Host Security Service

Preguntas frecuentes

Edição 01

Data 2023-10-27

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Marcas registadas e permissões

e outras marcas registadas da Huawei são marcas registadas da Huawei Technologies Co., Ltd. Todos as outras marcas registadas e os nomes registados mencionados neste documento são propriedade dos seus respectivos detentores.

Aviso

Os produtos, os serviços e as funcionalidades adquiridos são estipulados pelo contrato estabelecido entre a Huawei Cloud e o cliente. Os produtos, os serviços e as funcionalidades descritos neste documento, no todo ou em parte, podem não estar dentro do âmbito de aquisição ou do âmbito de uso. Salvo especificação em contrário no contrato, todas as declarações, informações e recomendações neste documento são fornecidas "TAL COMO ESTÃO" sem garantias ou representações de qualquer tipo, sejam expressas ou implícitas.

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

Huawei Cloud Computing Technologies Co., Ltd.

Endereço: Huawei Cloud Data Center, Rua Jiaoxinggong
Avenida Qianzhong
Novo Distrito de Gui'an
Guizhou 550029
República Popular da China

Site: https://www.huaweicloud.com/intl/pt-br/

Índice

1 Sobre o HSS

1.1 O que é o HSS?

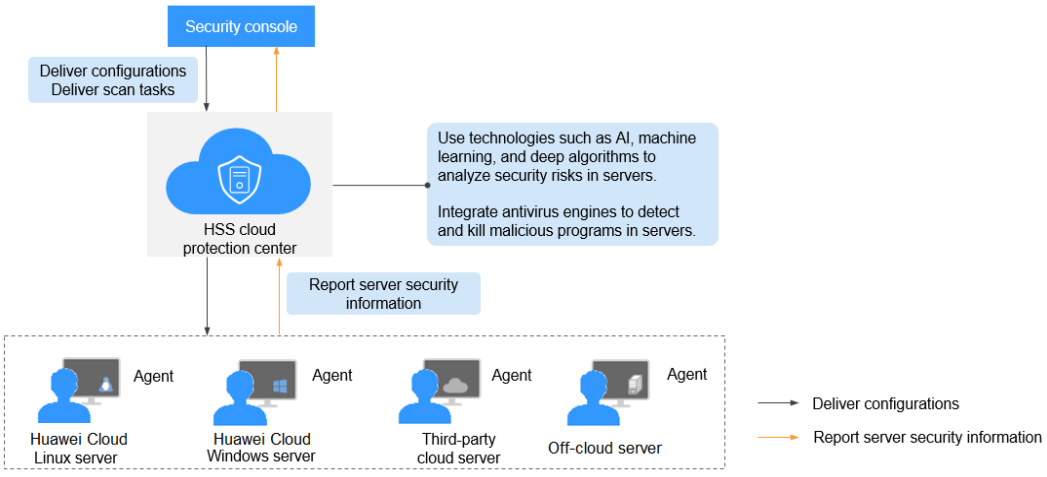
O HSS ajuda a identificar e gerenciar os ativos em seus servidores, eliminar riscos e defender-se contra invasões e adulteração de páginas da Web. Há também funções avançadas de proteção e operações de segurança disponíveis para ajudá-lo a detectar e lidar facilmente com ameaças

Como funciona o HSS

Instale o agente do HSS em seus servidores e você poderá verificar o status de segurança do servidor e os riscos em uma região no console do HSS.

Figura 1-1 mostra o princípio de funcionamento de HSS.

Figura 1-1 Princípios de funcionamento



As funções e processos de trabalho dos componentes do HSS são descritos da seguinte forma:

Tabela 1-1 Componentes

Componente	Descrição
Console de gerenciamento	Uma plataforma de gerenciamento visualizada, onde você pode aplicar configurações de maneira centralizada e visualizar o status de proteção e os resultados da verificação de servidores em uma região.
Centro de proteção em nuvem de HSS	● Analisa os riscos de segurança em servidores usando IA, aprendizado de máquina e algoritmos de aprendizado profundo. ● Integra vários mecanismos antivírus para detectar e eliminar programas maliciosos em servidores. ● Recebe configurações e tarefas de verificação enviadas do console e as encaminha para agentes nos servidores. ● Recebe informações do servidor relatadas pelos agentes, analisa os riscos de segurança e exceções nos servidores e exibe os resultados da análise no console.
Agente	● Comunica-se com o centro de proteção em nuvem de HSS via HTTPS e WSS. A porta 10180 é usada por padrão. ● Verifica todos os servidores todas as manhãs; monitora o status de segurança dos servidores; e relata as informações coletadas do servidor (incluindo configurações não compatíveis, configurações inseguras, rastreamentos de intrusão, lista de software, lista de portas e lista de processos) para o centro de proteção em nuvem. ● Bloqueia ataques ao servidor com base nas políticas de segurança que você configurou. **NOTA** ● Se nenhum agente for instalado ou se o agente instalado for anormal, o HSS não estará disponível. ● O agente pode ser instalado em Elastic Cloud Servers (ECSs) e Bare Metal Servers (BMSs) da Huawei Cloud, servidores locais e servidores de nuvem de terceiros. ● Selecione o agente e o comando de instalação adequados para o seu SO. ● O agente do HSS pode ser usado em todas as edições, incluindo segurança de container e Proteção contra adulterações na Web (WTP). Você só precisa instalar o agente uma vez no mesmo servidor.

1.2 O que é o Container Security Service?

O Container Security Service (CGS) verifica vulnerabilidades e informações de configuração em imagens, ajudando as empresas a detectar riscos de containers que não podem ser encontrados usando software de segurança convencional. O CGS também fornece funções como lista branca do processo de container, monitoramento de arquivos de container, coleta de informações de container e detecção de escape de container para reduzir os riscos.

1.3 O que é Proteção contra adulteração na Web?

A WTP (Proteção contra adulteração na Web) monitora diretórios de sites em tempo real, faz backup de arquivos e restaura arquivos adulterados usando o backup. A WTP protege seus sites contra cavalos de Troia, links ilegais e adulterações.

A WTP (Proteção contra adulteração na Web) pode detectar e impedir a adulteração de arquivos em diretórios especificados, incluindo páginas da Web, documentos e imagens e restaurá-los rapidamente usando arquivos de backup válidos.

Esta seção descreve o processo de operação e as principais funções de WTP. Consulte **Figura 1-2** e **Tabela 1-2**.

Figura 1-2 Processo de operação de WTP

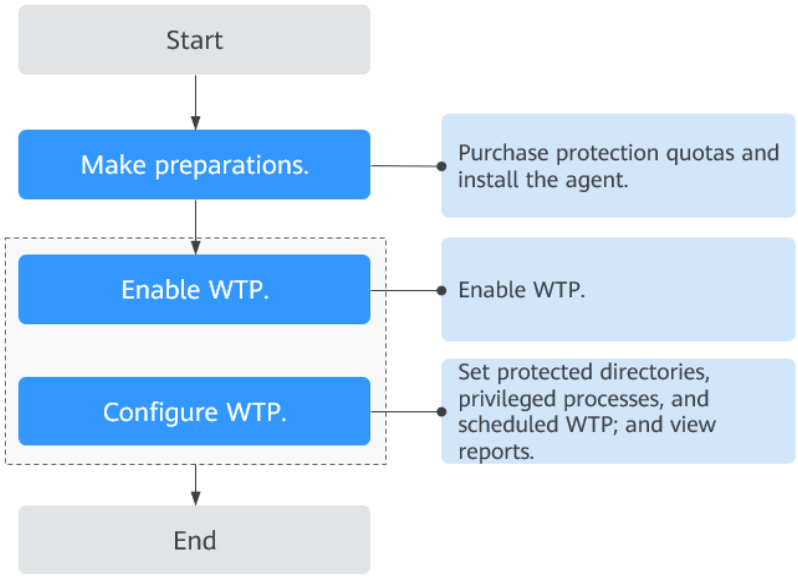


Tabela 1-2 Descrição do processo e da função da operação de WTP

Tipo	Operação	Descrição e referência
Preparações	--	Se nenhuma conta de operador de VDC estiver disponível, contacte um administrador de operações para criar uma conta de administrador de VDC e, em seguida, use a conta de administrador de VDC para criar um operador de VDC.
Primeiros passos com a WTP	Solicitação de cota	Solicite a cota de WTP.

Tipo	Operação	Descrição e referência
	Instalação de um agente	O agente é fornecido pelo HSS. Ele executa tarefas de verificação para verificar todos os servidores, monitora a segurança do servidor e relata as informações coletadas do servidor para o centro de proteção da nuvem. Você só pode ativar a WTP após a instalação do agente.
	Parâmetros necessários para configurar notificações de alarme	Depois que a notificação de alarme estiver ativada, você poderá receber notificações de alarme enviadas pelo HSS para aprender sobre os riscos de segurança enfrentados por seus servidores e páginas da Web. Sem essa função, é necessário fazer logon no console de gerenciamento para visualizar os alarmes.
	Ativar o HSS	Aloque uma cota para um servidor e ative o HSS para o servidor.
Ativar WTP	Adicionar um diretório protegido	Adicione um diretório a ser protegido por WTP.
	Criar backup remoto	Por padrão, o HSS faz backup dos arquivos dos diretórios protegidos para o diretório de backup local que você especificou quando adicionou os diretórios protegidos. Para proteger os arquivos de backup locais contra adulteração, você deve ativar a função de backup remoto.
	Adicionar um processo privilegiado	Depois que a WTP é ativada, o conteúdo nos diretórios protegidos é somente leitura. Para permitir que determinados processos modifiquem arquivos nos diretórios, adicione-os à lista de processos privilegiados.
	Definir proteção programada de WTP	Você pode programar a proteção WTP para permitir atualizações do site em períodos específicos.
	Ativar a WTP dinâmica	A WTP dinâmica protege seus dados enquanto o Tomcat está em execução, detectando adulteração dinâmica de dados em bancos de dados.
	Visualizar relatórios de WTP	Depois que a WTP estiver ativada, o HSS verificará imediatamente os diretórios protegidos especificados. É possível verificar os registros sobre adulterações detectadas.

1.4 Quais são as relações entre imagens, contêineres e aplicações?

- Uma imagem é um sistema de arquivos especial. Ela fornece programas, bibliotecas, recursos, arquivos de configuração e outros arquivos necessários para um contêiner em execução. Uma imagem também contém alguns parâmetros de configuração (como volumes anônimos, variáveis de ambiente e usuários) preparados para um contêiner em execução. Uma imagem não contém dados dinâmicos e seu conteúdo é imutável após a criação.
- A relação entre a imagem e o contêiner é semelhante àquela entre a classe e a instância no design do programa. Uma imagem é estática, e um contêiner é a entidade para uma imagem em execução. Um contêiner pode ser criado, iniciado, interrompido, excluído e suspenso.
- Vários contêineres podem ser iniciados para uma imagem.
- Uma aplicação pode incluir um ou um conjunto de contêineres.

1.5 Como usar o HSS?

Para usar o HSS, execute as seguintes etapas:

Passo 1 **Compre o HSS**.

Passo 2 **Instale o agente**.

Você pode ativar o HSS após instalar o agente.

Passo 3 **Ative as notificações de alarme**.

Depois que as notificações de alarme são ativadas, você pode receber notificações de alarme enviadas por HSS para aprender sobre os riscos de segurança enfrentados pelo servidor. Sem essa função, é necessário fazer logon no console de gerenciamento para visualizar os alarmes.

Passo 4 **Ative o HSS**.

- Depois que o agente for instalado, você poderá ativar a proteção para os servidores.
- Antes de ativar o HSS, você precisa alocar uma cota para um servidor especificado. Se o serviço for desativado ou o servidor for excluído, a cota poderá ser alocada a outros servidores.

Passo 5 **Visualize os resultados da detecção** e lide com os riscos.

----Fim

1.6 O HSS pode proteger servidores IDC locais?

Sim, desde que seus servidores se conectem à Internet.

Para obter detalhes sobre a solução, consulte **Gerenciamento e implementação de várias nuvens de HSS**.

1.7 O HSS está em conflito com qualquer outro software de segurança?

O HSS pode entrar em conflito com o DenyHosts, G01 ou 360 Guard (edição do servidor).

Conflitos entre o Agente e o DenyHosts

Para obter detalhes, consulte **O Agente está em conflito com qualquer outro software de segurança?**

Conflitos entre a função de autenticação de dois fatores e o G01 ou 360 Guard (edição do servidor)

Em um servidor do Windows em que o HSS está ativado, a função de autenticação de dois fatores pode entrar em conflito com a função de autenticação de logon do G01 ou 360 Guard (edição de servidor). Nesse caso, ative apenas uma das funções.

1.8 Quais são as diferenças entre HSS e WAF?

HSS e Web Application Firewall (WAF) são fornecidos pela Huawei Cloud para ajudá-lo a defender servidores, sites e aplicações Web contra riscos e ameaças, melhorando a segurança do sistema. Recomenda-se que os serviços sejam usados em conjunto.

Tabela 1-3 Diferenças entre HSS e WAF

Nome do serviço	Categoria	Objeto protegido	Função
HSS	Segurança da infraestrutura	Servidores	• Gerenciamento de ativos • Gerenciamento de vulnerabilidades • Detecção de intrusão • Inspeção de linha de base • Proteção contra adulteração na Web
WAF	Segurança de aplicações	Aplicações Web	• Proteção básica da Web • Proteção contra ataque CC • Proteção precisa

1.9 O HSS pode ser usado entre contas?

Não. Cada conta deve comprar e implementar o HSS separadamente. No entanto, o HSS pode ser compartilhado por vários usuários do IAM.

Compartilhamento de HSS entre vários usuários do IAM

Suponha que você tenha criado uma conta, *domain1*, registrando-se na Huawei Cloud, e usado *domain1* para criar dois usuários do IAM, *sub-user1a* e *sub-user1b*, no IAM. Se você concedeu as permissões de HSS para *sub-user1b*, *sub-user1b* pode usar o serviço HSS de *sub-user1a*.

1.10 O que é o agente de HSS?

O agente de HSS é usado para verificar todos os servidores e containers, monitorar seu status em tempo real e coletar suas informações e informar ao centro de proteção em nuvem.

Existem diferentes versões de agentes para SOs Linux e Windows. As funções de proteção de HSS estarão disponíveis depois que você **instalar o agente** e ativar **a proteção de HSS**.

Funções do agente

- O agente executa tarefas de verificação todos os dias no início da manhã para verificar todos os servidores e containers, monitora sua segurança e relata informações coletadas deles para o centro de proteção em nuvem.
- O agente bloqueia ataques direcionados a servidores e containers com base nas políticas de segurança configuradas.

NOTA

- Se nenhum agente for instalado ou se o agente instalado for anormal, o HSS não estará disponível.
- O agente pode ser instalado em Elastic Cloud Servers (ECSs) e Bare Metal Servers (BMSs) da HUAWEI CLOUD, servidores locais e servidores de nuvem de terceiros.

Processos do agente do Linux

O processo do agente precisa ser executado pelo usuário **root**.

O agente contém os seguintes processos:

Tabela 1-4 Processos do agente do Linux

Nome do processo do agente	Função	Caminho
hostguard	Detecta problemas de segurança, protege o sistema e monitora o agente.	/usr/local/hostguard/bin/hostguard
upgrade	Atualiza o agente.	/usr/local/hostguard/bin/upgrade

1.11 Posso usar o HSS se meus serviços não estiverem implementados na HUAWEI CLOUD?

Sim.

Você pode instalar o agente em ECSs, BMSs, servidores locais e servidores de nuvem de terceiros da Huawei Cloud na mesma região para gerenciá-los de maneira unificada.

Para obter detalhes sobre a solução, consulte **Gerenciamento e implementação de várias nuvens do HSS**.

1.12 Posso atualizar minha edição do HSS?

Sim.

Precauções

- As edições WTP e de container são as edições mais altas e não podem ser atualizadas.
- Uma edição pode ser atualizada diretamente para a edição empresarial ou premium. Para atualizar para a edição WTP, você precisa comprá-la separadamente e, em seguida, vinculá-la a um servidor.
- A edição básica pode ser atualizada para a edição empresarial, premium ou WTP. A edição empresarial pode ser atualizada para a edição premium ou WTP. A edição premium pode ser atualizada apenas para a edição WTP.

Atualização para a edição empresarial/premium

Para atualizar uma cota, seu **Usage Status** deve ser **Idle**.

- **Atualizar uma cota ociosa**

  Atualize a cota na guia **Quotas** da página **Servers & Quota**. Para obter mais informações, consulte **Atualização de sua edição**.

- **Atualizar uma cota em uso**

  a. Desvincule a cota do servidor que ela protege. Para obter mais informações, consulte **Desvinculação de uma cota de um servidor**.

  b. Verifique o status da cota. Espera-se que mude para **Idle**.

  c. Atualize a cota. Para obter mais informações, consulte **Atualização para a edição empresarial/premium**.

Atualização para a edição WTP

A edição WTP não pode ser atualizada diretamente de uma edição inferior e precisa ser comprada separadamente. Antes de proteger um servidor com WTP, verifique se o servidor não está vinculado a nenhuma cota.

1. Compre a WTP no console do HSS. Para obter mais informações, consulte **Compra de uma cota de HSS**.
2. Desvincule um servidor de sua cota existente. Para obter mais informações, consulte **Desvinculação de uma cota de um servidor**.
3. Vincule o servidor à WTP. Para obter mais informações, consulte **Atualização para a edição WTP**.

2 Perguntas frequentes do agente

2.1 É necessário instalar o agente do HSS após a compra do HSS?

Sim. O agente do HSS não é instalado automaticamente após a compra. Você pode copiar um comando fornecido para instalar rapidamente o agente.

Cenários de instalação do agente

O agente pode ser instalado:

- Automaticamente durante a compra do servidor
- Manualmente após a compra do servidor

Instalação automática durante a compra do servidor

Ao comprar um ECS da Huawei Cloud, se você ativar o HSS, o HSS instalará seu agente no ECS e protegerá o ECS.

- Se você selecionar **Yearly/Monthly** para **Billing Mode**, poderá selecionar a edição básica, empresarial ou WTP (Proteção contra adulteração na Web).
- Se você selecionar **Pay-per-use** para **Billing Mode**, poderá selecionar a edição empresarial.

Se a edição do HSS comprada não atender aos seus requisitos, você pode **comprar outra edição**. Não é necessário reinstalar o agente. Para obter mais informações, consulte **Edições**.

Instalação manual após a compra do servidor

Se você comprar o HSS separadamente, o HSS não instalará automaticamente o agente em seus servidores. Nesse caso, use o comando de instalação adequado para o SO do seu servidor no console do HSS, faça logon no servidor e instale manualmente o agente. Para obter detalhes, consulte **Instalação do agente**.

2.2 O agente está em conflito com algum outro software de segurança?

Sim, ele pode estar em conflito com DenyHosts.

- Sintoma: o endereço IP do host de logon é identificado como um endereço IP de ataque, mas não pode ser desbloqueado.
- Causa: HSS e DenyHosts bloqueiam possíveis endereços IP de ataque, mas o HSS não consegue desbloquear endereços IP bloqueados pelo DenyHosts.
- Método de tratamento: pare DenyHosts.
- Procedimento

  a. Efetue logon como usuário **root** no ECS.

  b. Execute o seguinte comando para verificar se DenyHosts foi instalado:

  ps -ef | grep denyhosts.py

  Se forem exibidas informações semelhantes às seguintes, o DenyHosts foi instalado:

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

  c. Execute o seguinte comando para parar o DenyHosts:

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

  d. Execute o seguinte comando para cancelar a inicialização automática do DenyHosts na inicialização do host:

  chkconfig --del denyhosts;

2.3 Como instalar o agente?

- Para obter detalhes sobre como instalar o agente do Linux, consulte **Instalação de um agente no Linux**.
- Para obter detalhes sobre como instalar o agente do Windows, consulte **Instalação de um agente no Windows**.

2.4 Como desinstalar o agente?

Dois métodos de desinstalação estão disponíveis: desinstalação com um clique e desinstalação local manual.

Cenário

- O agente foi instalado usando um pacote incorreto e você precisa desinstalá-lo.
- O agente foi instalado usando comandos incorretos e você precisa desinstalá-lo.
- Se o agente não for atualizado, desinstale o agente.

Pré-requisitos

Quando você desinstala o agente no console de gerenciamento, o **Agent Status** do servidor é **Online**.

Desinstalar o agente no console com um clique

Você pode desinstalar um agente do HSS do console do HSS.

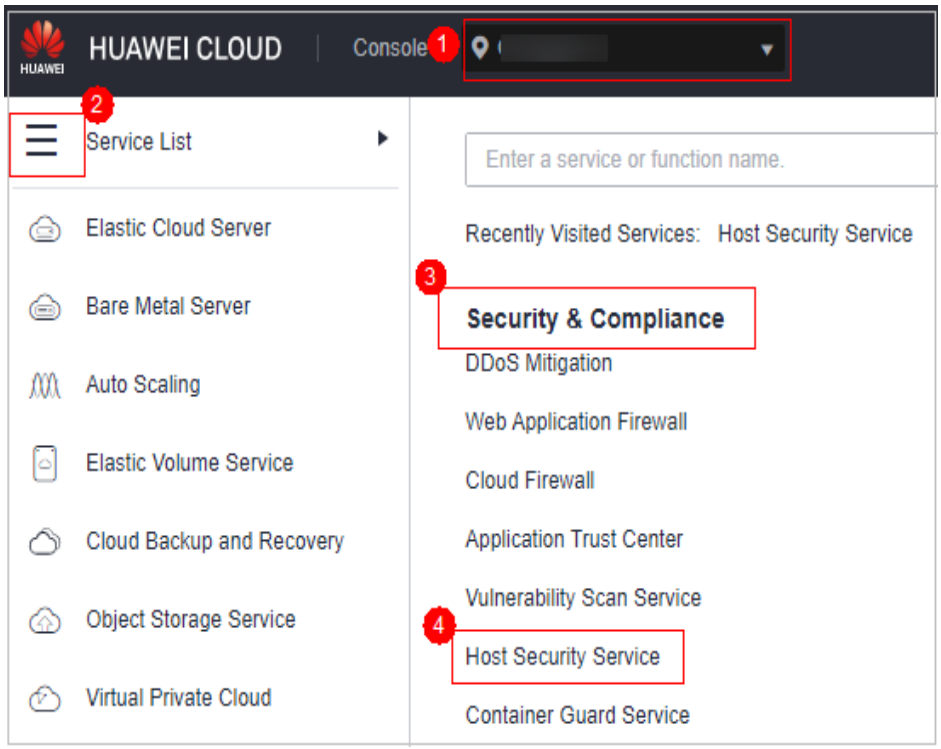
NOTA

Depois que o agente for desinstalado de um servidor, o HSS não fornecerá nenhuma proteção para o servidor.

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 2-1 Acessar o HSS



Passo 3 No painel de navegação, escolha **Installation and Configuration**.

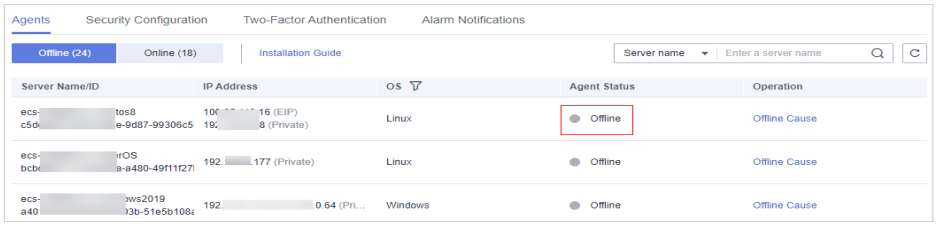
Passo 4 Na página exibida, clique na guia **Agents** e clique em **Online**. Na linha que contém o servidor desejado, clique em **Uninstall Agent** na coluna **Operation**.

Se for necessário desinstalar o agente em lotes, selecione servidores e clique em **Uninstall Agent** acima da lista.

