciados sin afectar a sus servicios.

12 Protección de ransomware

12.1 ¿Cuáles son las diferencias entre la copia de respaldo de protección contra ransomware y la copia de respaldo en la nube?

La copia de respaldo de la protección contra ransomware HSS depende de Cloud Backup and Recovery (CBR). La política de copia de respaldo del servidor solo tiene efecto después de comprar el CBR.

No hay diferencia entre los dos en términos de mecanismo de copia de respaldo y gestión. La única diferencia es que la copia de respaldo de ransomware genera una biblioteca de copia de respaldo de ransomware dedicada.

El mecanismo de copia de respaldo de la protección de ransomware hereda el de CBR (Copia de respaldo en la nube y restauración). Los archivos de copia de respaldo de la protección contra ransomware se pueden gestionar y ver de forma centralizada en CBR. Para obtener más información sobre el mecanismo CBR, consulte **¿Qué es CBR?**.