Passo 5 Na caixa de diálogo exibida, clique em **OK**.

Na lista de servidores, se **Agent Status** do servidor for **Offline**, seu agente será desinstalado com sucesso.

Figura 2-2 Agente desinstalado



----Fim

Desinstalar o agente do servidor

Você pode desinstalar manualmente um agente de HSS em um servidor quando não estiver mais usando o HSS ou precisar reinstalar o agente.

NOTA

Depois que o agente for desinstalado de um servidor, o HSS não fornecerá nenhuma proteção para o servidor.

- **Desinstalar o agente do Linux**
  a. Efetue logon no servidor do qual deseja desinstalar o agente. Em seguida, execute o comando **su - root** para mudar para o usuário **root**.
  b. Em qualquer diretório, execute o seguinte comando para desinstalar o agente:
     i. Se o agente foi instalado usando um pacote .rpm, execute o comando **rpm -e --nodeps hostguard**.
     ii. Se o agente foi instalado usando o pacote .deb, execute o comando **dpkg -P hostguard**.

     Se as seguintes informações forem exibidas, o agente será desinstalado:

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

- **Desinstalar o agente do Windows**
  a. Efetue logon no servidor do qual deseja desinstalar um agente do HSS.
  b. Clique em **Start** e selecione **Control Panel** > **Programs**. Em seguida, selecione **HostGuard** e clique em **Uninstall**.

     NOTA

     - Como alternativa, vá para o diretório de instalação e clique duas vezes em **unins000.exe**.
     - Se você criou uma pasta para armazenar o atalho do agente no menu **Start** ao instalar o agente, também pode escolher **Start** > **HostGuard** > **Uninstall HostGuard** para desinstalar o HostGuard.

  c. Na caixa de diálogo **Uninstall HostGuard**, clique em **Yes**.
  d. Após a conclusão da desinstalação, clique em **OK**.

2.5 O que devo fazer se a instalação do agente falhar?

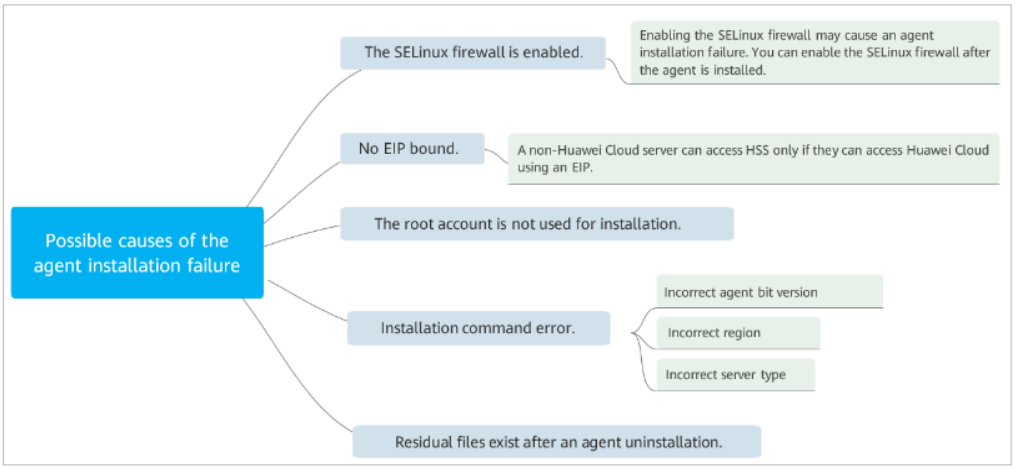
Se você usou o HSS de uma versão anterior e instalou o agente na nova versão do HSS, mas a página ainda exibe que o agente não está instalado, consulte **O que posso fazer se o status do agente ainda estiver "Not installed" após a instalação?**

Se esta for a primeira vez que você instala o agente e a instalação falhar, corrija a falha seguindo as instruções fornecidas nesta seção.

Sintomas

O agente falha ao ser instalado pela execução de comandos. A página de lista de servidores no console ainda indica que o agente não está instalado.

Possíveis causas



Solução

Passo 1 Verifique se o firewall do SELinux do servidor está desativado.

- Se sim, vá para o próximo passo.
- Se não, desative-o e instale o agente novamente.

Passo 2 Verifique se há um EIP vinculado ao servidor.

- Se sim, vá para a **Etapa 3**.
- Se não, vincule um EIP ao servidor e reinstale o agente.

Passo 3 Verifique se o comando de instalação é adequado para a região do servidor e o SO.

1. Alterne para a região do servidor.
2. Copie os comandos de instalação adequados para o SO do servidor.
   - Execute comandos de instalação de 32-bit em um servidor de 32-bit.
   - Execute comandos de instalação de 64-bit em um servidor de 64-bit.

- Se sim, vá para **Passo 4**.
- Se os comandos usados estiverem incorretos, instale o agente novamente com os corretos.

Passo 4 Verifique se a instalação foi realizada pelo usuário **root**.

- Se sim, vá para **Passo 5**.
- Se não, instale o agente novamente como usuário **root**.

Passo 5 **Desinstale o agente** como usuário **root** e instale-o forçosamente.

- Se a instalação for bem-sucedida, nenhuma ação adicional será necessária.
- Se a instalação falhar, entre em contato com o suporte técnico.

----Fim

2.6 Como corrigir um agente anormal?

Seu agente provavelmente está anormal se estiver no estado **Not installed** ou **Offline**. Os status dos agentes e seus significados são os seguintes:

- **Uninstalled**: nenhum agente foi instalado no servidor ou o agente foi instalado, mas não iniciado.
- **Offline**: a comunicação entre o agente e o servidor é anormal. O agente no servidor foi excluído ou um servidor não da HUAWEI CLOUD está off-line.
- **Online**: o agente no servidor está funcionando corretamente.

Possíveis causas

- O status do agente no console não é atualizado.

  O status do agente não foi atualizado. Depois que o agente é instalado, leva de 5 a 10 minutos para que o console atualize seu status.
- Versão do SO não suportada.

  Para obter detalhes, consulte **SOs suportados**.
- A rede está com defeito.

  O agente ou a central de proteção de nuvem é anormal. Por exemplo, a NIC é defeituosa, o endereço IP é alterado ou a largura de banda é baixa.
- O processo do agente é anormal.

Solução

Passo 1 Verifique se o status do agente permanece **Offline** no console por mais de 10 minutos após a instalação do agente.

- Se sim, vá para **2**.
- Se não, aguarde até que o agente fique on-line. Nenhuma ação adicional é necessária. Depois que o agente é instalado, leva de 5 a 10 minutos para o console atualizar seu status.

Passo 2 Verifique se o SO do servidor está dentro do escopo de suporte em **SOs suportados**.

- Se sim, vá para **3**.
- Se não, o agente do HSS não pode ser instalado ou executado no servidor. Atualize o SO para uma versão suportada pelo HSS e tente novamente.

Passo 3 Verifique se a rede do servidor está normal.

- Se sim, vá para 4.
- Se não, verifique se o grupo de segurança do servidor permite o acesso à porta 10180 do bloco CIDR 100.125.0.0/16 na direção de saída e se o servidor pode acessar a rede. Depois que o servidor puder acessar a rede, verifique o status do agente.

Passo 4 Reinicie o processo do agente.

- Windows
  a. Efetue logon no servidor como usuário **administrator**.
  b. Abra o Gerenciador de tarefas.
  c. Na página de guia **Services**, selecione **HostGuard**.
  d. Clique com o botão direito do mouse no serviço e escolha **Restart**.
- Linux

  Execute o seguinte comando na CLI como usuário **root** para reiniciar o agente:

  service hostguard restart

  Se as informações a seguir forem exibidas, a reinicialização foi bem-sucedida:

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

Depois que o processo for reiniciado, aguarde cerca de 2 minutos.

- Se o status do agente for **Online**, nenhuma ação adicional será necessária.
- Se o status do agente ainda for **Not installed** ou **Offline**, desinstale o agente e instale-o novamente.

----Fim

2.7 Qual é o caminho de instalação do agente padrão?

Os caminhos de instalação do agente em servidores que executam o sistema operacional Linux ou Windows não podem ser personalizados. Tabela 2-1 descreve os caminhos padrão.

Tabela 2-1 Caminhos de instalação do agente padrão

SO	Caminho de instalação padrão
Linux	/usr/local/hostguard/
Windows	C:\Program Files\HostGuard

2.8 Quantos recursos de CPU e memória são ocupados pelo agente quando ele executa verificações?

O HSS usa agentes leves, que ocupam apenas alguns recursos e não afetam seus serviços.

O uso de CPU e memória é o seguinte.

Utilização máxima de CPU

Um agente em execução ocupa no máximo 20% de uma vCPU. O uso real depende das especificações do seu servidor. Para mais detalhes, consulte **Uso de recursos de especificações diferentes enquanto o agente está em execução**.

Se o uso de CPU atingir 20% de uma vCPU, o agente reduzirá automaticamente o uso de CPU, gastando mais tempo em verificações. Isso não afeta seus serviços.

NOTA

O agente está programado para verificar seus servidores das 00:00 às 04:00 todos os dias, evitando os horários de pico de seu serviço.

Uso máximo de memória

Um agente em execução ocupa cerca de 500 MB de memória.

Se o uso da memória atingir 500 MB, o agente será reiniciado automaticamente em 5 minutos.

Uso de recursos de especificações diferentes enquanto o agente está em execução

A tabela a seguir descreve o uso de CPU e memória de diferentes especificações quando o agente está em execução.

Tabela 2-2 Uso de recursos do agente

vCPUs	Uso máximo de CPU do agente	Uso máximo de memória
1 vCPU	20%	500MB
2 vCPUs	10%	500MB
4 vCPUs	5%	500MB
8 vCPUs	2,5%	500MB
12 vCPUs	Cerca de 1,67%	500MB
16 vCPUs	Cerca de 1,25%	500MB
24 vCPUs	Cerca de 0,84%	500MB
32 vCPUs	Cerca de 0,63%	500MB
48 vCPUs	Cerca de 0,42%	500MB
60 vCPUs	Cerca de 0,34%	500MB
64 vCPUs	Cerca de 0,32%	500MB

2.9 WTP e HSS usam o mesmo agente?

Sim.

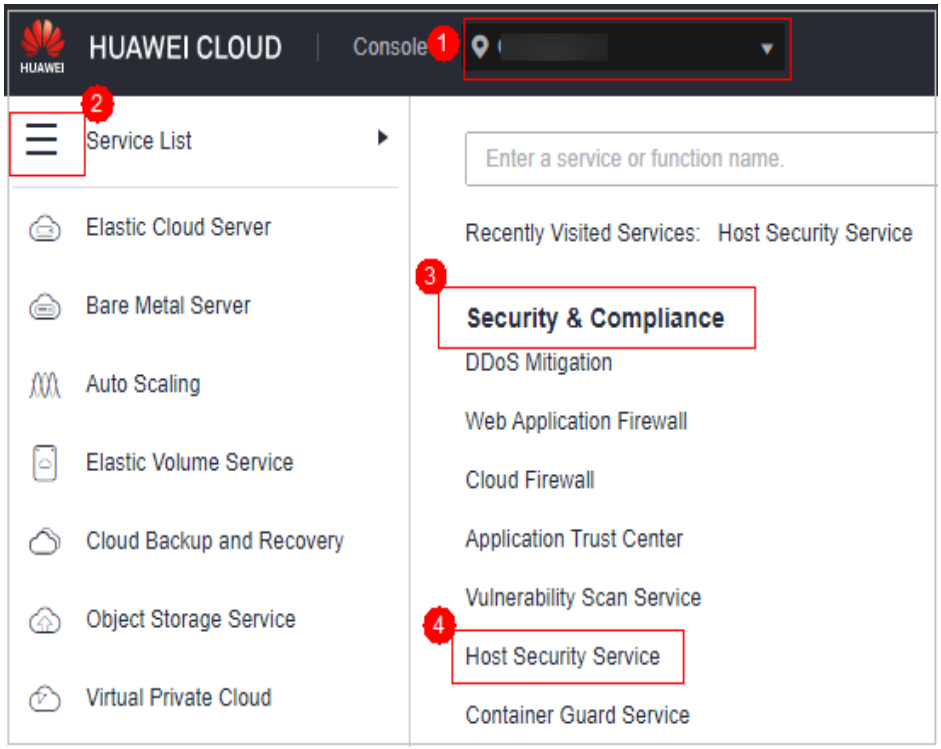
Todas as edições do HSS podem usar o mesmo agente instalado em um servidor.

2.10 Como visualizar os servidores em que nenhum agente foi instalado?

Passo 1 **Faça logon no console de gerenciamento**.

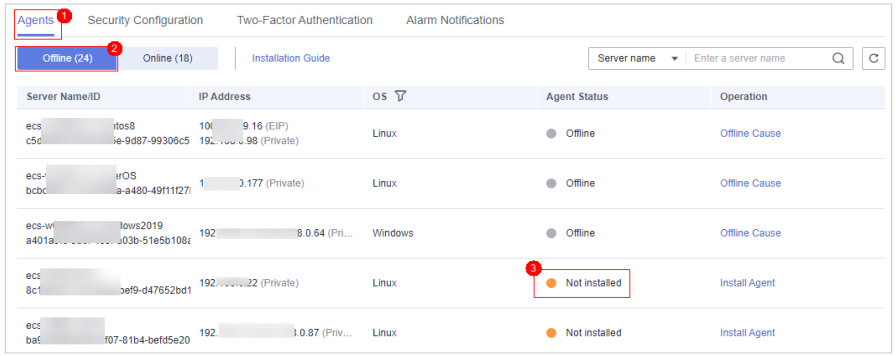
Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 2-3 Acessar o HSS



Passo 3 Na página **Installation & Configuration**, clique na guia **Agents** e clique em **Offline**. Visualize os servidores em que o agente não está instalado.

Figura 2-4 Servidores em que o agente não está instalado



Os possíveis status do agente são:

- **Not installed**: o agente não foi instalado ou iniciado com sucesso.
- **Online**: o agente está sendo executado corretamente.
- **Offline**: a comunicação entre o agente e o servidor do HSS é anormal e o HSS não pode proteger seus servidores.

  Clique em **Offline Cause** para exibir as possíveis causas.

----Fim

2.11 O que posso fazer se o status do agente ainda estiver "Not installed" após a instalação?

Precauções

Em um servidor, você só precisa instalar o agente uma vez.

Após a instalação, recomenda-se reiniciar os servidores antes de ativar o HSS e as cotas de vinculação.

Possível causa

Agora, os consoles do HSS (novo) e HSS (anterior) estão em uso. Os status de agente e proteção de um servidor podem ser exibidos corretamente em apenas um dos consoles.

Por exemplo, se você tiver instalado o agente no servidor A no console anterior e tentar instalá-lo novamente no novo console, uma mensagem será exibida indicando que a instalação foi bem-sucedida, mas o status da instalação no novo console ainda será **Not installed**.

Solução

Use apenas um console. Não alterne entre o console anterior e o novo.

Você pode **atualizar o agente** para usar HSS (novo). A atualização é gratuita e não afeta os serviços.

NOTA

O HSS (novo) fornece proteção contra ransomware mais forte e recursos adicionais de proteção de aplicações, que não estão disponíveis na versão anterior. Você é aconselhado a usar a nova versão.

2.12 Como atualizar o agente?

Você pode atualizar o agente do HSS de 1.0 para 2.0 no console de HSS (anterior). Após a atualização, você pode visualizar e gerenciar o status de proteção no console de HSS (novo). O HSS (anterior) interromperá a detecção e a proteção.

Verificar o status da atualização do agente

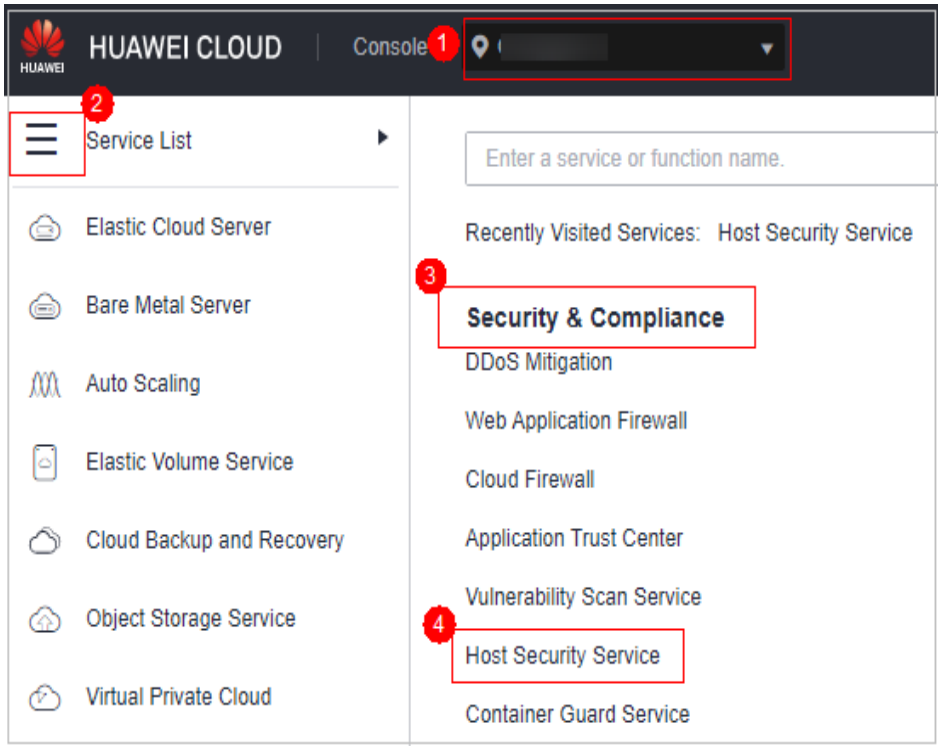
Vá para o console do HSS (anterior) e verifique o status do agente.

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service** para acessar o console do HSS (anterior).

Passo 3 No aviso de atualização exibido, clique em link de **service list** para ir para a guia **Servers** do console do HSS (anterior).

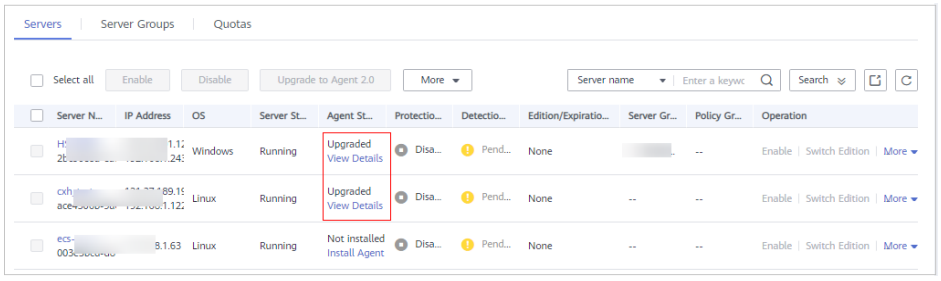
Figura 2-5 Ir para o console do HSS (anterior)



Passo 4 Verifique os status dos agentes de todos os servidores. Se o **Agent Status** for **Upgraded**, o agente foi atualizado.

Se o status for **Online**, você poderá **atualizar** o agente.

Figura 2-6 Verificar o status do agente



Passo 5 Clique em **View Details** para ir para o console do HSS (novo) e verificar o status do servidor.

----Fim

Pré-requisitos de atualização

- O **Agent Status** de um servidor é **Online**.

- Você está no console do HSS (anterior).

Precauções

- A atualização do agente é gratuita.
- A atualização não afeta as cargas de trabalho em seus servidores de nuvem.
- Após a atualização, a cobrança é interrompida no console anterior e iniciada no novo console.
- Após a atualização, seus servidores estarão protegidos por HSS (novo).

  NOTA

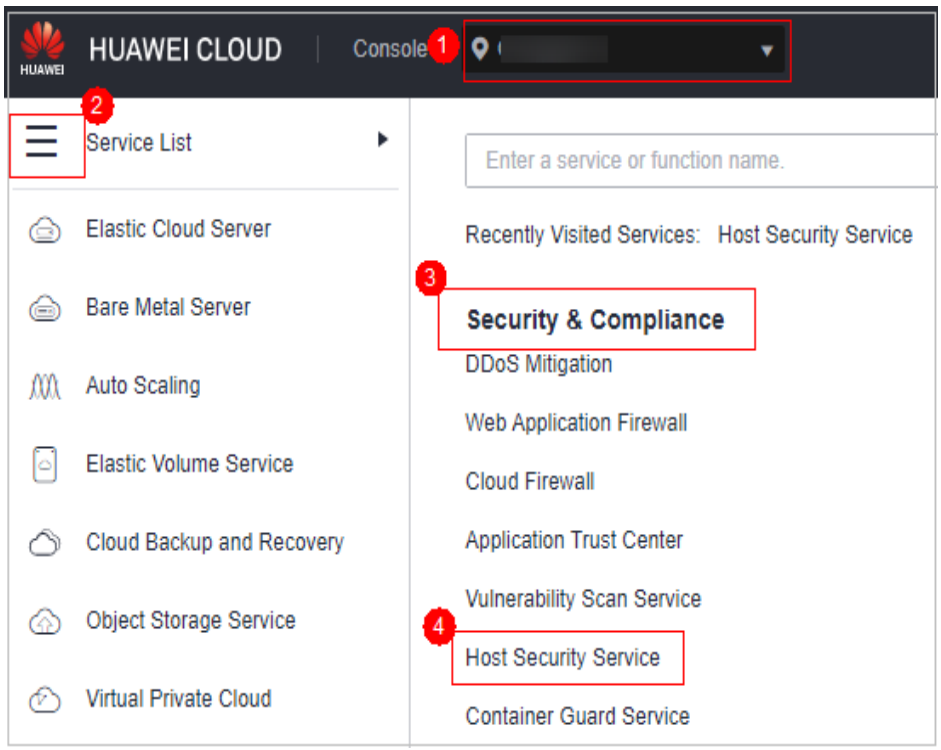
  - Atualmente, o HSS está disponível nas seguintes regiões: CN South-Guangzhou, CN-Hong Kong, AP-Bangkok e AP-Singapore.
  - No console do HSS (novo), você pode clicar em **Back to Old Console** no canto superior esquerdo para alternar para o console do HSS (anterior).
- Após a atualização, você pode ativar a prevenção aprimorada contra ransomware.
- Após a atualização, o novo agente será mais seguro, estável e confiável.

Atualizar para o agente 2.0 no console

Passo 1 **Faça logon no console de gerenciamento**.

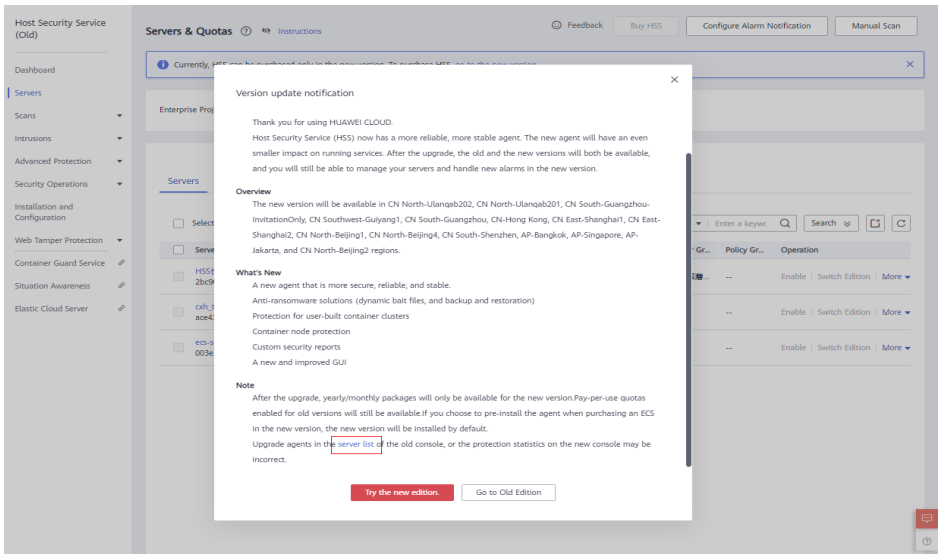
Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 2-7 Ir para o console do HSS (anterior)



Passo 3 No aviso de atualização exibido, clique em link de **service list** para ir para a guia **Servers** do console do HSS (anterior).

Figura 2-8 Ir para a lista de servidores para atualizar o agente



Passo 4 Selecione os servidores e clique em **Upgrade to Agent 2.0**.

NOTA

- Selecione um ou mais servidores cujo **Agent Status** esteja **Online**.
- Se a edição de WTP tiver sido ativada para um servidor, vá para a página **Web Tamper Protection** e desative a edição WTP. Caso contrário, o servidor não pode ser selecionado para atualização do agente.

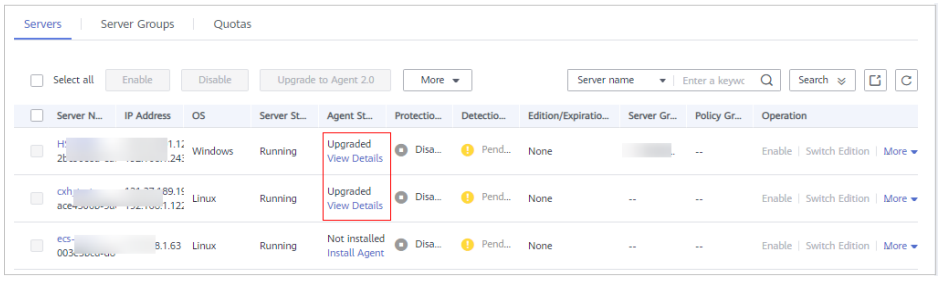
Passo 5 Na caixa de diálogo, confirme as informações do servidor e clique em **OK**. A plataforma realiza a atualização automaticamente.

Passo 6 Verifique o status da atualização na lista de servidores na **etapa 3**. Se o status do agente for **Upgraded**, a atualização foi bem-sucedida.

NOTA

- Se a atualização do agente falhar ou o status do agente for **Not installed** após a instalação bem-sucedida, solucione o problema consultando **Perguntas frequentes**.

Figura 2-9 Verificar o status do agente



----Fim

Atualizar manualmente para o agente 2.0 em um servidor do Windows

Se o agente não for atualizado para 2.0 para o servidor do Windows no console, você poderá atualizá-lo manualmente.

Passo 1 Efetue logon remotamente no servidor do Windows onde o agente 2.0 deve ser atualizado.

- Servidor da Huawei Cloud
  - Efetue logon no console do ECS, localize o servidor de destino e clique em **Remote Login** na coluna **Operation** para efetuar logon no servidor. Para obter detalhes, consulte **Fazer logon usando VNC**.
  - Se um EIP tiver sido vinculado ao servidor, você poderá usar a Conexão de área de trabalho remota do Windows ou uma ferramenta de gerenciamento remoto de terceiros, como mstsc ou RDP, para fazer logon no servidor e instalar o agente no servidor como um administrador.
- Servidor não da Huawei Cloud

  Use uma ferramenta de gerenciamento remoto (como mstsc ou RDP) para se conectar ao EIP do servidor e fazer logon remotamente no servidor.

Passo 2 Vá para **C:\Program Files (x86)\HostGuard** no servidor do Windows.

Passo 3 Exclua o arquivo **PkgConfMgr.exe**.

⚠ CUIDADO

Se você autorizar o agente 1.0 a ativar o firewall ao ativar o HSS (anterior), o agente 1.0 adicionará regras que permitem todo o tráfego de entrada e saída (**hostguard_AllowAnyIn** e **hostguard_AllowAnyOut**), o que protege suas cargas de trabalho de serem afetadas pelo firewall. Se o agente 1.0 for desinstalado, as regras serão excluídas e o acesso à rede de suas cargas de trabalho será bloqueado, a menos que você crie uma regra de bypass para as cargas de trabalho. Para resolver esse problema, exclua o arquivo **PkgConfMgr.exe**, para que as regras não sejam excluídas com a desinstalação do agente.

Passo 4 Clique duas vezes no arquivo **unins000.exe** para desinstalar o agente 1.0.

Passo 5 Na caixa de diálogo **HostGuard Uninstall**, clique em **Yes** para excluir o HostGuard e todos os seus componentes.

Passo 6 (Opcional) Reinicie o servidor.

- Se você ativou a WTP, será necessário reiniciar o servidor após a desinstalação do agente 1.0. Na caixa de diálogo **HostGuard Uninstall**, clique em **Yes** para reiniciar o servidor.
- Se você não tiver ativado a WTP, não será necessário reiniciar o servidor. Na caixa de diálogo **HostGuard Uninstall**, clique em **No** para ignorar a reinicialização do servidor.

Passo 7 Verifique a desinstalação. Se o diretório **C:\Program Files (x86)\HostGuard** não for encontrado no servidor do Windows, o agente 1.0 foi desinstalado.

Passo 8 **Faça logon no console de gerenciamento**.

Passo 9 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Passo 10 No painel de navegação, escolha **Installation & Configuration** e clique na guia **Agents**.

Passo 11 Clique em **Installation Guide**.

Passo 12 No painel deslizante exibido, copie o link de download do agente adequado para a arquitetura do sistema e o SO.

Passo 13 No servidor do Windows onde o agente 2.0 será instalado, use o Internet Explorer para baixar o pacote de instalação do agente a partir do endereço de download do agente copiado e descompactá-lo.

Passo 14 Execute o programa de instalação do agente 2.0 como administrador.

Selecione um tipo de servidor na página **Select host type**.

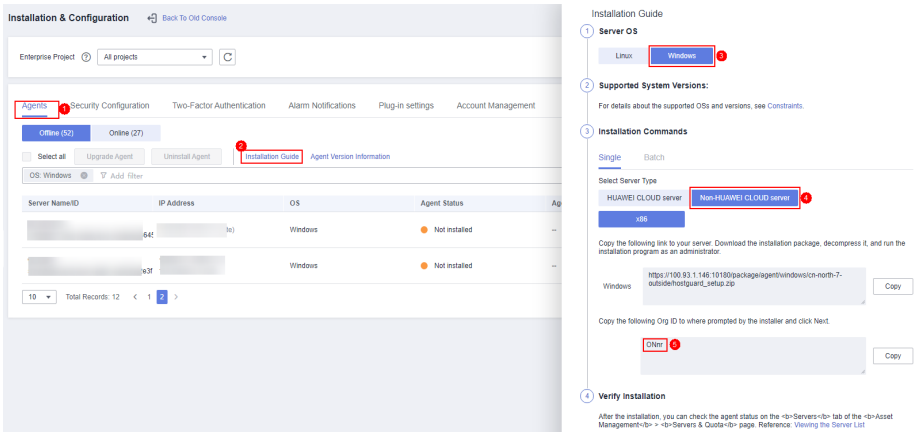
- Servidor da Huawei Cloud: selecione **Huawei Cloud Host**.
- Servidor não da Huawei Cloud: selecione **Other Cloud Host**.

  Copie o ID da organização de guia de instalação do agente, conforme mostrado em **Figura 2-10**. Digite o ID da organização na caixa de prompt do programa de instalação e, em seguida, instale o agente conforme solicitado.

AVISO

Certifique-se de que o ID da organização esteja correto. Caso contrário, o status do agente poderá ser exibido como **Not installed**, mesmo que a instalação tenha sido bem-sucedida.

Figura 2-10 Obtenção do ID da organização (para um servidor não da Huawei Cloud)



Passo 15 Verifique os processos **HostGuard.exe** e **HostWatch.exe** no Gerenciador de tarefas do Windows.

Se ambos os processos existirem, o agente foi instalado.

Passo 16 Leva de 3 a 5 minutos para que o console atualize o status do agente após a instalação do agente.

----Fim

Atualizar manualmente para o agente 2.0 em um servidor do Linux

Se o agente não for atualizado para 2.0 para o servidor do Linux no console, você poderá atualizá-lo manualmente.

Passo 1 Efetue logon remotamente no servidor do Linux onde o agente 2.0 deve ser atualizado.

- **Servidor da Huawei Cloud**

  - Efetue logon no console do ECS, localize o servidor de destino e clique em **Remote Login** na coluna **Operation** para efetuar logon no servidor. Para obter detalhes, consulte **Fazer logon usando VNC**.
  - Se o servidor tiver um EIP vinculado, você também poderá usar uma ferramenta de gerenciamento remoto, como PuTTY ou Xshell, para efetuar logon no servidor e instalar o agente no servidor como usuário **root**.

- **Servidor não da Huawei Cloud**

  Use uma ferramenta de gerenciamento remoto (como PuTTY ou Xshell) para se conectar ao EIP de seu servidor e fazer logon remotamente em seu servidor.

Passo 2 Se o agente 1.0 tiver sido instalado, execute um dos seguintes comandos para desinstalá-lo.

NOTA

Não execute o comando de desinstalação no diretório **/usr/local/hostguard/**. Você pode executar o comando de desinstalação em qualquer outro diretório.

- Para EulerOS, CentOS, SUSE, Red Hat ou outros SOs que suportam a instalação de RPM, execute o comando **rpm -e hostguard;**.
- Para Ubuntu, Debian e outros SOs que suportam instalação de DEB, execute o comando **dpkg -P hostguard;**.

Passo 3 Verifique a desinstalação. Se o diretório **/usr/local/hostguard/** não for encontrado no servidor do Linux, o agente 1.0 foi desinstalado.

Passo 4 **Faça logon no console de gerenciamento**.

Passo 5 No canto superior esquerdo da página, selecione uma região, clique em  e escolha **Security & Compliance** > **Host Security Service**.

Passo 6 No painel de navegação, escolha **Installation & Configuration** > **Agents**.

Passo 7 Clique em **Installation Guide**.

Passo 8 No painel deslizante exibido, copie o link de instalação do agente adequado para a arquitetura do sistema e o SO.

Passo 9 No servidor do Linux, execute o comando de instalação obtido na etapa anterior como usuário **root** para instalar o agente 2.0.

Se informações semelhantes às seguintes forem exibidas, o agente 2.0 foi instalado.

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

Passo 10 Execute o comando **service hostguard status** para verificar o status de execução do agente.

Se as seguintes informações forem exibidas, o agente está sendo executado corretamente:

```
Hostguard is running
```

Passo 11 Leva de 3 a 5 minutos para que o console atualize o status do agente após a instalação do agente.

----Fim

2.13 O que devo fazer se a atualização do HSS falhar?

Sobre a atualização

- Os servidores são exibidos tanto no console anterior quanto no novo do HSS, independentemente de seus agentes terem sido atualizados. Os status do servidor são exibidos corretamente no console que você está usando.
- A atualização do agente é gratuita.
- Antes de atualização, certifique-se de que **Agent Status** esteja **Online**.
- A atualização não afeta as cargas de trabalho em seus servidores de nuvem.
- Após a atualização, a cobrança é interrompida no console anterior e iniciada no novo console.
- Após a atualização, seus servidores estarão protegidos por HSS (novo).

Como o agente é atualizado

Depois de iniciar a atualização do agente no console do HSS, o sistema desinstala automaticamente o agente 1.0 e, em seguida, instala o agente 2.0.

- No console anterior, os status do agente durante a atualização são os seguintes:
  - **Upgraded**: o agente foi atualizado. Você pode ir para o console do HSS (novo) para verificar o status da proteção.
  - **Upgrading**: o agente está sendo atualizado.
  - **Upgrade failed**: o agente falhou ao ser atualizado.
- No novo console, os status do agente durante a atualização são os seguintes:
  - **Uninstalled**: o servidor de destino não instalou um agente no novo console.
  - **Online**: o agente está sendo executado corretamente.
  - **Offline**: a comunicação do agente está anormal.

Possíveis causas

NOTA

Após a conclusão da atualização automática, leva de 5 a 10 minutos para que o status do agente seja atualizado.

As possíveis causas de status anormais do agente são as seguintes:

1. Falha na resolução de DNS. O agente pode ser atualizado somente por meio de resolução de DNS da intranet. Verifique se o endereço do servidor DNS privado está correto.
2. O acesso à porta 10180 é restrito. A atualização do agente requer acesso à porta 10180.
3. A memória disponível da VM é insuficiente. A atualização do agente ocupa determinada memória. Se a memória disponível for inferior a 300 MB, a atualização será afectada.
4. Falha ao obter os metadados. Para atualizar o agente, é necessário obter o ID, o nome e a região do servidor.

Localizar e corrigir o problema

- **Falha na resolução de DNS**
  - Procedimento de solução de problemas
    i. Use uma ferramenta de gerenciamento remoto, como SecureFX ou WinSCP, para fazer logon no servidor.
    ii. Execute o seguinte comando para verificar o endereço de DNS privado do servidor:

    cat /etc/resolv.conf

    iii. Anote o endereço de DNS e a região do servidor e verifique se eles estão corretos. Para obter detalhes, consulte **Endereço do servidor DNS privado**.
    iv. Se a sua região e o endereço do servidor DNS corresponderem, o problema não foi causado pela resolução do DNS. Neste caso, verifique se há outras causas.

    Se a sua região e o endereço do servidor DNS não corresponderem, o problema foi causado por uma falha de resolução de DNS.
  - Solução

    Verifique se seus serviços serão afetados se o endereço do servidor DNS privado configurado no servidor for alterado.
    - Se os seus serviços não forem afetados pela alteração de endereço, corrija o endereço do servidor DNS privado e tente fazer a atualização novamente. Para obter detalhes, consulte **Alteração do endereço do servidor DNS privado**.
    - Se os seus serviços forem afetados pela alteração de endereço, crie o mapeamento entre o nome do servidor e o endereço IP atual e tente fazer a atualização novamente. Execute as seguintes etapas:
      1) Faça logon no seu servidor de nuvem.
      2) Execute o seguinte comando para alternar para o usuário **root**:

      sudo su -
      3) Execute o seguinte comando para editar o arquivo de configuração de **hosts**:

      vi /etc/hosts
      4) Pressione **i** para entrar no modo de edição.
      5) Adicione declarações no seguinte formato:

      Private_IP_address Hostname

      [Exemplo]

      192.168.0.1 hostname01

      192.168.0.2 hostname02
      6) Pressione **Esc** para sair do modo de edição.
      7) Execute o seguinte comando para salvar a configuração e sair:

      :wq

- **Acesso restrito à porta 10180**

  Certifique-se de que o servidor onde o agente será instalado ou atualizado possa se comunicar com o segmento de rede. O grupo de segurança do seu servidor deve permitir acesso de saída à porta 10180 no segmento de rede 100.125.X.X/16.

– Procedimento de solução de problemas

i. No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Compute** > **Elastic Cloud Server**.

ii. Clique no nome do servidor. Na página de detalhes do servidor que é exibida, clique na guia **Security Groups**.

iii. Clique na guia **Outbound Rules** e verifique se a porta 10180 é especificada na política de negação.

1) Se não for especificada, o problema não foi causado pela restrição de acesso à porta.

2) Se for especificada, o problema foi causado pela restrição de acesso à porta.

– Solução

Permite o acesso à porta. Para obter detalhes, consulte a etapa 8 em **Configuração de regras de grupo de segurança**.

- **Memória de VM insuficiente**

– Procedimento de solução de problemas

i. Use uma ferramenta de gerenciamento remoto, como SecureFX ou WinSCP, para fazer logon no servidor.

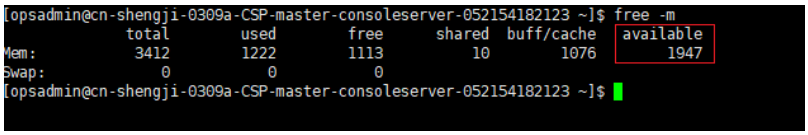
ii. Execute o seguinte comando para verificar o uso de memória do servidor:

free -m

iii. Verifique o valor de **free** na saída do comando, como mostrado na **Figura 2-11**.

Se o valor de **available** for menor que 300, a memória é insuficiente.

Figura 2-11 Consulta de memória



– Solução

■ Feche as aplicações com alto uso de memória.

■ Expanda a memória e tente novamente a instalação. Para obter detalhes sobre como expandir a capacidade de memória, consulte **Operações gerais para modificar especificações**.

- **Falha ao obter metadados**

– Procedimento de solução de problemas

Para obter detalhes sobre como verificar se os metadados podem ser obtidos, consulte **Obtenção de metadados**.

– Solução

Defina a rota para 169.254.169.254. Para obter detalhes, consulte **Por que meu ECS do Linux não consegue obter metadados?**

2.14 E se eu não fizer a atualização da versão do HSS (anterior) para a versão do HSS (novo)?

O HSS (anterior) ainda pode funcionar corretamente, até que seja completamente substituído pela versão de HSS (novo).

Por que você precisa atualizar para o HSS (novo)

- No futuro, a versão de HSS (novo) substituirá a versão de HSS (anterior), que será colocada off-line após a substituição.
- A versão de HSS (novo) fornece novos recursos e aprimora os recursos existentes, conforme descrito na tabela a seguir.

Tabela 2-3 Principais alterações na versão de HSS (novo)

Recurso	Descrição	Tipo
Verificação gratuita em servidores desprotegidos	O HSS verifica periodicamente seus servidores desprotegidos e fornece relatórios para você verificar on-line.	Novo
Gerenciamento de impressão digital de ativos	O HSS verifica profundamente os ativos nos servidores e classifica os ativos em diferentes tipos, como contas, portas, processos, diretórios da Web e informações de software; e exibe estatísticas sobre esses tipos.	Novo
Importância dos ativos	Você pode configurar a importância dos ativos para seus servidores e executar operações neles em lotes, incluindo, mas não se limitando a, implementação de políticas, ativação ou desativação de proteção, atribuição de grupos e instalação de agentes. Para obter detalhes, consulte **Configuração da importância do ativo**.	Novo
Vulnerabilidades de aplicações	O HSS procura vulnerabilidades em serviços da Web, estruturas da Web, sites, middleware e módulos do kernel. Para obter mais informações, consulte **Visualização de detalhes de uma vulnerabilidade**.	Novo
Exportação de relatório de linha de base	Você pode filtrar e exportar os resultados da verificação de configurações de linha de base e senhas fracas comuns.	Novo

Recurso	Descrição	Tipo
Proteção da aplicação	Para proteger as aplicações em execução, basta adicionar sondas a essas aplicações, sem precisar modificar os arquivos da aplicação. Os riscos detectáveis incluem, mas não estão limitados a, injeções de SQL, injeções de comando, entrada de desserialização, passagem de arquivos e execução JSP de comandos do SO. Para obter mais informações, consulte **Ativação da proteção de aplicações**.	Novo
Instalação do agente	Você pode instalar agentes em lotes com apenas alguns cliques. Para obter mais informações, consulte **Instalação de agentes em lote**.	Novo
Gerenciamento de cotas de proteção	Você pode atualizar diretamente uma versão anterior para uma versão posterior. Para obter mais informações, consulte **Gerenciamento de cotas de proteção**.	Novo
Verificação da linha de base	Você pode selecionar itens de verificação de linha de base para avaliar se o seu sistema atende aos requisitos de conformidade. Para obter mais informações, consulte **Gerenciamento de políticas de verificação de linha de base**.	Novo
Gerenciamento de alarmes	Ransomware e shells reversos podem ser isolados e eliminados. Alarmes podem ser gerados para as explorações de vulnerabilidades comuns e vulnerabilidades de Redis, Hadoop e MySQL. Para obter mais informações, consulte **Eventos de alarme de servidor**.	Novo
Relatório de segurança	Você pode personalizar o período do relatório, o conteúdo e o tempo de envio. Para obter mais informações, consulte **Assinatura de um relatório de segurança**.	Atualizado
Detecção de ransomware	O HSS monitora novos arquivos e processos em execução em tempo real, gera dinamicamente arquivos honeypot para atrair e remover ransomware e periodicamente faz backup de servidores com base em políticas definidas pelo usuário. Para obter mais informações, consulte **Ativação da prevenção de ransomware**.	Atualizado
Proteção de container	O Container Guard Service (CGS) original foi integrado à versão de HSS (novo) para gerenciar cargas de trabalho do servidor de maneira unificada.	Integração

2.15 O ECS da Huawei Cloud acessaria quais endereços IP após instalar um agente?

Tabela 2-4 descreve os dispositivos, endereços IP e portas que os servidores da Huawei Cloud normalmente acessam após a instalação de um agente.

Tabela 2-4 Descrição dos endereços IP

Dispositivo de origem	IP de origem	Porta de origem	Dispositivo de destino	IP de destino	Porta de destino (escuta)	Protocolo	Descrição do acesso	Observações
Agente do HSS	Endereço IP de gerenciamento do agente	Aleatória	Servidor HSS	Servidor HSS-IP1 Servidor HSS-IP2	10180	TCP	O agente HSS pode acessar os nós do servidor HSS para obter políticas, configurações e instruções fornecidas pelo servidor, fazer download de pacotes de software do agente, pacotes de atualização e bancos de dados de assinatura, relatar eventos de alarme, bancos de dados de impressões digitais de ativos e resultados de verificação de linha de base e carregar arquivos de programas executáveis suspeitos com autorização do usuário.	O endereço IP do servidor HSS em cada região é diferente. O agente acessa cada endereço IP usando um nome de domínio. O formato do nome de domínio é **hss-agent.{{*REGION_ID*}}.myhuaweicloud.com.*REGION_ID***. Para obter detalhes sobre o nome de domínio de cada região, consulte os comandos de instalação no *Guia de instalação do agente*.

Dispositivo de origem	IP de origem	Porta de origem	Dispositivo de destino	IP de destino	Porta de destino (escuta)	Protocolo	Descrição do acesso	Observações
			Nó do serviço de metadados	Endereço IP do nó de serviço de metadados	80		O agente HSS obtém as informações de metadados do servidor em que o agente está localizado, incluindo o UUID, availability_zone, project_id e enterprise_project_id do ECS.	-

2.16 Como usar imagens para instalar agentes em lotes?

Você pode usar uma imagem privada existente para instalar e implementar um agente em um novo servidor.

NOTA

Não use imagens privadas existentes entre regiões. Caso contrário, o status do agente será **Uninstalled**.

Por exemplo, se você criar uma imagem privada na região A e implementá-la na região B, após a conclusão da implementação, o status do agente na região B será **Uninstalled**. Se você implementar a imagem na região A, o status do agente será **Installed**.

Se precisar usar uma imagem entre regiões, instale a imagem, **desinstale o agente na região original** e limpe suas informações, obtenha o comando de instalação do agente na região de destino e execute comandos para **instalar o agente** na região de destino.

Windows

Execute as seguintes etapas para instalar os agentes do Windows em lotes usando imagens:

Passo 1 Compre um ECS da Huawei Cloud. Selecione a imagem do Windows de destino. Para obter detalhes, consulte **Compra de um ECS**.

Passo 2 Instale um agente no ECS que você comprou. Para obter detalhes, consulte **Instalação de um agente em um servidor Windows**.

NOTA

Não habilite serviços ou modifique configurações diferentes das necessárias para a instalação de agentes do HSS.

Passo 3 Pare o processo do HostGuard no Gerenciador de tarefas do Windows.

Passo 4 Pare o ECS e use-o para criar uma imagem. Para obter detalhes, consulte **Criação de uma imagem**.

NOTA

Depois de interromper o ECS, não o reinicie antes de criar uma imagem. Caso contrário, você precisa repetir **Etapa 3**.

Passo 5 Use a imagem criada para instalar agentes em ECSs do Windows em lotes.

NOTA

O status do agente será atualizado automaticamente de 5 a 10 minutos após a instalação ser bem-sucedida.

----Fim

Linux

Execute as seguintes etapas para instalar agentes no servidor Linux em lotes usando imagens:

Passo 1 Compre um ECS da Huawei Cloud e selecione a imagem do Linux desejada. Para obter detalhes, consulte **Compra de um ECS**.

Passo 2 Instale o agente no ECS comprado. Para obter detalhes, consulte **Instalação de um agente no sistema operacional Linux**.

NOTA

Não habilite serviços ou modifique configurações diferentes das necessárias para a instalação de agentes do HSS.

Passo 3 Interrompa o processo de HSS no ECS.

Execute o comando **ps -ef** para verificar o PID do HSS e, em seguida, execute o comando **kill -pid** para parar o processo de hostguard no sistema operacional Linux.

Passo 4 Pare o ECS e use-o para criar uma imagem. Para obter detalhes, consulte **Criação de uma imagem**.

NOTA

Depois que o ECS for interrompido, não o reinicie antes de criar uma imagem. Caso contrário, você precisa executar as etapas 3 e 4 novamente.

Passo 5 Use a imagem criada para instalar agentes em ECSs do Windows em lotes.

NOTA

O status do agente será atualizado automaticamente de 5 a 10 minutos após a instalação ser bem-sucedida.

----Fim

2.17 O que devo fazer se não conseguir acessar o link de download do agente do Windows?

Possíveis causas

O link para baixar o agente do Windows é um endereço privado da Huawei Cloud. Antes de baixar o agente do Windows, você precisa configurar um endereço DNS privado da Huawei Cloud para o seu servidor. Caso contrário, o servidor não poderá acessar o link.

Solução

Resolva o nome de domínio do servidor usando um **endereço de servidor DNS privado fornecido pela Huawei Cloud** e, em seguida, abra o link para baixar o agente do Windows.

2.18 O que devo fazer se a atualização do agente falhar e a mensagem "File replacement failed" for exibida?

Sintoma

No console do HSS, escolha **Installation & Configuration** e clique na guia **Agents**. Clique em **Online**. Depois que o agente é atualizado, o status de atualização do agente é **Upgrade failed**. Quando você passa o cursor sobre o status, a mensagem "File replacement failed" é exibida.

Solução

O agente 3.2.4 do HSS ou anterior não pode ser atualizado diretamente para a versão mais recente. Você precisa desinstalar manualmente o agente anterior e instalar o agente do HSS mais recente. Para obter detalhes, consulte:

- **Desinstalação do agente**
- **Instalação do agente**

3 Defesa de ataque de força bruta

3.1 Como o HSS intercepta ataques de força bruta?

Tipos de ataques de força bruta detectáveis

O HSS pode detectar os seguintes tipos de ataques de força bruta:

- Windows: SqlServer (interceptação automática não é suportada atualmente) e Rdp
- Linux: MySQL, vfstp e SSH

Se o MySQL ou o VSFTP estiver instalado em seu servidor, depois que o HSS for ativado, o agente adicionará regras a iptables para evitar ataques de força bruta do MySQL e VSFTP. Ao detectar um ataque de força bruta, o HSS adicionará o endereço IP de origem à lista de bloqueio. As regras adicionadas estão destacadas abaixo.

Figura 3-1 Regras adicionadas

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
IN_HIDS_MYSQLD_BIP_DROP  tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:3306
IN_HIDS_MYSQLD_DENY_DROP  tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:3306

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain IN_HIDS_MYSQLD_BIP_DROP (1 references)
target     prot opt source               destination

Chain IN_HIDS_MYSQLD_DENY_DROP (1 references)
target     prot opt source               destination
```

AVISO

As regras existentes do iptables são usadas para bloquear ataques de força bruta. É aconselhável mantê-las. Se elas forem excluídas, o HSS não será capaz de proteger o MySQL ou o VSFTP de ataques de força bruta.

Como os ataques de força bruta são interceptados

Os ataques de força bruta são um tipo de ataque de intrusão comum. Os atacantes enviam muitas senhas de servidor até que, eventualmente, adivinham corretamente e ganham controle sobre um servidor.

O HSS usa algoritmos de detecção de força bruta e uma lista negra de endereços IP para prevenir efetivamente ataques de força bruta e bloquear endereços IP de ataque. A duração do bloqueio para ataques SSH suspeitos é de 12 horas e para outros ataques suspeitos é de 24 horas. **Se um endereço IP bloqueado não realizar ataques de força bruta na duração de bloqueio padrão, ele será desbloqueado automaticamente**. O HSS suporta **2FA** para autenticar a identidade do usuário, impedindo efetivamente que invasores invadam contas.

Você pode **definir endereços IP de logon comuns** e **lista branca de endereços IP SSH** que não serão bloqueados.

NOTA

Se o HSS detectar ataques de quebra de contas em servidores usando o Kunpeng EulerOS (EulerOS com ARM), ele não bloqueará os endereços IP de origem e gerará apenas alarmes. A lista branca de endereços IP de logon SSH não entra em vigor para esses servidores.

Políticas de alarme

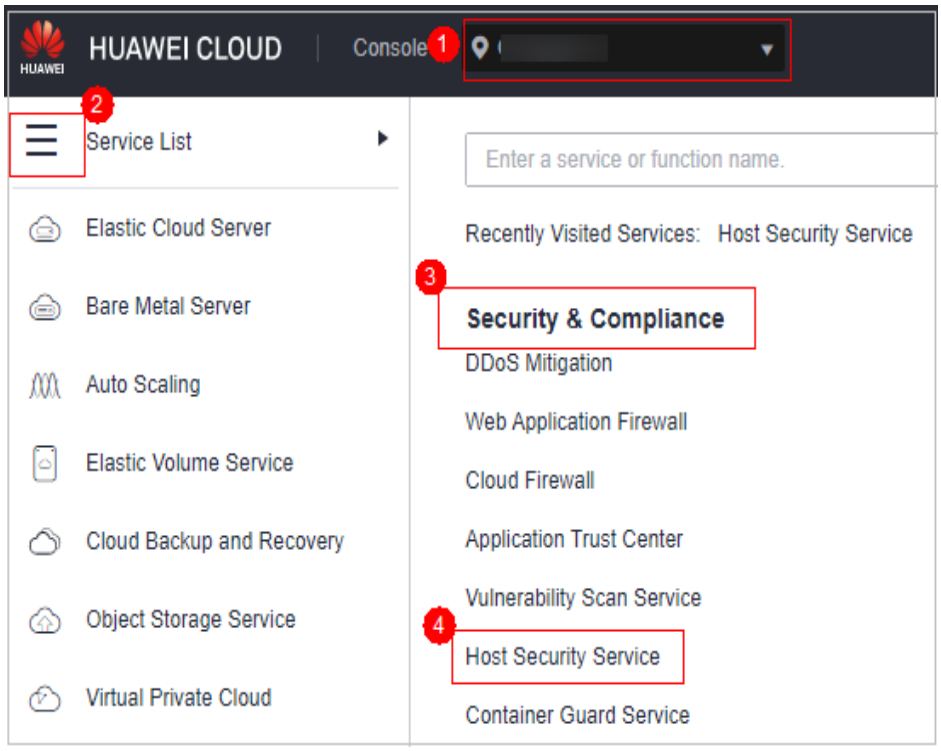
- Se um hacker quebrar com sucesso a senha e fizer logon em um servidor, um alarme em tempo real será enviado imediatamente aos destinatários especificados.
- Se um ataque de força bruta e riscos de invasão de contas forem detectados, um alarme em tempo real será enviado imediatamente para os destinatários especificados.
- Se um ataque de força bruta for detectado e falhar, e nenhuma configuração insegura (como senhas fracas) for detectada no servidor, nenhum alarme em tempo real será enviado. O HSS resumirá todos os ataques em um dia em seu relatório diário de alarme. Você também pode visualizar ataques bloqueados na página **Intrusions** do console do HSS.

Visualização dos resultados da detecção de quebra por força bruta

Passo 1 **Faça logon no console de gerenciamento**.

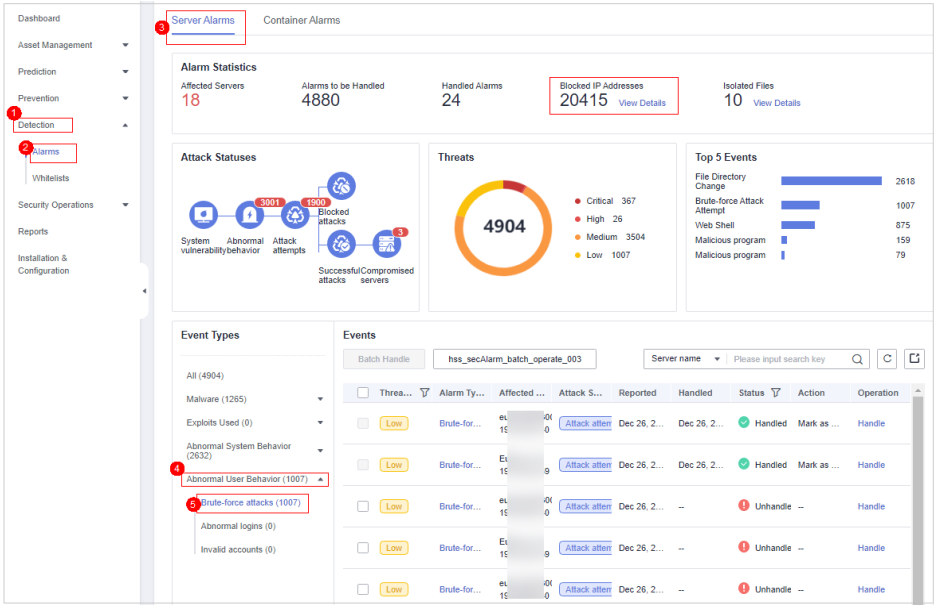
Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 3-2 Acessar o HSS



Passo 3 Na tabela exibida após clicar em **Brute-force attacks**, você pode visualizar ataques bloqueados em servidores protegidos.

Figura 3-3 Ataques de força bruta



Passo 4 Clique em **View Details** em **Blocked IP Addresses** para verificar os endereços IP de origem, os tipos de ataques, o número de ataques interceptados, a hora da primeira e da última interceptação e o status da interceptação.

- **Blocked** indica que o ataque de força bruta foi bloqueado pelo HSS.

- **Canceled** indica que você desbloqueou o endereço IP de origem do ataque de força bruta.

  NOTA

  Por padrão, os invasores SSH suspeitos são bloqueados por 12 horas. Outros tipos de invasores suspeitos são bloqueados por 24 horas. Se um endereço IP bloqueado não realizar ataques de força bruta na duração de bloqueio padrão, ele será desbloqueado automaticamente.

----Fim

Gerenciamento de endereços IP bloqueados

- Se um servidor é frequentemente atacado, é aconselhável corrigir suas vulnerabilidades em tempo hábil e eliminar os riscos.

  É aconselhável ativar a **2FA** e configurar **endereços IP de logon comuns** e a **lista branca de IP de logon SSH**.
- Se um endereço IP válido for bloqueado por engano (por exemplo, depois que o pessoal de O&M inserir senhas incorretas várias vezes), **desbloqueie manualmente o endereço IP**.

AVISO

Se você desbloqueou manualmente um endereço IP, mas tentativas incorretas de senha desse endereço IP atingirem o limite novamente, esse endereço IP será bloqueado novamente.

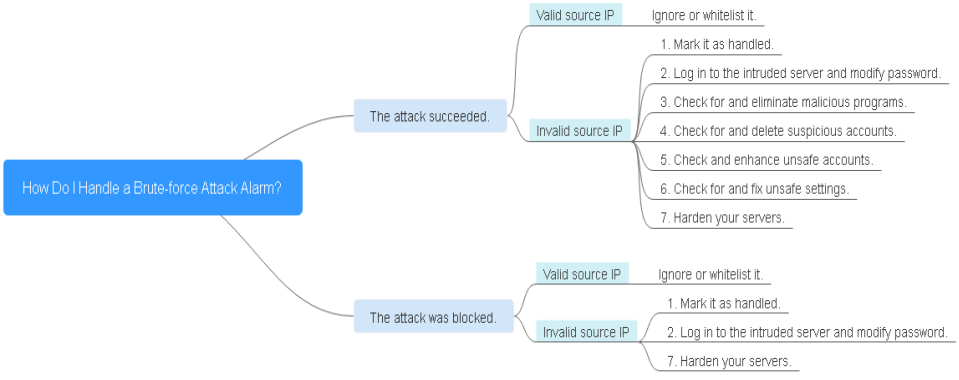
3.2 Como lidar com um alarme de ataque de força bruta?

- Se um ataque de força bruta foi bem-sucedido, tome medidas imediatas para evitar que os invasores realizem outras ações, como violação de dados, realização de ataques de DDoS ou implementação de ransomware, mineradores ou cavalos de Troia.
- Se um ataque de força bruta foi bloqueado, tome medidas imediatas para melhorar seus servidores.

Mapa de ideias para solução de problemas

O mapa de ideias a seguir descreve como lidar com um alarme de ataque de força bruta.

Figura 3-4 Mapa de ideias para solução de problemas



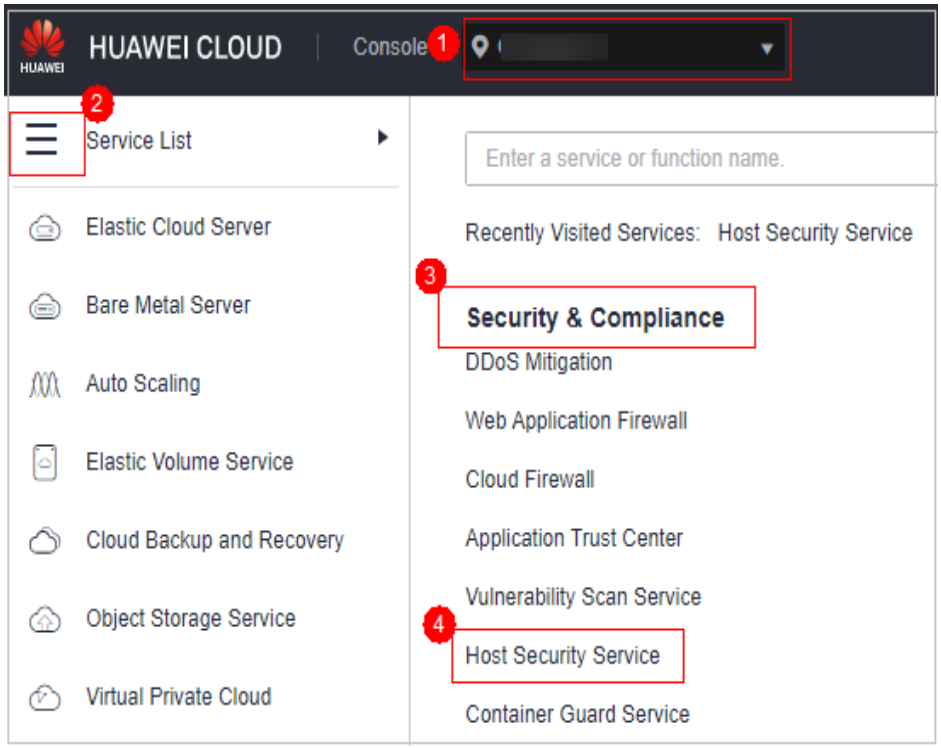
Lidar com o alarme de um ataque de força bruta bem-sucedido

Se você recebeu uma notificação de alarme indicando que sua conta foi invadida, é aconselhável reforçar os seus servidores o mais rápido possível.

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 3-5 Acessar o HSS



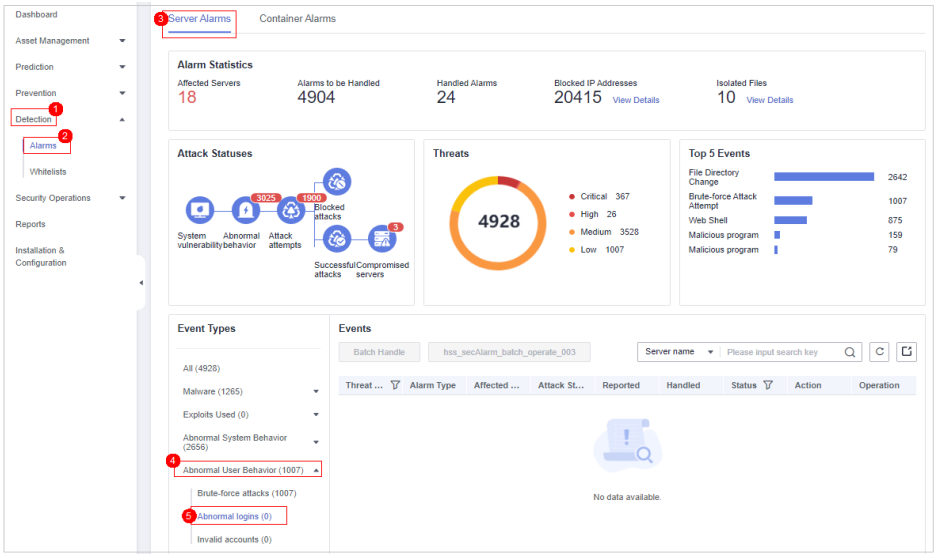
Passo 3 Verifique se o endereço IP que acionou o alarme é válido.

Escolha **Detection** > **Alarms**. Na área **Event Types**, escolha **Abnormal User Behavior** > **Abnormal logins** e verifique o endereço IP de logon.

- Se o endereço IP for de um usuário normal (por exemplo, quem digitou a senha incorreta por várias vezes, mas fez logon antes de sua conta ser bloqueada), seu servidor não será invadido. Nesse caso, você pode clicar em **Handle** e ignorar o evento.
- Se o endereço IP for inválido, o seu servidor pode ter sido invadido.

  Nesse caso, marque esse evento como tratado, faça logon no servidor invadido e altere sua senha para uma mais forte. Para mais detalhes, consulte **Como definir uma senha segura?**

Figura 3-6 Logons anormais



Passo 4 Verifique e elimine programas maliciosos.

Escolha **Malware** > **Malicious programs** e verifique eventos de alarme.

- Se você encontrar programas maliciosos implementados em seus servidores, localize-os com base em seus caminhos de processo, usuários que os executam e tempo de inicialização.

  Para eliminar um programa malicioso em um evento de alarme, clique em **Handle** na linha deste evento e selecione **Isolate and kill**.

- Se você confirmou que todos os alarmes do programa malicioso são falsos, vá para **Etapa 8**.

Passo 5 Verifique se existem registos de alterações de contas suspeitos.

Escolha **Asset Management** > **Asset Fingerprints** e clique na guia **Account Information**. Detecte registros de alteração de conta suspeitos para impedir que invasores criem contas ou aumentem permissões de conta (por exemplo, adicionar permissões de logon a uma conta). Para obter detalhes, consulte **Verificação do histórico da operação**.

Passo 6 Verifique e lide com contas inválidas.

Escolha **Detection** > **Alarms**. Escolha **Abnormal User Behavior** > **Invalid accounts** para visualizar e lidar com os alarmes de contas inválidas. Para obter detalhes, consulte **Tratamento de alarmes do servidor**.

Passo 7 Verifique e corrija configurações inseguras.

Verifique e corrija políticas de complexidade de senha fraca e configurações de software inseguras em seus servidores. Para obter detalhes, consulte **Sugestões sobre como corrigir configurações inseguras**.

Passo 8 Reforce os seus servidores.

- Para obter mais informações, consulte **Reforço da segurança para logons SSH em ECSs de Linux**.

----Fim

Lidar com o alarme de um ataque de força bruta bloqueado

Se você ativou uma edição superior ao HSS básico, o HSS protegerá seus servidores contra ataques de força bruta.

Você pode configurar uma política de segurança de logon para especificar o modo de determinação de quebra por força bruta e a duração do bloqueio. Para obter detalhes, consulte **Verificação de segurança de logon**.

Se você não tiver configurado nenhuma política de detecção de segurança de logon, será usada a seguinte política de segurança de logon padrão: o HSS bloqueará um endereço IP se ele tiver cinco ou mais tentativas de ataque de força bruta detectadas em 30 segundos ou 15 ou mais tentativas de ataque de força bruta detectadas em 3.600 segundos.

Se você receber um alarme indicando que um endereço IP de origem de ataque está bloqueado, verifique se o endereço IP de origem é um endereço IP confiável.

Restrições e limitações

- Linux

  Em servidores que executam o EulerOS com ARM, o HSS não bloqueia os endereços IP suspeitos de ataques de força bruta de SSH, mas apenas gera alarmes.

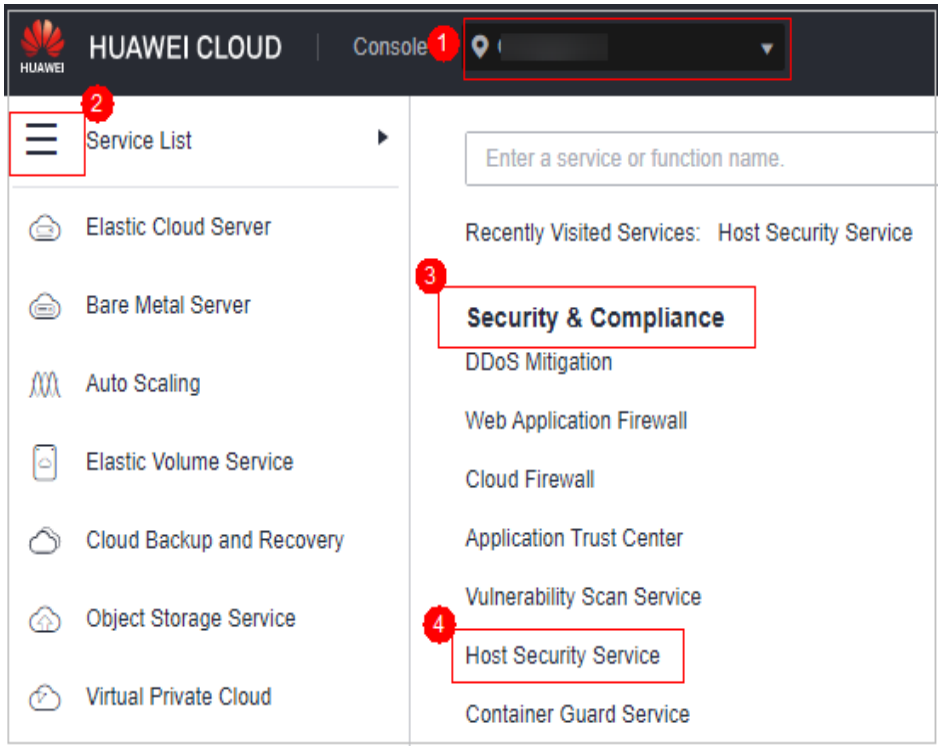
- Windows
  - Autorize o firewall do Windows quando ativar a proteção para um servidor do Windows. Não desative o firewall do Windows durante o período de serviço do HSS. Se o firewall do Windows estiver desativado, o HSS não poderá bloquear endereços IP de ataque de força bruta.
  - Se o firewall do Windows estiver ativado manualmente, o HSS também pode falhar ao bloquear endereços IP de ataque de força bruta.

Procedimento

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 3-7 Acessar o HSS

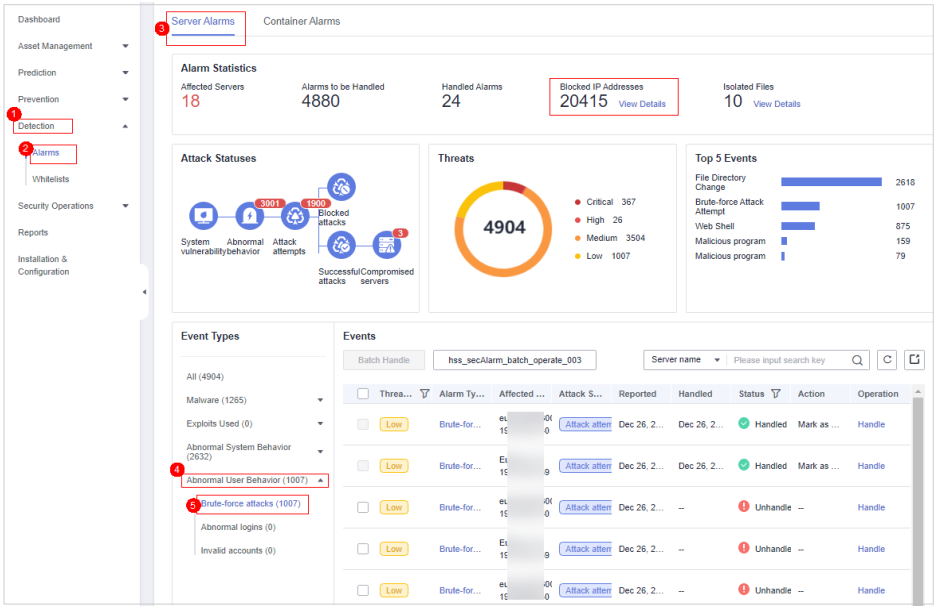


Passo 3 Escolha **Detection** > **Alarms**. Escolha **Abnormal User Behavior** > **Brute-force attacks** para visualizar eventos de força bruta da conta.

Alarmes de ataque de força bruta serão gerados se:

- O sistema que usa senhas fracas, estiver a ser alvo de ataques de força bruta e os endereços IP dos atacantes estiverem bloqueados.
- Os usuários não conseguirem fazer logon após várias tentativas de senha incorreta e os seus endereços IP forem bloqueados.

Figura 3-8 Ataques de força bruta



Passo 4 Verifique se o endereço IP de logon que aciona o alarme é válido.

- Se o endereço IP for válido,
  - Para lidar com um alarme falso, clique em **Handle** na linha do evento de alarme. Ignore ou coloque o endereço IP na lista branca.

    Isso não desbloqueia o endereço IP.
  - Para desbloquear o endereço IP, clique em **View Details** em **Blocked IP Addresses**, selecione o endereço IP e desbloqueie-o. Alternativamente, você pode apenas esperar que ele seja desbloqueado automaticamente quando sua duração de bloqueio expirar.

    Por padrão, os invasores SSH suspeitos são bloqueados por 12 horas. Outros tipos de invasores suspeitos são bloqueados por 24 horas.
- Se o endereço IP de origem for inválido ou desconhecido,

  Marque esse evento como tratado.

  Imediatamente faça logon no seu servidor e altere sua senha para uma mais forte. Também é possível melhorar a defesa contra ataques de força bruta seguindo as instruções fornecidas em **Como me defender contra ataques de força bruta?**

----Fim

Links úteis

- **Como o HSS intercepta ataques de força bruta?**
- **Como desbloquear um endereço IP?**

3.3 Como me defender contra ataques de força bruta?

Impacto dos ataques de força bruta

Intrusos que invadiram contas de servidores podem explorar permissões para roubar ou adulterar dados em servidores, interrompendo serviços empresariais e causando grandes perdas.

Medidas preventivas

- Configure a lista branca do logon SSH.

  A lista branca de logon SSH permite logons a partir de apenas endereços IP da lista branca, efetivamente impedindo a quebra de contas. Para obter detalhes, consulte **Configuração de uma lista branca de endereços IP de logon SSH**.
- Ative a 2FA.

  A 2FA exige que os usuários forneçam códigos de verificação antes de fazer logon. Os códigos serão enviados para seus telefones celulares ou caixas de e-mail.

  Escolha **Installation & Configuration**. Na guia **Two-Factor Authentication**, selecione servidores e clique em **Enable 2FA**. Para obter detalhes, consulte **Ativação de 2FA**.
- Use portas não padrão.

  Altere as portas de gerenciamento remoto padrão 22 e 3389 para outras portas.
- Configure regras de grupo de segurança para impedir que os endereços IP de ataque acessem suas portas de serviço.

> **NOTA**
>
> É aconselhável permitir que apenas endereços IP especificados acessem as portas de gerenciamento remoto abertas (por exemplo, para SSH e logon na área de trabalho remota).

O HSS **intercepta ataques de força bruta** em contas de servidor em tempo real e bloqueia endereços IP de origem de ataque. Você pode **configurar regras de grupo de segurança** para controlar o acesso aos seus servidores.

Para uma porta usada para logon remoto, você pode definir endereços IP com permissão para efetuar logon remotamente em seus ECSs.

Para permitir que o endereço IP **192.168.20.2** acesse remotamente os ECSs de Linux em um grupo de segurança por meio do protocolo SSH e da porta 22, você pode configurar a seguinte regra de grupo de segurança.

Tabela 3-1 Configurar endereços IP para se conectar remotamente a ECSs

Direção	Protocolo/ aplicação	Porta	Fonte
Entrada	SSH	22	Por exemplo, 192.168.20.2/32

- Defina uma senha forte.

  A verificação da política de senha e **a detecção de senhas fracas** podem encontrar contas que usam senhas fracas em seus servidores. Você pode visualizar e lidar com riscos de senha no console.

3.4 Como fazer se a função de prevenção de quebra de conta não tiver efeito em algumas contas do Linux?

Possíveis causas

O serviço SSHD no sistema host não depende do **libwrap.so**.

> **NOTA**
>
> Como uma biblioteca de software gratuita, libwrap implementa a função universal TCP Wrapper. Qualquer daemon que contenha **libwrap.so** pode usar as regras nos arquivos **/etc/hosts.allow** e **/etc/hosts.deny** para executar controle de acesso simples no host.

Solução

Faça logon no servidor e instale o agente do HSS. Em seguida, execute o seguinte comando:

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

Versões de imagem afetadas

- A seguir estão as imagens de Gentoo que têm o problema:
  - Gentoo Linux 17.0 64bit (40 GB)
  - Gentoo Linux 13.0 64bit (40 GB)

- A seguir estão as imagens de OpenSUSE que têm o problema:
  - OpenSUSE 42.2 64bit (40 GB)
  - OpenSUSE 13.2 64bit (40 GB)

3.5 Como desbloquear um endereço IP?

O HSS bloqueará um endereço IP se ele tiver cinco ou mais tentativas de ataque de força bruta detectadas dentro de 30 segundos ou 15 ou mais tentativas de ataque de força bruta detectadas dentro de 3600 segundos. Se um endereço IP normal for bloqueado por engano (por exemplo, após pessoal de O&M inserir senhas incorretas várias vezes), você pode desbloquear o endereço IP.

Se você desbloqueou manualmente um endereço IP, mas tentativas incorretas de senha desse endereço IP atingirem o limite novamente, esse endereço IP será bloqueado novamente.

NOTA

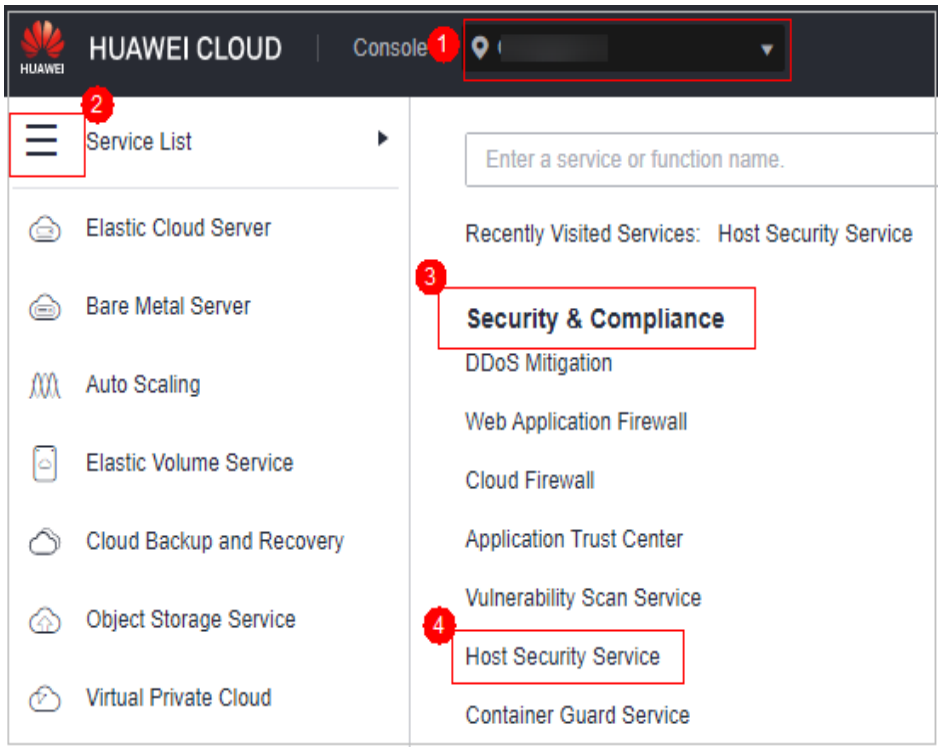
- Por padrão, os invasores SSH suspeitos são bloqueados por 12 horas. Outros tipos de invasores suspeitos são bloqueados por 24 horas.
- Se um endereço IP bloqueado não realizar ataques de força bruta na duração de bloqueio padrão, ele será desbloqueado automaticamente.

Procedimento

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

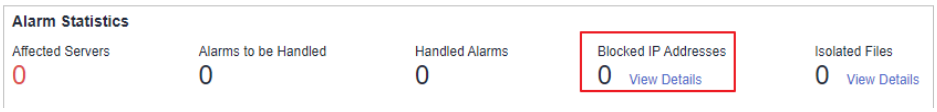
Figura 3-9 Acessar o HSS



Passo 3 Na árvore de navegação à esquerda, selecione **Detection** > **Alarms** e clique em **Server Alarms**.

Passo 4 Na área de **Alarm Statistics**, clique em **View Details** em **Blocked IP Addresses**.

Figura 3-10 Endereços IP bloqueados



Passo 5 Na lista de endereços IP bloqueados, selecione um endereço IP e clique em **Cancel Interception**.

Figura 3-11 Desbloquear um endereço IP

----Fim

3.6 O que devo fazer se o HSS relatar alarmes de força bruta com frequência?

NOTA

Um alarme indica que um ataque foi detectado. Isso não significa que seus servidores em nuvem foram invadidos.

Se você receber um alarme, trate-o e tome as contramedidas em tempo hábil.

Possível causa: nenhum controle de acesso é configurado para as portas usadas para conexão remota aos seus servidores. Como resultado, os vírus na rede frequentemente atacavam suas portas.

Solução: tome qualquer uma das seguintes medidas.

1. Configure uma lista branca.
2. Use outra porta.
3. Configure regras de grupos de segurança.
4. Habilite a 2FA.
5. Configure uma senha forte.

Para obter detalhes, consulte **Como defender contra ataques de força bruta?**

3.7 Como lidar com alarmes sobre ataques de força bruta lançados a partir de um endereço IP da Huawei Cloud?

NOTA

Um alarme indica que um ataque foi detectado. Isso não significa que seus servidores em nuvem foram invadidos.

Se você receber um alarme, trate-o e tome as contramedidas em tempo hábil.

Possível causa

Alguns usuários de servidores da Huawei Cloud usam senhas simples ou portas comuns, ou não usam nenhum produto de proteção de segurança. As contas desses usuários podem ser facilmente quebradas. Os atacantes podem explorar as contas e atacar outros usuários. Desta forma, os alarmes são reportados a partir dos endereços IP das contas exploradas.

Solução

- Restrinja o acesso dos endereços IP que acionaram os alarmes. Para obter detalhes, consulte **Adição de uma regra de grupo de segurança**.
- Quando ataques de força bruta são detectados, eles são bloqueados imediatamente e os alarmes são relatados. Trate o alarme dentro de sete dias ou os EIPs que acionaram os alarmes serão bloqueados até que seus alarmes sejam tratados.

NOTA

- Você pode aumentar a segurança definindo senhas fortes e alterando portas. Para obter detalhes, consulte **Como me defender de ataques de força bruta?**
- Você pode comprar HSS para proteger seus servidores. Para obter mais informações, consulte **Compra de cotas de HSS**. Para obter detalhes sobre as edições do HSS, consulte **Edições**.

3.8 O que devo fazer se a porta do meu servidor remoto não for atualizada nos registros de ataques de força bruta?

Sintoma

A porta remota de um servidor foi alterada, mas os registros de ataque de força bruta ainda exibem a porta anterior.

Solução

A configuração de porta remota é sincronizada com o HSS por meio de agente. Se a porta remota for alterada, execute as seguintes operações para reiniciar o agente:

- Windows: efetue logon no servidor como um administrador. Abra o Gerenciador de Tarefas, clique com o botão direito do mouse em **HostGuard** e escolha **Restart** no menu de atalho.
- Linux: execute o comando **service hostguard restart** como usuário **root**.

4 Senhas fracas e contas inseguras

4.1 Como lidar com um alarme de senha fraca?

Servidores que usam senhas fracas estão expostos a invasões. Se um alarme de senha fraca for relatado, é aconselhável alterar a senha alarmada imediatamente.

Causas

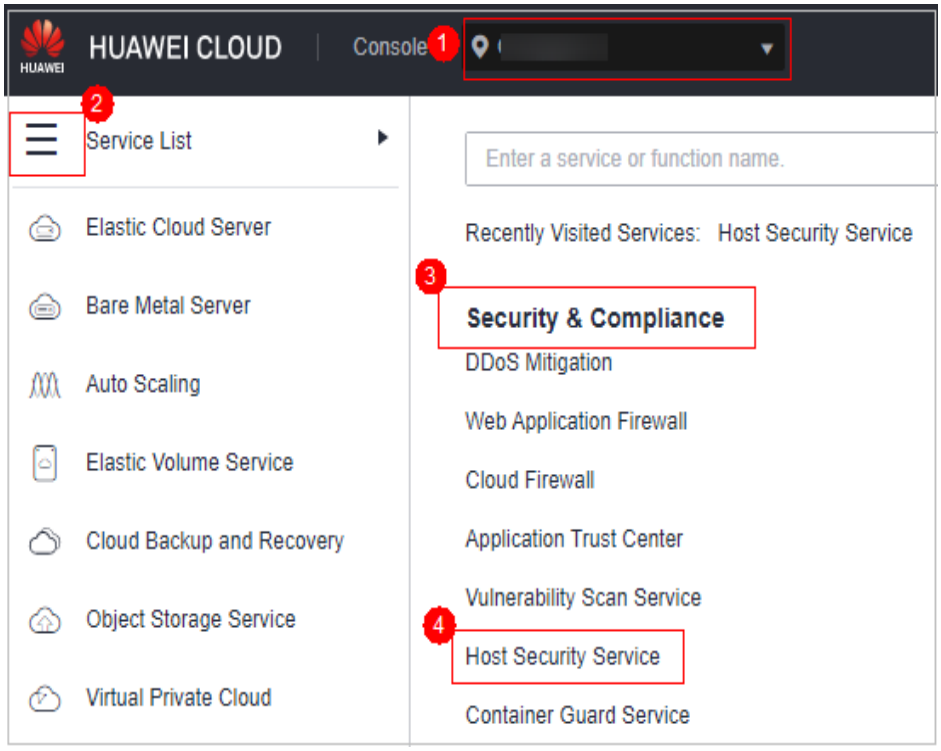
- Se forem usadas senhas simples que correspondam às da biblioteca de senhas fracas, será gerado um alarme de senha fraca.
- Uma senha usada por várias contas de membros será considerada uma senha fraca e acionará um alarme.

Verificar e alterar senhas fracas

Passo 1 **Faça logon no console de gerenciamento**.

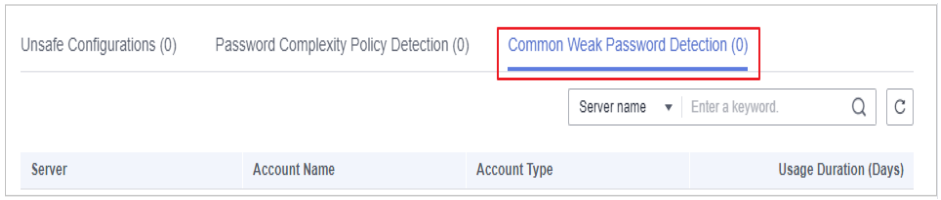
Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 4-1 Acessar o HSS



Passo 3 Escolha **Prediction** > **Baseline Checks** e clique na guia **Common Weak Password Detection**.

Figura 4-2 Senhas fracas comuns



Passo 4 Verifique o servidor, o nome da conta, o tipo de conta e a duração de uso da senha fraca. Faça logon no servidor e altere a senha.

----Fim

Alteração de uma senha fraca

Sistema	Procedimento	Observações
SO Windows	Para alterar a senha no Windows 10, execute as seguintes etapas: 1. Faça logon no SO Windows. 2. Clique em  no canto inferior esquerdo e clique em  . 3. Na janela **Windows Settings**, clique em **Accounts**. 4. Escolha **Sign-in options** na árvore de navegação. 5. Na guia **Sign-in options**, clique em **Change** em **Password**.	Nenhuma
SO Linux	Faça logon no servidor do Linux e execute o seguinte comando: **passswd [<*user*>]**	Se você não especificar nenhum nome de usuário, estará alterando a senha do usuário atual. Depois que o comando for executado, digite a nova senha conforme solicitado. **NOTA** Substitua <*user*> pelo nome de usuário.

Sistema	Procedimento	Observações
Banco de dados MySQL	1. Faça logon no banco de dados MySQL. 2. Execute o seguinte comando para verificar a senha do usuário do banco de dados: **SELECT user, host, authentication_string From user;** Este comando é provavelmente inválido em certas versões do MySQL. Nesse caso, execute o seguinte comando: **SELECT user, host password From user;** 3. Execute o seguinte comando para alterar a senha: **SET PASSWORD FOR'*Username*'@'*Host*'=PASSWORD('*New_password*');** 4. Execute o seguinte comando para atualizar as configurações de senha: **flush privileges;**	Nenhuma
Banco de dados Redis	1. Abra o arquivo de configuração do banco de dados Redis **redis.conf**. 2. Execute o seguinte comando para alterar a senha: **requirepass <*password*>;**	● Se já houver uma senha, o comando irá alterá-la para a nova senha. ● Se não houver uma senha definida, o comando definirá a senha. **NOTA** Substitua <*password*> pela nova senha.
Tomcat	1. Abra o arquivo de configuração **conf/tomcat-user.xml** no diretório raiz do Tomcat. 2. Altere o valor de **password** no nó de **user** para uma senha forte.	Nenhuma

4.2 Como definir uma senha segura?

Observe as seguintes regras:

- Use uma senha com alta complexidade.

  A senha deve atender aos seguintes requisitos:

  a. Contém pelo menos oito caracteres.

b. Contém pelo menos três tipos dos seguintes caracteres:
   i. Letras maiúsculas (A-Z)
   ii. Letras minúsculas (a-z)
   iii. Digitais (0-9)
   iv. Caracteres especiais
c. A senha não pode ser o nome de usuário ou o nome de usuário na ordem inversa.

- Não use senhas fracas comuns que são fáceis de quebrar, incluindo:
  – Aniversário, nome, carteira de ID, número de celular, endereço de e-mail, ID do usuário, hora ou data
  – Dígitos e letras consecutivos, caracteres de teclado adjacentes ou senhas em tabelas arco-íris
  – Frases
  – Palavras comuns, como nomes de empresas, **admin** e **root**
- Não use senhas vazias ou padrão.
- Não reutilize as últimas cinco senhas que você usou.
- Use senhas diferentes para sites e contas diferentes.
- Não use o mesmo par de nome de usuário e senha para vários sistemas.
- Altere sua senha pelo menos uma vez a cada 90 dias.
- Se uma conta tiver uma senha inicial, force o usuário a alterar a senha no primeiro logon ou dentro de um período limitado de tempo.
- É aconselhável definir uma política de bloqueio para todas as contas. Se as falhas consecutivas de logon de uma conta excederem cinco vezes, a conta será bloqueada e será desbloqueada automaticamente em 30 minutos.
- Você é aconselhado a definir uma política de logout. As contas que estiverem inativas por mais de 10 minutos serão automaticamente desconectadas ou bloqueadas.
- Você é aconselhado a forçar os usuários a alterar as senhas iniciais de suas contas no primeiro logon.
- É aconselhável manter os registros de logon da conta por pelo menos 180 dias. Os logs não podem conter senhas de usuários.

4.3 Por que os alarmes de senha fraca ainda são relatados depois que a política de senha fraca é desativada?

Se você tiver melhorado senhas antes de desativar a política de senha fraca, o alarme de senha fraca não será relatado novamente.

Se você não melhorar as senhas antes de desativar a política de senha fraca, o alarme relatado persistirá e será retido por 30 dias.

- Para melhorar a segurança do servidor, é aconselhável modificar as contas com senhas fracas em tempo hábil, como contas de SSH.
- Para proteger os dados internos do seu servidor, é aconselhável modificar contas de software que usam senhas fracas, como contas de MySQL e contas de FTP.

Depois de modificar senhas fracas, é aconselhável executar a detecção manual imediatamente para verificar o resultado. Se você não executar a verificação manual e não desativar a

verificação de senha fraca, o HSS verificará automaticamente as configurações no dia seguinte no início da manhã.

5 Invasões

5.1 Como visualizar e lidar com alarmes relatados pelo HSS?

Visualizar alarmes

Para obter detalhes sobre como visualizar alarmes do HSS, consulte **Visualização de alarmes de intrusão**. Para obter detalhes sobre como visualizar alarmes de CGS, consulte **Visualização de alarmes de container**.

Manipulação de alarmes

Você pode corrigir vulnerabilidades, verificar e bloquear intrusões e corrigir configurações inseguras com base nas sugestões fornecidas. Para obter detalhes, consulte **Manipulação de alarmes do servidor**.

O CGS permite que você lide com alarmes. Para obter detalhes, consulte **Manipulação de alarmes de containers**.

5.2 O que devo fazer se meus servidores forem submetidos a um ataque de mineração?

Tome medidas imediatas para conter o ataque, evitando que os mineradores ocupem a CPU ou afetem outras aplicações. Se um servidor é invadido por um programa de mineração, o programa de mineração pode penetrar na intranet e persistir no servidor invadido.

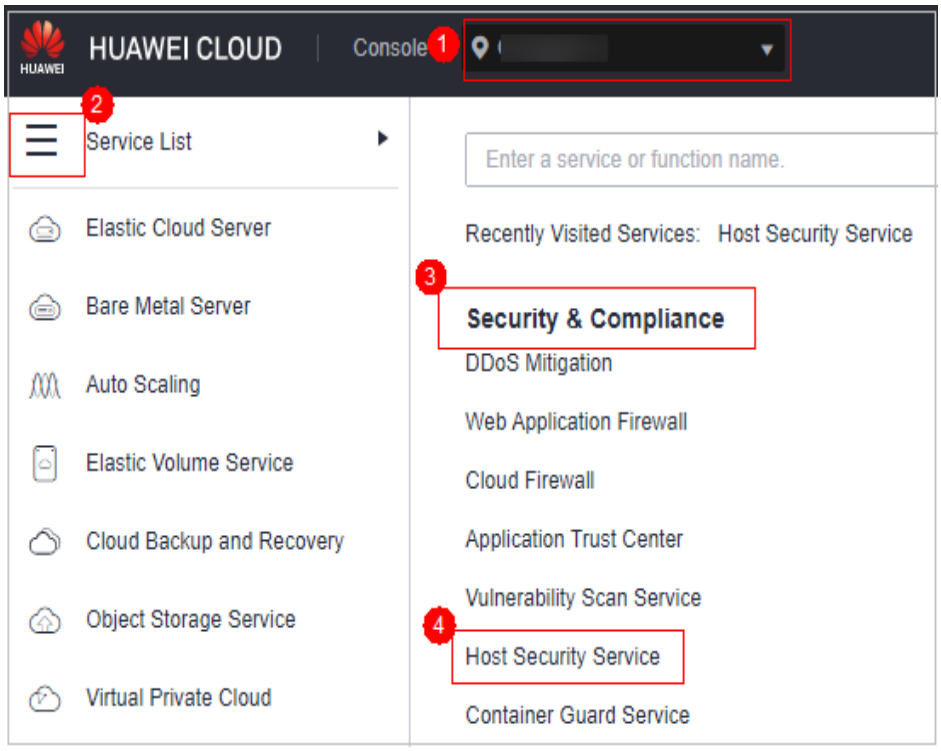
Você também deve fortalecer seus servidores para bloquear melhor as invasões.

Procedimento de solução de problemas

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

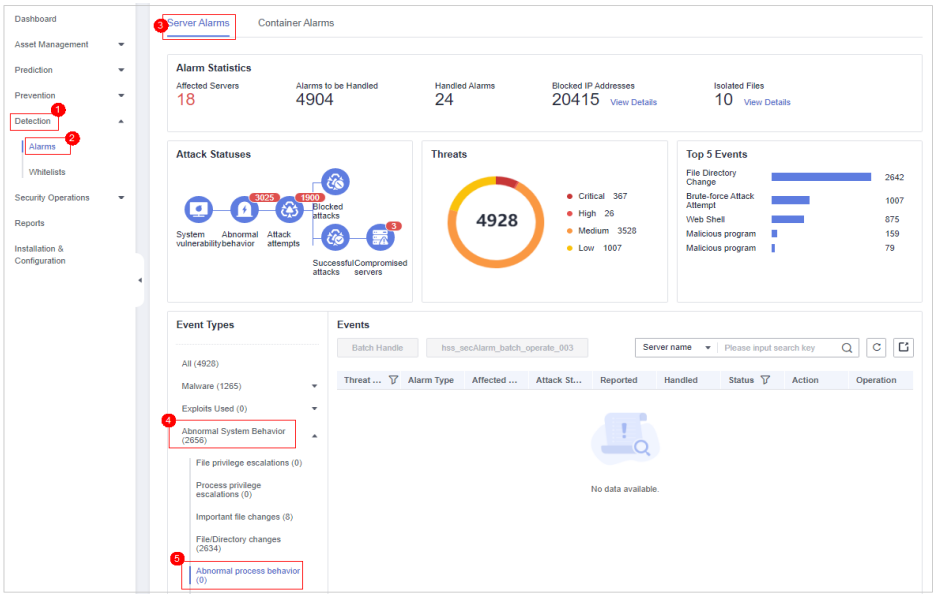
Figura 5-1 Acessar o HSS



Passo 3 Verifique eventos de **Abnormal process behavior**.

Escolha **Detection** > **Alarms** e clique em **Server Alarms**. Escolha **Abnormal System Behavior** > **Abnormal process behavior** para visualizar e manipular os alarmes de comportamento anormal do processo. Clique em **Handle** na coluna **Operation** de um evento.

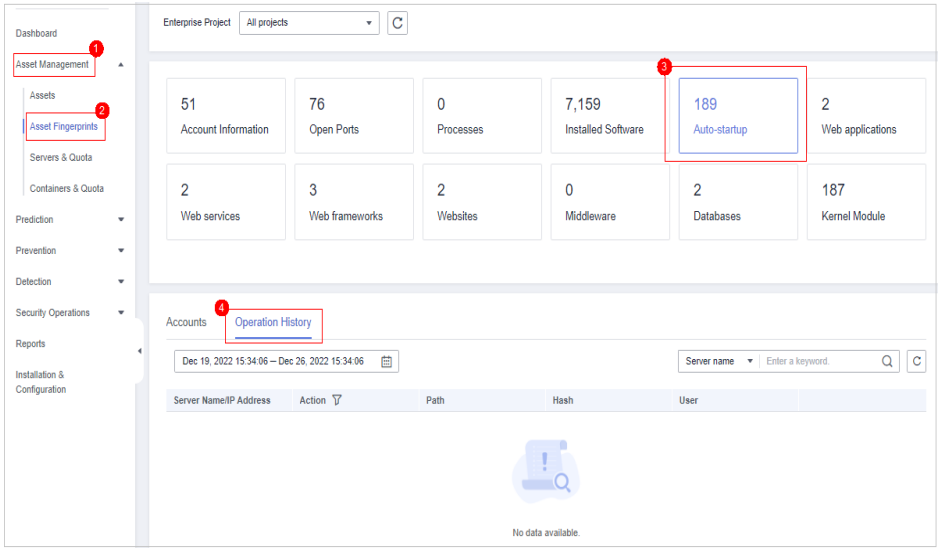
Figura 5-2 Manipulação do comportamento anormal do processo



Passo 4 Verifique os itens de inicialização automática. Alguns de seus itens de inicialização automática provavelmente foram criados por invasores para iniciar programas de mineração após a reinicialização do servidor.

Escolha **Asset Management** > **Asset Fingerprints**, clique em **Auto-startup** e selecione **Operation History** para visualizar o histórico de alterações.

Figura 5-3 Verificação de itens de inicialização automática



----Fim

Fortalecimento de servidores

Depois de excluir programas de mineração, fortaleça seus servidores para se defender melhor contra invasões.

Servidores do Linux

1. Deixe o HSS verificar automaticamente seus servidores e aplicações no início da manhã todos os dias para ajudá-lo a detectar e eliminar riscos de segurança.
2. Defina senhas mais fortes para todas as contas (incluindo contas do sistema e da aplicação) ou altere o modo de logon para logon baseado em chave.
   a. Defina a senha de segurança. Para mais detalhes, consulte **Como definir uma senha segura?**.
   b. Use uma chave para fazer logon no servidor. Para obter detalhes, consulte **Uso de uma chave privada para fazer logon no ECS de Linux**.
3. Controle estritamente o uso de contas de administrador do sistema. Conceda apenas as permissões mínimas necessárias para aplicações e middleware e controle estritamente seu uso.
4. Configure regras de acesso em grupos de segurança. Abra apenas as portas necessárias. Para portas especiais (como portas de logon remoto), permita apenas o acesso de endereços IP especificados ou use VPN ou bastion hosts para estabelecer seus próprios canais de comunicação. Para obter detalhes, consulte **Regras de grupo de segurança**.

Servidores do Windows

Use o HSS para verificar e eliminar riscos de segurança de forma abrangente. Melhore a segurança da sua conta, senha e autorização.

- **Fortalecimento da conta**

Conta	Descrição	Procedimento
Garantir a segurança da conta padrão.	● Desativar usuário **Guest**. ● Desativar e excluir contas desnecessárias. (Você é aconselhado a desativar contas inativas por três meses antes de excluí-las.)	1. Abra **Control Panel**. 2. Clique em **Administrative Tools**. Abra **Computer Management**. 3. Escolha **System Tools** > **Local Users and Groups** > **Users**. 4. Clique duas vezes em **Guest**. Na janela **Guest Properties**, selecione **Account is disabled**. 5. Clique em **OK**.
Atribuir contas apenas com as permissões necessárias aos usuários.	Criar usuários e grupos de usuários de tipos específicos. Exemplo: administradores, usuários de banco de dados, usuários de auditoria	1. Abra **Control Panel**. 2. Clique em **Administrative Tools**. Abra **Computer Management**. 3. Escolha **System Tools** > **Local Users and Groups**. Crie usuários e grupos conforme necessário.
Verificar periodicamente e excluir contas desnecessárias.	Excluir ou bloquear periodicamente contas desnecessárias.	1. Abra **Control Panel**. 2. Clique em **Administrative Tools**. Abra **Computer Management**. 3. Escolha **System Tools** > **Local Users and Groups**. 4. Escolha **Users** ou **User Groups** e exclua usuários ou grupos de usuários desnecessários.
Não exibir o último nome de usuário.	Proibir que a página de logon exiba o último usuário logado.	1. Abra **Control Panel**. 2. Clique em **Administrative Tools**. Abra **Local Security Policy**. 3. Escolha **Local Policies** > **Security Options**. 4. Clique duas vezes em **Interactive logon: Do not display last user name**. 5. Na caixa de diálogo exibida, selecione **Enable** e clique em **OK**.

- **Fortalecimento de senha**

Configuração	Descrição	Procedimento
Complexidade	De acordo com os requisitos definidos em **Como definir uma senha segura**.	1. Abra **Control Panel**. 2. Clique em **Administrative Tools**. Abra **Local Security Policy**. 3. Escolha **Account Policies** > **Password Policy**. 4. Ative a política **Password must meet complexity requirements**.
Duração máxima da senha	No modo de autenticação de senha estática, forçar os usuários a alterar suas senhas a cada 90 dias ou em intervalos mais curtos.	1. Abra **Control Panel**. 2. Clique em **Administrative Tools**. Abra **Local Security Policy**. 3. Escolha **Account Policies** > **Password Policy**. 4. Defina **Maximum password age** para 90 dias ou menos.
Política de bloqueio de conta	No modo de autenticação de senha estática, bloquear uma conta de usuário se a autenticação para o usuário falhar por 10 vezes consecutivas.	1. Abra **Control Panel**. 2. Clique em **Administrative Tools**. Abra **Local Security Policy**. 3. Escolha **Account Policies** > **Account Lockout Policy**. 4. Defina **Account lockout threshold** como **10** ou menor.

- **Fortalecimento da autorização**

Autorização	Descrição	Procedimento
Desligamentos remotos	Atribuir a permissão **Force shutdown from a remote system** somente ao grupo de **Administrators**.	1. Abra **Control Panel**. 2. Clique em **Administrative Tools**. Abra **Local Security Policy**. 3. Escolha **Local Policies** > **User Rights Assignment**. 4. Atribua a permissão **Force shutdown from a remote system** somente ao grupo de **Administrators**.

Autorização	Descrição	Procedimento
Desligamento local	Atribuir a permissão **Shut down the system** apenas ao grupo de **Administrators**.	1. Abra **Control Panel**. 2. Clique em **Administrative Tools**. Abra **Local Security Policy**. 3. Escolha **Local Policies** > **User Rights Assignment**. 4. Atribua a permissão **Shut down the system** apenas ao grupo de **Administrators**.
Atribuição de direitos de usuário	Atribuir a permissão **Take ownership of files or other objects** somente para o grupo de **Administrators**.	1. Abra **Control Panel**. 2. Clique em **Administrative Tools**. Abra **Local Security Policy**. 3. Escolha **Local Policies** > **User Rights Assignment**. 4. Atribua a permissão **Shut down the system** apenas ao grupo de **Administrators**.
Logon	Autorizar os usuários a fazer logon no computador localmente.	1. Abra **Control Panel**. 2. Clique em **Administrative Tools**. Abra **Local Security Policy**. 3. Escolha **Local Policies** > **User Rights Assignment**. 4. Atribua a permissão **Allow log on locally** aos usuários que você deseja autorizar.
Acesso a partir da rede	Permitir que apenas os usuários autorizados acedam a este computador a partir da rede (por exemplo, por meio de compartilhamento de rede). O acesso a partir de outros terminais não é permitido.	1. Abra **Control Panel**. 2. Clique em **Administrative Tools**. Abra **Local Security Policy**. 3. Escolha **Local Policies** > **User Rights Assignment**. 4. Atribua a permissão **Access this computer from the network** para os usuários que você deseja autorizar.

5.3 Por que um processo ainda é isolado depois de ser colocado na lista branca?

Depois de adicionar um processo à lista branca, ele não mais acionará certos alarmes, mas seu isolamento não será cancelado automaticamente.

Isolar e eliminar um programa malicioso

- Escolha **Installation & Configuration** e clique na guia **Security Configuration**. Clique na guia **Isolation and Killing of Malicious Programs** e habilite essa função.
- Escolha **Detection** > **Alarms**. Na área **Events**, isole e elimine manualmente os programas maliciosos.

Se um programa for isolado e eliminado, ele será encerrado imediatamente e não será mais capaz de executar operações de leitura ou gravação. Arquivos de origem isolados de programas ou processos são exibidos no painel deslizante **Isolated Files** e não podem prejudicar seus servidores.

Cancelamento do isolamento de arquivos

- Escolha **Detection** > **Events**. Na área **Alarm Statistics**, clique em **View Details** em **Isolated Files**, localize o servidor de destino e clique em **Restore** na coluna **Operation**.

Depois de cancelar o isolamento, as permissões de leitura/gravação dos arquivos serão restauradas, mas os processos encerrados não serão iniciados automaticamente.

5.4 O que devo fazer se um processo de mineração for detectado em um servidor?

Você é aconselhado a:

1. Fazer backup de dados e desativar portas desnecessárias.
2. Definir uma senha de servidor mais forte.
3. Ativar o HSS. Seus servidores estarão protegidos de processos de mineração por suas funções de detecção de intrusão, como prevenção de quebra de conta, detecção de logon remoto, detecção de programas maliciosos e detecção de web shell; bem como funções de eliminação de programas maliciosos e correção de vulnerabilidades.

5.5 Por que alguns ataques a servidores não são detectados?

- Não é possível detectar intrusões nos seus servidores antes de ativação do HSS.
- Se você comprou o HSS, lembre-se de ativá-lo para detectar intrusões.
- Os ataques à Web não podem ser detectados, pois o HSS defende principalmente seus servidores. Para proteger sites, você pode consultar o Arquiteto de soluções de segurança ou usar outros serviços seguros (como WAF e Anti-DDoS).

5.6 Posso desbloquear um endereço IP bloqueado pelo HSS e como?

Se você pode desbloquear um endereço IP depende do motivo pelo qual ele foi bloqueado. Um endereço IP será bloqueado se for considerado a fonte de um ataque de força bruta, listado na lista negra de IP comum ou não na lista branca de IP definida.

Verificar ataques de quebra de conta

- O HSS bloqueia o ataque a endereços IP para evitar invasões. A duração do bloqueio para ataques SSH suspeitos é de 12 horas e para outros ataques suspeitos é de 24 horas. Se um endereço IP bloqueado não executar ataques de força bruta na duração de bloqueio padrão, ele será desbloqueado automaticamente.
- Se você tiver certeza de que um endereço IP de origem pode ser confiável, poderá desbloqueá-lo manualmente. Escolha **Detection** > **Alarms**, clique em **View Details** em **Blocked IP Addresses** e desbloqueie o endereço IP no painel deslizante exibido.

  Se você desbloqueou manualmente um endereço IP, mas as tentativas incorretas de senha desse endereço IP excederem o limite novamente, esse endereço IP será bloqueado novamente.

Endereço IP na lista negra de IP comum

Você não pode desbloquear manualmente esses endereços IP.

Endereço IP não está na lista branca de IP de logon SSH

Se você configurou a **lista branca de IP de logon SSH**, os endereços IP que não estão na lista branca serão bloqueados. Para desbloquear um endereço IP, adicione-o à lista branca.

5.7 Por que um endereço IP bloqueado é desbloqueado automaticamente?

Se um endereço IP bloqueado não executar ataques de força bruta nas próximas 24 horas, o endereço IP será desbloqueado automaticamente.

5.8 Com que frequência o HSS detecta, isola e elimina programas maliciosos?

Período de detecção: detecção em tempo real

Período de isolamento e eliminação:

- Se você tiver ativado o isolamento e a eliminação automáticos, o sistema fará a verificação e eliminará os vírus em tempo real.
- Se você não tiver ativado o isolamento e eliminação automáticos, terá de verificar e lidar manualmente com os alarmes.

AVISO

1. O HSS pode detectar, isolar e eliminar programas maliciosos (por verificação na nuvem) e comportamentos anormais de processos. Para obter mais informações, consulte **Edições**.
2. O isolamento e a eliminação do HSS podem ser realizados de forma automática ou manual.
   - Para obter mais informações sobre isolamento e eliminação automáticos, consulte "Isolamento e eliminação de programas maliciosos" em **Configuração de segurança**.
   - Para obter mais informações sobre isolamento e eliminação manuais, consulte "Isolamento e eliminação de arquivos" em **Gerenciamento de arquivos isolados**.

5.9 O que devo fazer se um endereço IP for bloqueado pelo HSS?

Verifique se o endereço IP bloqueado é um endereço IP malicioso ou normal.

- Se for normal, **adicione-o à lista branca**.
- Se for malicioso, nenhuma outra operação será necessária.

5.10 Como me defender contra ataques de ransomware?

Geralmente, o ransomware é espalhado por meio de implementação de cavalo de Troia, e-mails, arquivos, vulnerabilidades, pacotes e mídia de armazenamento.

Para se defender contra invasões de ransomware, **evite ataques de força bruta** e lide com alarmes do HSS em tempo hábil.

5.11 O que devo fazer se o HSS (novo) não gerar alarmes após uma atualização do HSS (anterior)?

As funções de notificação de alarme das versões HSS (anterior) e HSS (novo) são separadas. A notificação de alarme do HSS (novo) é desativada por padrão e não herda as configurações do HSS (anterior). Portanto, o HSS (novo) não envia notificações de alarme. Você precisa ativar manualmente a notificação de alarme no console do HSS (novo). Para obter detalhes, consulte **Ativação de notificações de alarme**.

6 Logons anormais

6.1 Por que ainda recebo alarmes de logon remoto após configurar a lista branca de IP de logon?

Mesmo endereços IP na lista branca podem acionar certos alarmes. A lista branca de endereços IP de logon SSH, a lista branca de logon e as funções de logon remoto se concentram em diferentes aspectos de segurança, conforme descrito em **Tabela 6-1**.

Tabela 6-1 Funções

Função	Descrição	Como mascarar o alarme
Lista branca de endereços IP de logon SSH	Somente os endereços IP nesta lista branca podem efetuar logon nos servidores especificados via SSH. **AVISO** Para evitar problemas de conexão, certifique-se de que não tenha perdido os endereços IP necessários antes de ativar essa função.	-
Lista branca de logon	Para reduzir os falsos alarmes de ataque de força bruta, adicione endereços IP de logon confiáveis e seus endereços IP de servidor de destino a essa lista branca.	Escolha **Detection** > **Whitelists**. Clique na guia **Login Whitelist** e adicione endereços IP. O HSS não gerará alarmes de força bruta para esses endereços IP.
Logon remoto	Logons que não sejam de **Common Login Locations** e **Common Login IP Addresses** acionarão alarmes de logon remoto. Você será informado sobre novos endereços IP que fazem logon em seus servidores.	Escolha **Installation & Configuration** e clique em **Security Configuration**. Adicione informações de logon nas guias **Common Login Locations** e **Common Login IP Addresses**. Os logons na lista branca não acionarão mais alarmes remotos.

6.2 Como verificar o endereço IP do usuário de um logon remoto?

Políticas de alarme

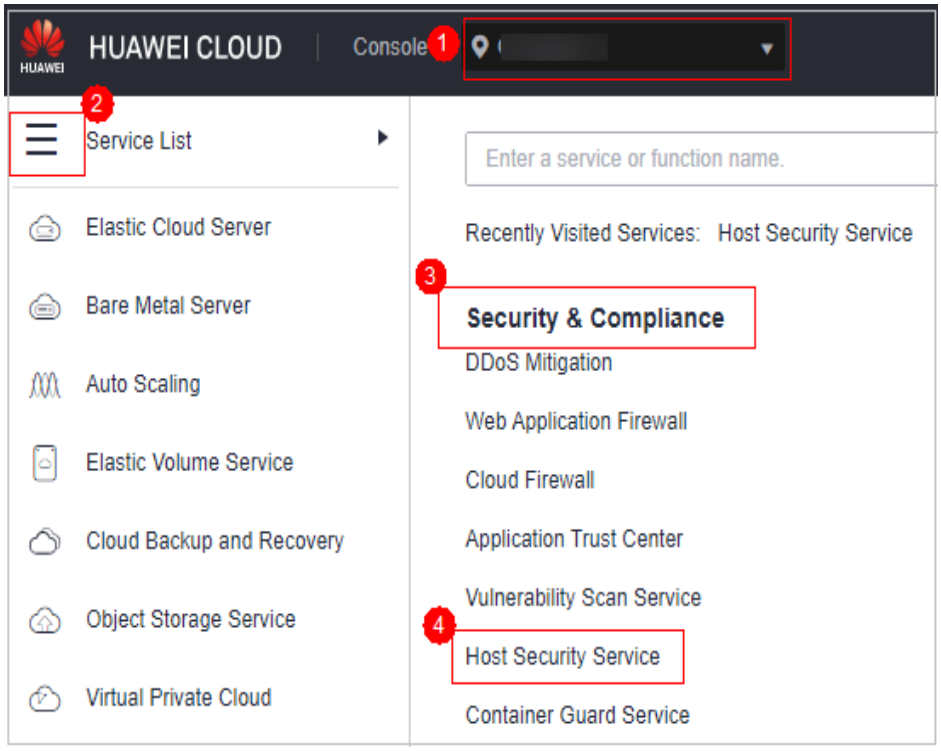
A função de detecção de logon remoto verifica logons remotos em seus servidores em tempo real. O HSS gera um alarme se detectar logons a partir de localizações diferentes das **localizações de logon comuns que definiu**.

Visualização de registros de logon remotos no console

Passo 1 **Faça logon no console de gerenciamento**.

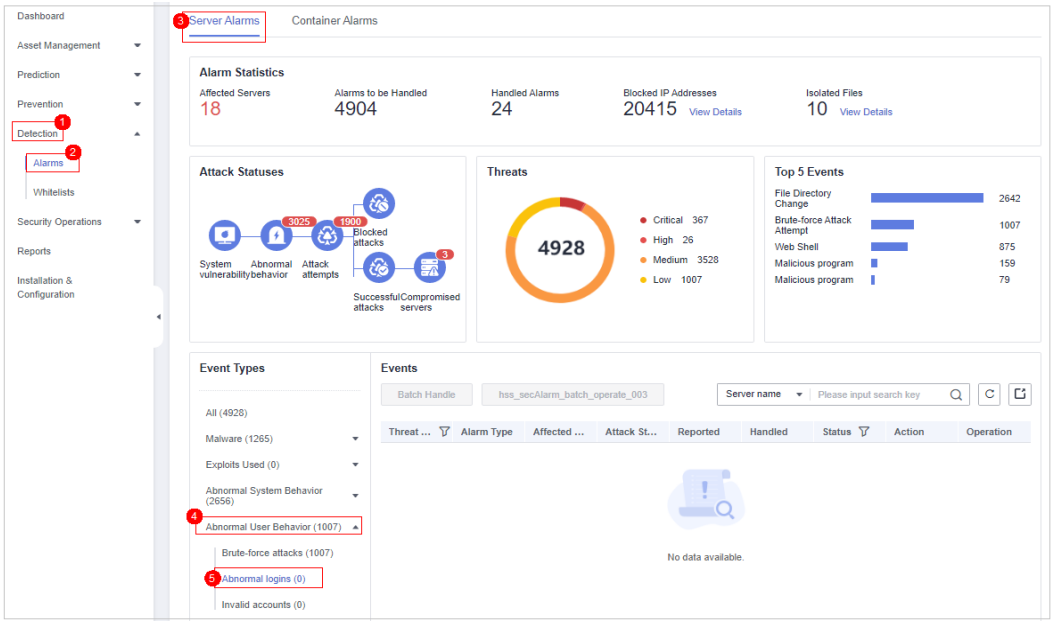
Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 6-1 Acessar o HSS



Passo 3 Como mostrado em **Figura 6-2**, verifique o **Abnormal logins**. Clique em **Remote Login** e clique no nome do alarme para ver os detalhes.

Figura 6-2 Logon anormal



----Fim

Visualizar localmente registros de logon remoto

Para servidores de Linux, você pode visualizar logs nos diretórios **/var/log/secure** e **/var/log/message** ou executar o comando **last** para verificar se há registros de logon anormais.

6.3 O que posso fazer se for relatado um alarme indicando logon bem-sucedido?

- Este alarme não indica necessariamente um problema de segurança. Se você selecionou **Successful Logins** na área **Real-Time Alarm Notifications**, o HSS enviará alarmes ao detectar logons bem-sucedidos.
- Se todas as contas em seus ECSs forem gerenciadas por um único administrador, esses alarmes o ajudarão a monitorar convenientemente as contas do sistema.
- Se as contas do sistema forem gerenciadas por vários administradores ou se servidores diferentes forem gerenciados por administradores diferentes, muitos alarmes interromperão o pessoal de O&M. Neste caso, é aconselhável desativar o item de alarme.
- Alarmes neste evento não indicam necessariamente ataques. Logons de endereços IP válidos não são ataques.

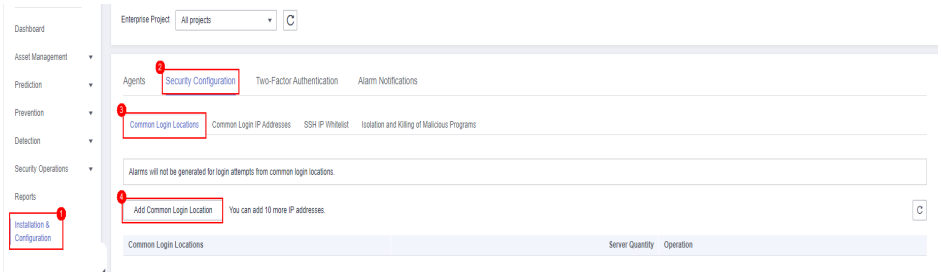
6.4 Posso desativar a detecção de logon remoto?

Não.

Se você não quiser receber notificações de alarme de logon remoto, adicione localizações com alarme como localizações de logon comuns ou desmarque o item de tentativa de logon remoto nas configurações de notificação de alarme.

- Na guia **Common Login Locations**, clique em **Add Common Login Location** e adicione localizações de logon comuns. O HSS não aciona alarmes de logon remotos em logons de localizações de logon comuns.

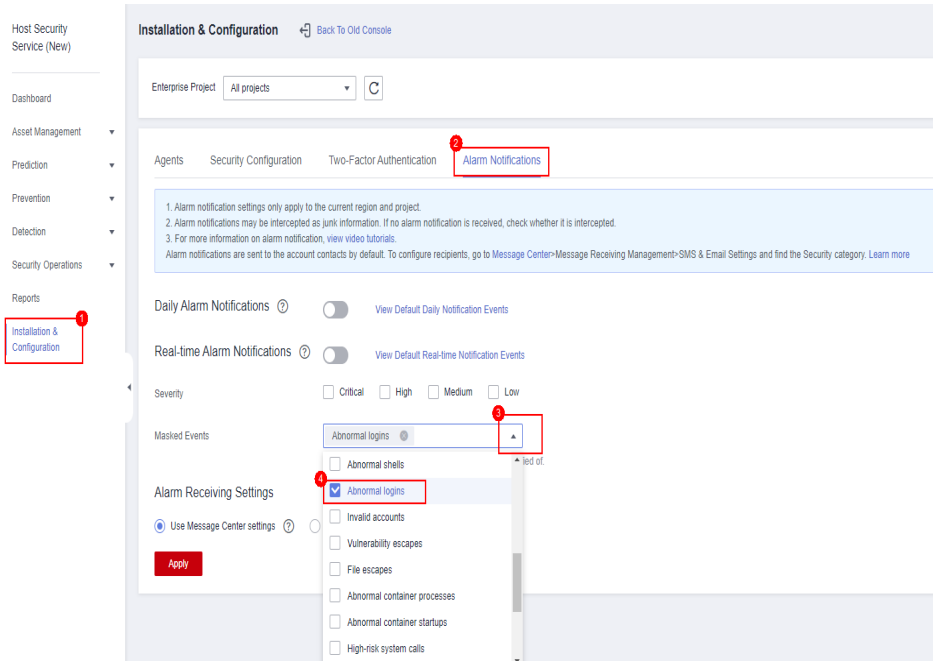
Figura 6-3 Adicionar uma localização de logon comum



- Escolha **Installation & Configuration** e clique em **Alarm Notifications**. Na caixa **Masked Events**, selecione **Abnormal logins**.

  Tenha cuidado ao desmarcar o item de notificação de **Abnormal Logins**. Logons anormais incluem logons remotos e hacks bem-sucedidos. Se você desmarcar este item, você não receberá alarmes sobre ataques de força bruta em tempo real.

Figura 6-4 Desmarcar logons anormais



6.5 Como saber se uma intrusão foi bem-sucedida?

- Se você ativou as notificações de alarme para detecção de intrusão, você será notificado imediatamente quando uma conta for quebrada ou puder ser quebrada.
- Você também pode verificar se os endereços IP de ataque estão bloqueados na página **Detection**.

- Para obter mais detalhes, visualize os logs em **/var/log/secure and /var/log/message** no servidor do Linux ou execute o comando **last** para verificar se há registros de logon anormais.

7 Configurações inseguras

7.1 Como instalar um PAM e definir uma política de complexidade de senha adequada em um sistema operacional Linux?

Instalação de um PAM

Sua política de complexidade de senha não poderá ser verificada se nenhum módulo de autenticação conectável (PAM) estiver em execução no seu sistema.

Para Debian ou Ubuntu, execute o comando **apt-get install libpam-cracklib** como administrador para instalar um PAM.

NOTA

Um PAM é instalado e executado por padrão no CentOS, Fedora e EulerOS.

Definir uma política de complexidade de senha

Uma política de complexidade de senha adequada seria: a senha deve conter pelo menos oito caracteres e deve conter letras maiúsculas, minúsculas, números e caracteres especiais.

NOTA

As configurações anteriores são requisitos básicos de segurança. Para obter mais configurações de segurança, execute os seguintes comandos para obter informações de ajuda em sistemas operacionais Linux:

- Para CentOS, Fedora e EulerOS baseados no Red Hat 7.0, execute:
  man pam_pwquality
- Para outros sistemas operacionais Linux, execute:
  man pam_cracklib

- CentOS, Fedora e EulerOS
  a. Execute o seguinte comando para editar o arquivo **/etc/pam.d/system-auth**:
     vi /etc/pam.d/system-auth

b. Encontre as seguintes informações no arquivo:

- Para CentOS, Fedora e EulerOS baseados no Red Hat 7.0:

  password requisite pam_pwquality.so try_first_pass retry=3 type=

- Para outros sistemas de CentOS, Fedora e EulerOS:

  password requisite pam_cracklib.so try_first_pass retry=3 type=

c. Adicione os seguintes parâmetros e seus valores: **minlen**, **dcredit**, **ucredit**, **lcredit** e **ocredit**. Se o arquivo já tiver esses parâmetros, altere seus valores. Para mais detalhes, consulte **Tabela 7-1**.

Exemplo:

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

NOTA

Defina **dcredit**, **ucredit**, **lcredit** e **ocredit** como números negativos.

Tabela 7-1 Descrição do parâmetro

Parâmetro	Descrição	Exemplo
minlen	Comprimento mínimo de uma senha. Por exemplo, se você quiser que o comprimento mínimo seja oito, defina o valor **minlen** como 8.	minlen=8
dcredit	Número de dígitos Um valor negativo (por exemplo, **-N**) indica o número (por exemplo, N) de dígitos necessários em uma senha. Um valor positivo indica que não há limite.	dcredit=-1
ucredit	Número de letras maiúsculas Um valor negativo (por exemplo, **-N**) indica o número (por exemplo, N) de letras maiúsculas necessárias em uma senha. Um valor positivo indica que não há limite.	ucredit=-1
lcredit	Número de letras minúsculas Um valor negativo (por exemplo, **-N**) indica o número (por exemplo, N) de letras minúsculas necessárias em uma senha. Um valor positivo indica que não há limite.	lcredit=-1
ocredit	Número de caracteres especiais Um valor negativo (por exemplo, **-N**) indica o número (por exemplo, N) de caracteres especiais necessários em uma senha. Um valor positivo indica que não há limite.	ocredit=-1

- Debian e Ubuntu

  a. Execute o seguinte comando para editar o arquivo **/etc/pam.d/common-password**:

  vi /etc/pam.d/common-password

  b. Encontre as seguintes informações no arquivo:

  password requisite pam_cracklib.so retry=3 minlen=8 difok=3

  c. Adicione os seguintes parâmetros e seus valores: **minlen**, **dcredit**, **ucredit**, **lcredit** e **ocredit**. Se o arquivo já tiver esses parâmetros, altere seus valores. Para mais detalhes, consulte **Tabela 7-1**.

  Exemplo:

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

7.2 Como definir uma política de complexidade de senha adequada em um sistema operacional Windows?

Uma política de complexidade de senha adequada seria: oito caracteres para o comprimento de uma senha e pelo menos três tipos dos seguintes caracteres usados: letras maiúsculas, letras minúsculas, dígitos e caracteres especiais.

Execute as seguintes etapas para definir uma política de segurança local:

Passo 1 Faça logon no sistema operacional como o usuário **Administrator**. Escolha **Start** > **Control Panel** > **System and Security** > **Administrative Tools**. Na pasta **Administrative Tools**, clique duas vezes em **Local Security Policy**.

NOTA

Como alternativa, clique em **Start** e digite **secpol.msc** na caixa **Search programs and files**.

Passo 2 Escolha **Account Policies** > **Password Policy** e execute as seguintes operações.

- Clique duas vezes em **Password must meet complexity requirements**, selecione **Enable** e clique em **OK** para habilitar a política.
- Clique duas vezes em **Minimum password length**, digite o comprimento (maior ou igual a **8**) e clique em **OK** para definir a política.

Passo 3 Execute o comando **gpupdate** para atualizar as configurações do sistema. Depois que a atualização for bem-sucedida, as configurações entrarão em vigor no sistema.

----Fim

7.3 Como lidar com configurações inseguras?

O HSS executa automaticamente uma detecção de configuração para servidores. Você pode reparar itens de configuração inseguros ou ignorar os itens de configuração em que confia com base no resultado da detecção.

- Modificação de itens de configuração inseguros

Visualize detalhes sobre uma regra de detecção, verifique o resultado da detecção com base na descrição da auditoria e trate a exceção com base na recomendação de modificação.

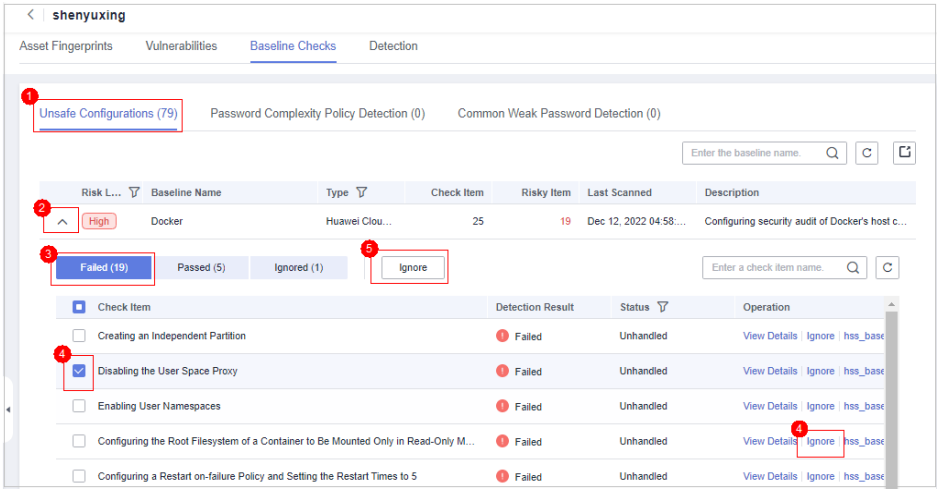
É aconselhável reparar as configurações com um alto nível de ameaça imediatamente. As configurações com um nível de ameaça médio ou baixo podem ser corrigidas posteriormente com base nos requisitos de serviço.

- Ignorar itens de configuração confiáveis

  a. Clique no nome de um ECS para exibir seus detalhes. Escolha **Baseline Checks** > **Unsafe Configurations**.

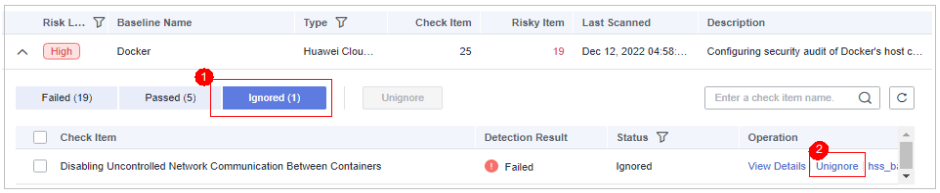
  b. Localize o item de risco de destino, clique em na frente de seu nome para expandir os itens de verificação e clique em **Ignore** na coluna **Operation**. Você também pode selecionar várias regras de detecção e clicar em **Ignore** na parte superior da página para ignorá-las em lotes.

Figura 7-1 Ignorar uma configuração arriscada



Para cancelar ignorar uma regra de detecção ignorada, clique em **Unignore** na coluna **Operation**. Você também pode selecionar várias regras de detecção ignoradas e clicar em **Unignore** na parte superior da página para cancelar ignorá-las em lotes.

Figura 7-2 Cancelamento de ignorar programas maliciosos



- Verificação

  Após modificar os itens de configuração, é aconselhável escolher **Prediction** > **Vulnerabilities** e clicar em **Scan** para executar a verificação manual imediatamente para verificar o resultado.

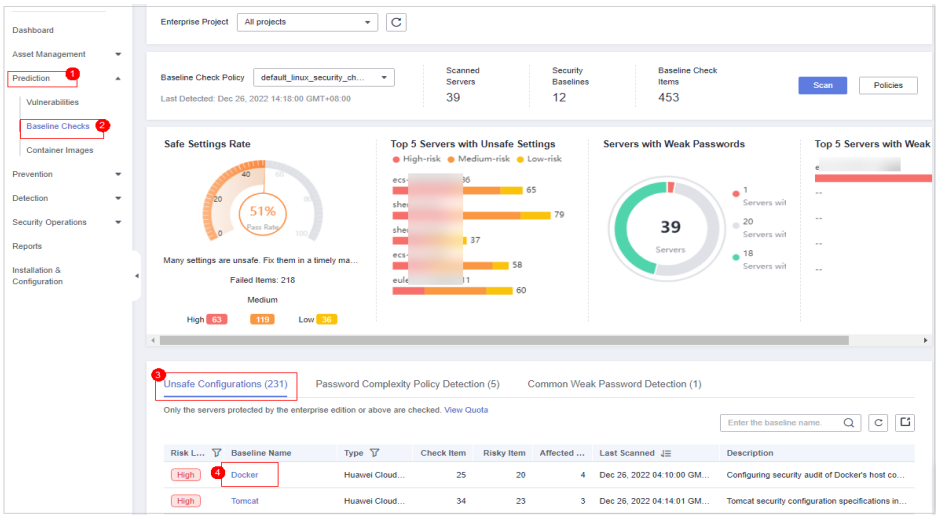
7.4 Como exibir relatórios de verificação de configuração?

Você pode exibir os detalhes da verificação de configuração on-line.

Procedimento

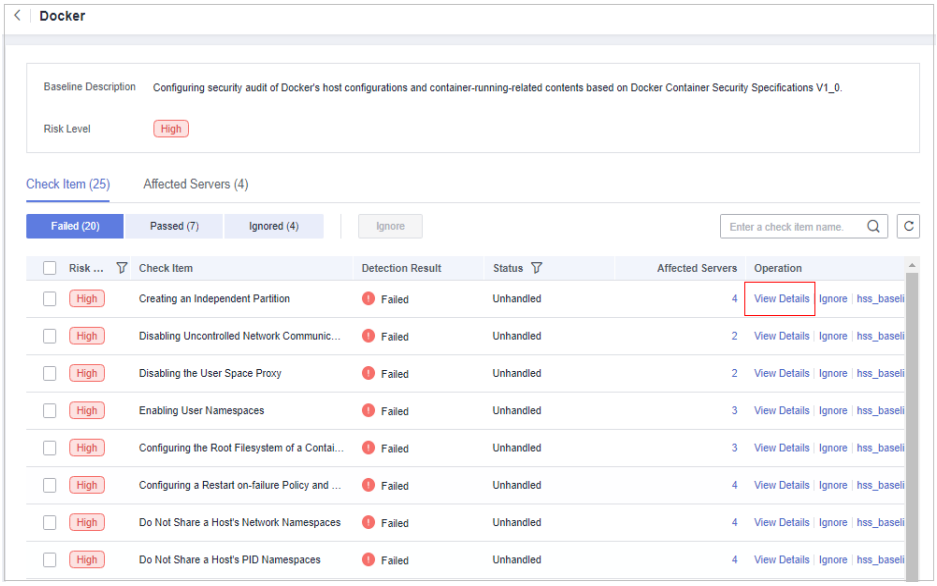
Passo 1 Na página de verificação de configuração, clique em um nome de linha de base de verificação de configuração.

Figura 7-3 Escolher um item de verificação



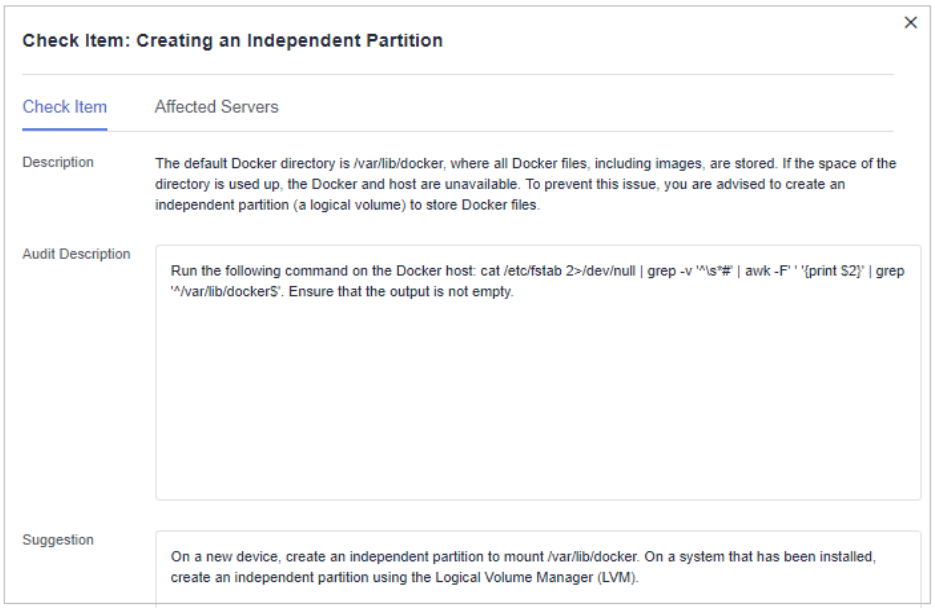
Passo 2 Na página de detalhes da regra de detecção, clique em **View Details**.

Figura 7-4 Detalhes da detecção



Passo 3 Você pode retificar itens de configuração inseguros e ignorar itens de configuração confiáveis com base nas sugestões fornecidas.

Figura 7-5 Configuração do relatório de detecção



----Fim

8 Gerenciamento de vulnerabilidades

8.1 Como corrigir vulnerabilidades?

Procedimento

Passo 1 **Verifique os resultados da detecção de vulnerabilidades**.

Passo 2 Com base nas soluções fornecidas, **corrija as vulnerabilidades** uma por uma em ordem decrescente por gravidade.

- Reinicie o SO Windows depois de corrigir suas vulnerabilidades.
- Reinicie o SO Linux depois de corrigir suas vulnerabilidades do kernel.

Passo 3 O HSS verifica todos os servidores do Linux, servidores do Windows e servidores Web-CMS em busca de vulnerabilidades todas as manhãs. Depois de corrigir as vulnerabilidades, é aconselhável executar uma verificação imediatamente para verificar o resultado.

----Fim

8.2 O que devo fazer se um alarme ainda existir depois que eu corrigir uma vulnerabilidade?

Execute as seguintes operações para localizar a causa e corrigir os problemas.

NOTA

Para obter detalhes sobre como corrigir vulnerabilidades, consulte **Correção de vulnerabilidades e verificação do resultado**.

Possíveis causas e soluções em um servidor do Linux

- Não foram configuradas as fontes do yum.

  Neste caso, configure uma fonte do yum adequada para o seu SO Linux e corrija a vulnerabilidade novamente.
- A fonte do yum não tem o pacote de atualização mais recente do software correspondente.

Mude para a fonte do yum que tem o pacote necessário e corrija a vulnerabilidade novamente.

- O ambiente de intranet não pode se conectar à Internet.

  Os servidores precisam acessar a Internet e usar fontes do yum externas para corrigir vulnerabilidades. Se seus servidores não puderem acessar a Internet ou as fontes de imagem externas não puderem fornecer serviços estáveis, você poderá usar a fonte da imagem.

- A versão anterior do kernel permanece.

  Versões anteriores do kernel geralmente permanecem nos servidores após a atualização. Você pode executar os **comandos de verificação** para verificar se a versão atual do kernel atende aos requisitos de correção de vulnerabilidade. Se isso acontecer, ignore a vulnerabilidade na guia **Linux Vulnerabilities** da página **Vulnerabilities**. Você não é aconselhado a excluir o kernel anterior.

Tabela 8-1 Comandos de verificação

SO	Comando de verificação
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 que um servidor exibido em informações de vulnerabilidade não existe?

Vulnerabilidades detectadas nas últimas 24 horas são exibidas. O nome do servidor em uma notificação de vulnerabilidade é o nome usado quando a vulnerabilidade foi detectada e pode ser diferente do nome do servidor mais recente.

8.4 Preciso reiniciar um servidor depois de corrigir suas vulnerabilidades?

Depois de corrigir as vulnerabilidades do SO Windows ou do kernel Linux, você precisa reiniciar os servidores para que a correção entre em vigor, ou o HSS continuará a avisá-lo sobre essas vulnerabilidades. Para outros tipos de vulnerabilidades, não é necessário reiniciar os servidores depois de corrigi-las.

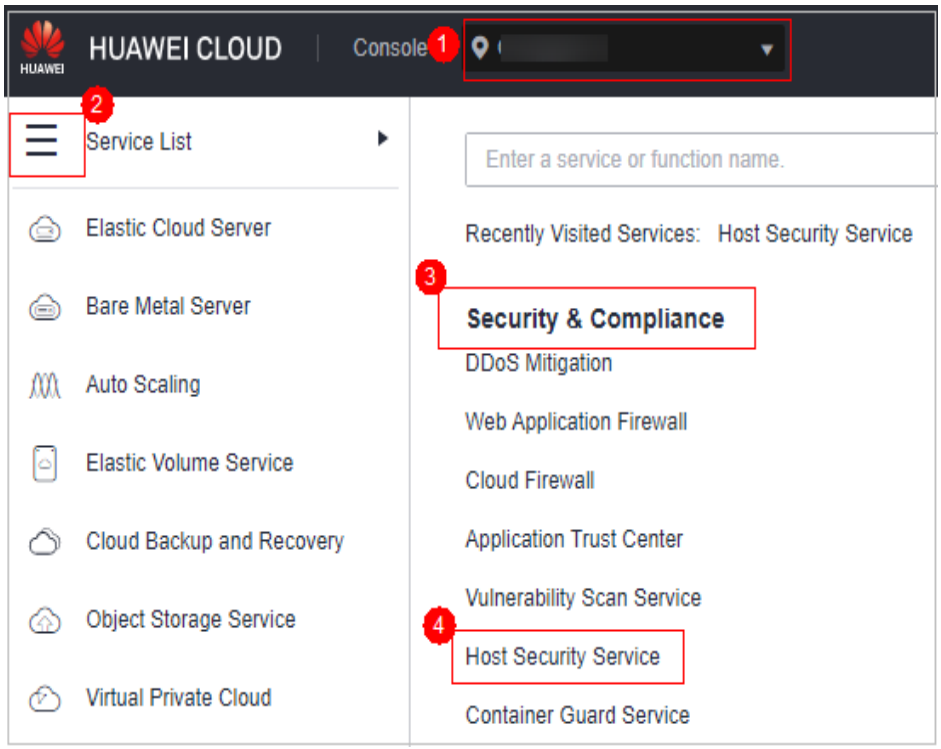
8.5 Posso verificar a vulnerabilidade e o histórico de correção de linha de base no HSS?

Visualização de vulnerabilidades corrigidas

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 8-1 Acessar o HSS

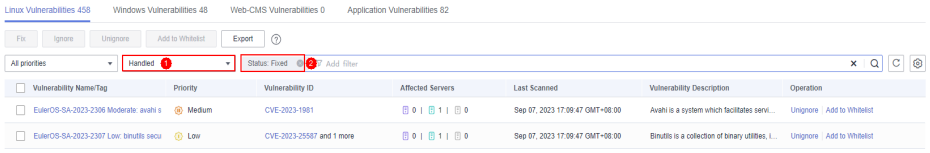


Passo 3 No painel de navegação, escolha **Prediction** > **Vulnerabilities**.

Passo 4 Nas guias de vulnerabilidades, filtre e visualize as vulnerabilidades corrigidas.

AVISO

As vulnerabilidades são apresentadas na lista de vulnerabilidades apenas durante sete dias. Você só pode verificar as vulnerabilidades que foram corrigidas nos últimos sete dias.



----Fim

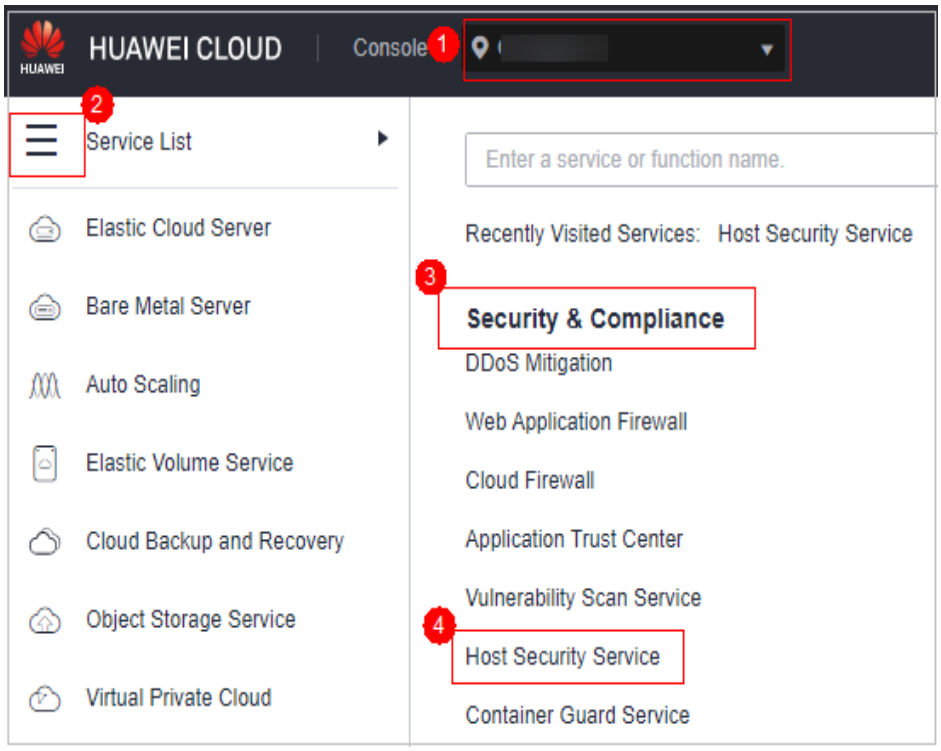
Visualização de problemas de linha de base corrigidos

O histórico de correção não mostra as configurações de política de complexidade de senha ou senhas fracas comuns que foram corrigidas. Para verificar outros itens de configuração corrigidos, execute as seguintes etapas:

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 8-2 Acessar o HSS



Passo 3 No painel de navegação, escolha **Prediction** > **Baseline Checks**.

Passo 4 Clique na guia **Unsafe Configurations**.

Passo 5 Clique em um nome de linha de base para ir para a página de detalhes.

Passo 6 Na guia **Check Items**, visualize os itens de verificação no estado **Passed**.

----Fim

8.6 O que devo fazer se a correção da vulnerabilidade falhar?

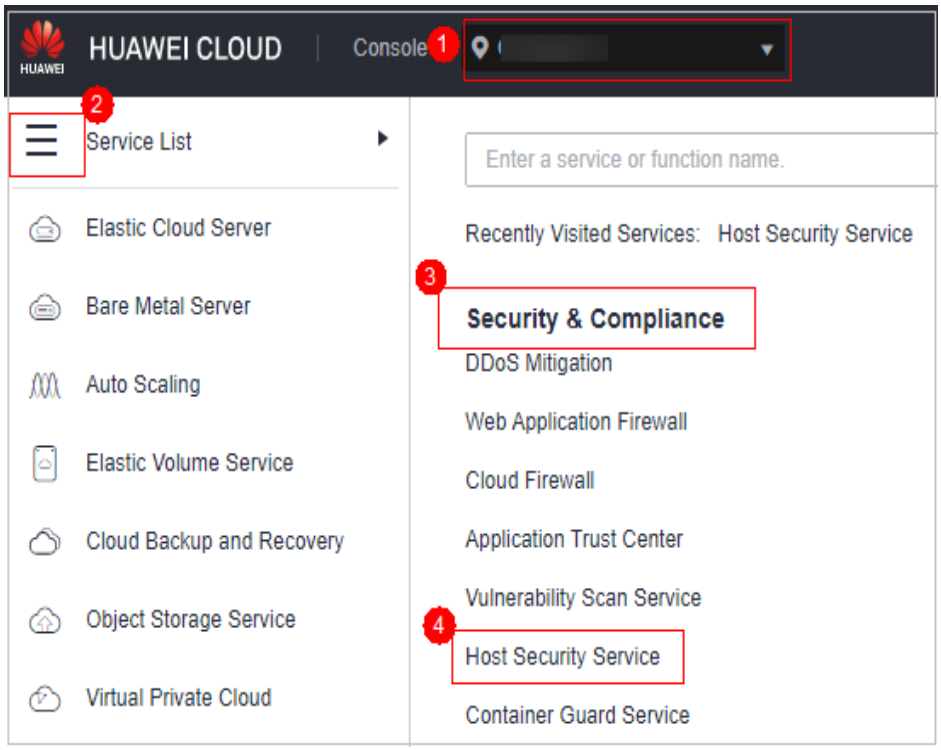
Se as vulnerabilidades do Linux ou do Windows não tiverem sido corrigidas no console do HSS, corrija a falha seguindo as instruções fornecidas nesta seção.

Visualização da causa de uma falha na correção de vulnerabilidades

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 8-3 Acessar o HSS



Passo 3 No painel de navegação, escolha **Prediction** > **Vulnerabilities**.

NOTA

If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Passo 4 No canto superior direito da página **Vulnerabilities**, clique em **Manage Task**.

Passo 5 Clique na guia **Fix Tasks** para visualizar os resultados de correção da vulnerabilidade.

- : o número exibido ao lado desse ícone indica o número de servidores que foram corrigidos com sucesso.
- : o número exibido ao lado desse ícone indica o número de servidores que não foram corrigidos.

Passo 6 Clique em . Na caixa de diálogo **Fix Failures**, visualize a causa e a descrição da falha.

Você pode lidar com a vulnerabilidade corrigindo falhas com base nas causas da falha. Para mais detalhes, consulte **Causas e soluções de falhas na correção de vulnerabilidades do Linux** e **Causas e soluções de falha de correção de vulnerabilidades do Windows**.

----Fim

Causas e soluções de falhas na correção de vulnerabilidades do Linux

AVISO

- As vulnerabilidades do kernel nos servidores do CCE, MRS e BMS não podem ser corrigidas. Corrigi-las pode tornar algumas funções indisponíveis.
- As causas de falha a seguir contêm apenas alguns campos-chave. Para obter detalhes, consulte as informações exibidas no console do HSS.

Causa da falha	Descrição	Solução
timeout	O tempo de reparo expirou.	Aguarde 1 hora e tente corrigir a vulnerabilidade novamente. Se a falha persistir, escolha **Service Tickets** > **Create Service Ticket** no canto superior direito do console de gerenciamento da Huawei Cloud para entrar em contato com o suporte técnico.
This agent version does not support vulnerability verification	A versão do agente é muito antiga.	**Atualize o agente** e tente corrigir a vulnerabilidade novamente.
Agent status is not normal	O status do agente é anormal.	O agente está off-line e a vulnerabilidade não pode ser corrigida. Recupere o status do agente consultando **Como corrigir um agente anormal?** e corrija a vulnerabilidade.

Causa da falha	Descrição	Solução

Error: software have multiple versions	Uma versão de software com vulnerabilidades não é excluída.	● Se esse problema ocorrer em softwares comuns, exclua os pacotes das versões anteriores e verifique se o problema persiste.
		Execute o seguinte comando para verificar se um erro é relatado quando um pacote de versão anterior é excluído:
		`rpm -e --test XXX`
		NOTA
		XXX indica o nome completo do componente de software, que contém o número da versão. Você pode executar o comando **rpm -qa** para consultar o nome completo do componente.
		– Se um erro for relatado durante a exclusão, há dependências no pacote de software e o pacote não pode ser excluído. É aconselhável ignorar esta vulnerabilidade.
		– Se nenhum erro for relatado durante a exclusão, execute o seguinte comando para excluir o pacote de versão anterior:
		`rpm -e XXX`
		● Se esse problema ocorrer em componentes relacionados ao kernel, como Kernel e Glibc, excluir o pacote da versão anterior pode causar problemas no SO. Nesse caso, é aconselhável ignorar essa vulnerabilidade.

<table>
<tr><th>Causa da falha</th><th>Descrição</th><th>Solução</th></tr>
<tr><td>No package marked for update
Error: software info not update
Error: kernel is not update
is already the newest version
Dependencies resolved. Nothing to do. Complete!</td><td>O pacote de atualização de uma versão posterior não foi encontrado.</td><td>A causa da falha indica que o software foi atualizado para a versão mais recente suportada pela fonte de imagem atual, mas a vulnerabilidade ainda existe.
NOTA
• CentOS 6 e CentOS 8 estão oficialmente em fim de vida (EOL) e não são mais mantidos. O HSS verifica-os em busca de vulnerabilidades com base nos avisos de patch de Red Hat, mas não pode corrigi-los devido à falta de patches oficiais. Você é aconselhado a mudar para outros SOs.
• O Ubuntu 18.04 e versões anteriores não suportam atualizações de patch gratuitas. Você precisa comprar e configurar o Ubuntu Pro para instalar pacotes de atualização.
• Possível causa 1: a fonte da imagem está configurada incorretamente.
Atualize a fonte da imagem e corrija a vulnerabilidade novamente. Para obter mais informações, consulte Configuração da fonte de imagem.
• Possível causa 2: as vulnerabilidades do kernel não podem ser corrigidas no servidor.
Corrigir vulnerabilidades do kernel pode tornar algumas funções indisponíveis. Para corrigir uma vulnerabilidade do kernel, escolha Service Tickets > Create Service Ticket no canto superior direito do console de gerenciamento da Huawei Cloud para entrar em contato com o suporte técnico.
AVISO
As vulnerabilidades do kernel nos servidores do CCE, MRS e BMS não podem ser corrigidas. Corrigi-las pode tornar algumas funções indisponíveis. Não atualize componentes do kernel.</td></tr>
</table>

Causa da falha	Descrição	Solução
Error: Failed to download metadata for repo One of the configured repositories failed Errors during downloading metadata for repository Error: Cannot retrieve repository metadata Failed connect to E: Failed to fetch	Falha ao conectar-se à fonte do yum.	Verifique se o servidor está em uma das seguintes regiões: CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou ou CN-Hong Kong. ● Se o servidor estiver em uma dessas regiões e não puder se conectar à Internet por algum motivo, configure a fonte da imagem fornecida pela Huawei Cloud. Para obter detalhes, consulte **Como usar uma ferramenta automatizada para configurar uma fonte de imagem da Huawei Cloud?** ● Se o servidor não estiver em nenhuma dessas regiões, verifique se o servidor pode acessar a Internet. Caso contrário, o servidor não poderá se conectar à fonte oficial da imagem ou a outras fontes.
Error: kernel is not update Error: kernel info not update	Kernel não atualizado.	● Possível causa 1: o servidor não é reiniciado após a correção da vulnerabilidade. Solução: reinicie o servidor. Depois que uma vulnerabilidade do kernel for corrigida, você precisará reiniciar o servidor para que a correção entre em vigor. Caso contrário, o sistema ainda relatará a vulnerabilidade na próxima verificação. ● Possível causa 2: as vulnerabilidades do kernel não podem ser corrigidas no servidor. Corrigir vulnerabilidades do kernel pode tornar algumas funções indisponíveis. Para corrigir uma vulnerabilidade do kernel, escolha **Service Tickets** > **Create Service Ticket** no canto superior direito do console de gerenciamento da Huawei Cloud para entrar em contato com o suporte técnico.
Please install a package which provides this module, or verify that the module is installed correctly command not found	O comando yum não está disponível.	Corrija o problema de indisponibilidade do comando com base nas sugestões fornecidas na causa da falha.

Causa da falha	Descrição	Solução
Error downloading packages	O pacote de atualização falha ao ser baixado.	Verifique se o servidor pode se conectar corretamente à Internet. ● Se sim, a fonte da imagem está configurada incorretamente. Atualize a fonte da imagem e corrija a vulnerabilidade novamente. Para obter mais informações, consulte **Configuração da fonte de imagem**. ● Se não, certifique-se de que seu servidor possa se conectar à Internet e corrija a vulnerabilidade novamente.
There are no enabled repositories Error: Cannot find a valid baseurl for repo There are no enabled repos	Nenhuma fonte disponível configurada.	Essa falha ocorre porque a fonte da imagem está configurada incorretamente. Atualize a fonte da imagem e corrija a vulnerabilidade novamente. Para obter mais informações, consulte **Configuração da fonte de imagem**.
dpkg was interrupted	O comando dpkg não está disponível.	Corrija o problema de indisponibilidade do comando com base nas sugestões fornecidas na causa da falha.

Causas e soluções de falha de correção de vulnerabilidades do Windows

AVISO

- Após a instalação de um patch do Windows, será necessário reiniciar o servidor ou os seguintes problemas poderão ocorrer:
  - O patch não faz efeito.
  - Quando você instala outros patches ou software do sistema, pode ocorrer a tela azul da morte (BSOD) ou falha na inicialização.
- As causas de falha a seguir contêm apenas alguns campos-chave. Para obter detalhes, consulte as informações exibidas no console do HSS.

Causa da falha	Descrição	Solução
timeout	O tempo de reparo expirou.	Aguarde 1 hora e tente corrigir a vulnerabilidade novamente. Se a falha persistir, escolha **Service Tickets** > **Create Service Ticket** no canto superior direito do console de gerenciamento da Huawei Cloud para entrar em contato com o suporte técnico.

Causa da falha	Descrição	Solução
Agent status is not normal	O status do agente é anormal.	O agente está off-line e a vulnerabilidade não pode ser corrigida. Recupere o status do agente consultando **Como corrigir um agente anormal?** e corrija a vulnerabilidade.
This agent version does not support vulnerability verification	A versão do agente é muito antiga.	**Atualize o agente** e tente corrigir a vulnerabilidade novamente.

Search patch failed: Search failed, errmsg(Unknown error 0x8024401C)	Falha ao encontrar o patch.	A falha ocorre porque o componente Windows Update no servidor está com defeito. Execute as seguintes operações para recuperar o componente Windows Update e corrigir a vulnerabilidade novamente:
		1. Abra a interface de linha de comando (CLI).
		2. Execute os seguintes comandos um por um:
		`net stop wuauserv`
		`reg delete HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate`
		`net start wuauserv`

Causa da falha	Descrição	Solução

Search patch failed: Search failed, errmsg(Unknown error 0x8024402C)	Falha ao encontrar o patch.	A falha ocorre porque o cliente do Windows Update não pode se conectar ao servidor do Windows Update. Execute as seguintes operações para recuperar o componente Windows Update e corrigir a vulnerabilidade novamente:
		1. Verifique se a conexão de rede do servidor está normal.
		Certifique-se de que seu servidor possa se conectar à Internet.
		2. Limpe o cache do Windows Update.
		a. Abra **Control Panel**.
		b. Clique em **System and Security**. Em **Administrative Tools**, clique em **Services**.
		c. Clique com o botão direito do mouse em **Windows Update** e escolha **Stop**.
		d. Abra a pasta **C:\Windows**. Exclua o arquivo **SoftwareDistribution**.
		e. Clique com o botão direito do mouse no serviço **Windows Update** e escolha **Start**.
		3. Execute os seguintes comandos para redefinir o componente Windows Update:
		`net stop wuauserv`
		`net stop cryptSvc`
		`net stop bits`
		`net stop msiserver`
		`ren C:\Windows\SoftwareDistribution SoftwareDistribution.old`
		`ren C:\Windows\System32\catroot2 catroot2.old`
		`net start wuauserv`
		`net start cryptSvc`
		`net start bits`
		`net start msiserver`

Search patch failed: Search failed, errmsg(Unknown error 0x80070422)	Falha ao encontrar o patch.	A falha ocorre porque o Windows Update está desativado no servidor. Execute as seguintes operações para iniciar o serviço e corrigir a vulnerabilidade novamente: 1. Abra **Control Panel**. 2. Clique em **System and Security**. Em **Administrative Tools**, clique em **Services**. 3. Clique duas vezes no serviço **Windows Update**. 4. Na janela **Windows Update Properties**, defina **Startup type** como **Automatic**. 5. Clique em **OK**.

<table>
<tr><th>Causa da falha</th><th>Descrição</th><th>Solução</th></tr>
<tr><td>Search patch failed: Get updates count is 0</td><td>Falha ao encontrar o patch.</td><td rowspan="7">A falha ocorre porque o Windows Update do servidor está com defeito. Execute as seguintes etapas para localizar a falha:
1. Verifique se a conexão de rede do servidor está normal.
● Se sim, vá para 2.
● Se não, corrija a vulnerabilidade novamente depois que a conexão de rede do servidor se tornar normal.
2. Abra o Windows Update e verifique se o patch a ser instalado está disponível.
● Se sim, instale o patch e reinicie o servidor.
● Se não, verifique se a causa da falha contém um código de erro.
Se contiver um código de erro, procure a solução correspondente no site oficial de Microsoft com base no código de erro.
Se ela não contiver nenhum código de erro, redefina o Windows Update consultando a documentação oficial de Microsoft.</td></tr>
<tr><td>Search patch failed: Search failed,errmsg</td><td>Falha ao encontrar o patch.</td></tr>
<tr><td>Not install security patch</td><td>Falha ao encontrar o patch.</td></tr>
<tr><td>Add patch to update collection failed: Update collection conut is 0</td><td>Falha ao encontrar o patch.</td></tr>
<tr><td>Not find patch</td><td>Nenhum patch encontrado.</td></tr>
<tr><td>Add patch to update collection failed</td><td>Falha ao instalar o patch.</td></tr>
<tr><td>Com init failed</td><td>Falha ao chamar o Windows Update.</td></tr>
</table>

Causa da falha	Descrição	Solução
Download patch failed	Falha ao baixar o patch.	● Possível causa 1: a configuração do Windows Update está incorreta. Esse problema pode ocorrer somente no Windows 2008 e 2012. Abra **Control Panel**. Clique em **Windows Update** e clique em **Change settings**. Configure os seguintes parâmetros: – **Important updates**: selecione **Download updates but let me choose when to install them**. – **Recommended update**: selecione esta caixa de seleção. – **Microsoft Update**: desmarque esta caixa de seleção. Após a conclusão da configuração, abra o Windows Update e clique em **Check for Update**. Depois que os patches a serem instalados forem encontrados, instale-os e reinicie o servidor. ● Possível causa 2: o servidor não foi corrigido por um longo tempo. Como resultado, o Windows Update está anormal. 1. Faça logon no servidor e abra o Windows Update. 2. Clique em **Check for Update**. 3. Depois que os patches a serem instalados forem encontrados, instale-os e reinicie o servidor. **NOTA** Alguns patches provavelmente não podem ser instalados por vez. Verifique se há atualizações após cada instalação de patch até que todos os patches sejam instalados.

8.7 Por que não consigo selecionar um servidor durante a verificação manual de vulnerabilidades?

Possíveis causas

Os seguintes servidores não podem ser selecionados para uma verificação manual de vulnerabilidades:

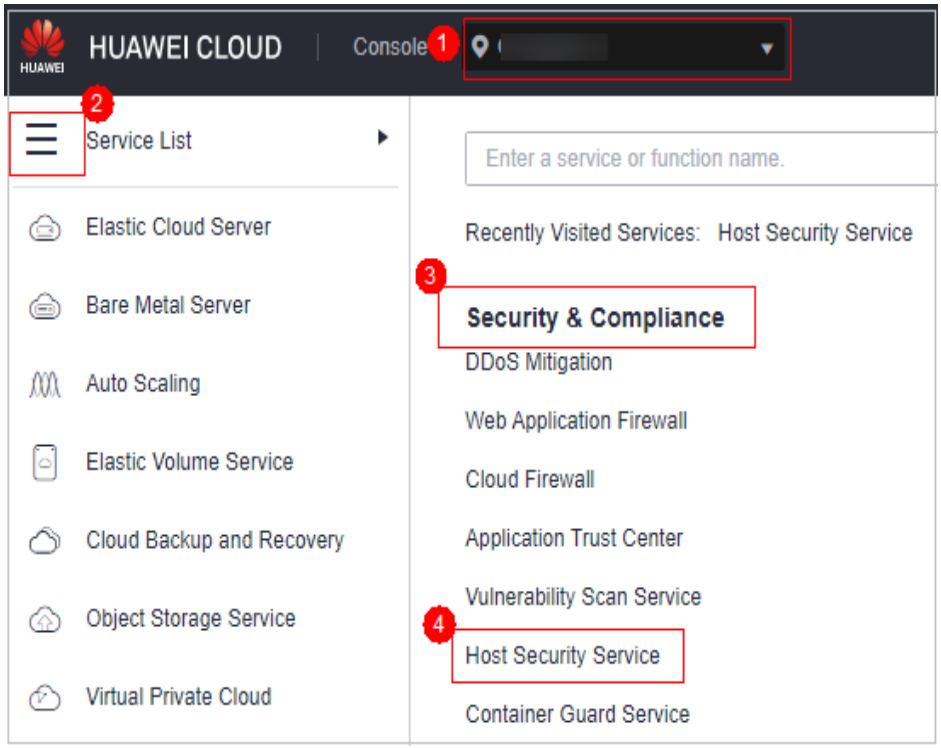
- Servidores que usam a edição básica do HSS
- Servidores que não estão no estado **Running**
- Servidores cujo status de agente está **Offline**

Solução

Passo 1 **Faça logon no console de gerenciamento**.

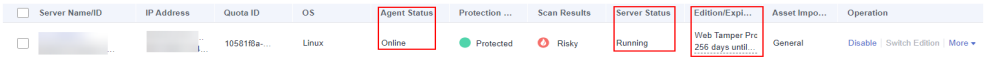
Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 8-4 Acessar o HSS



Passo 3 No painel de navegação, escolha **Asset Management** > **Servers & Quota**.

Passo 4 Na guia **Servers**, visualize o status de execução do servidor, o status do agente e a versão do HSS.



Corrija o problema com base nas condições do servidor.

- Servidores que usam a edição básica do HSS

  A edição básica do HSS não oferece suporte à verificação manual de vulnerabilidades. Para usar esse recurso, atualize a edição do HSS. Para obter detalhes, consulte **Atualização de sua edição**.

- Servidores que não estão no estado **Running**

  Verifique o servidor e verifique se o status do servidor está **Running**.

- Servidores cujo status de agente está **Offline**

  Um agente off-line não pode receber instruções entregues pelo console. Para colocar o agente novamente on-line, execute as operações descritas em **Como corrigir um agente anormal?**

Passo 5 No painel de navegação, escolha **Prediction** > **Vulnerabilities**. Inicie uma verificação manual novamente. Se o servidor de destino puder ser selecionado, o problema foi corrigido.

----Fim

9 Proteção contra adulteração na Web

9.1 Por que preciso adicionar um diretório protegido?

A WTP protege arquivos em diretórios. Se nenhum diretório for especificado, a WTP não poderá ter efeito mesmo que esteja ativada.

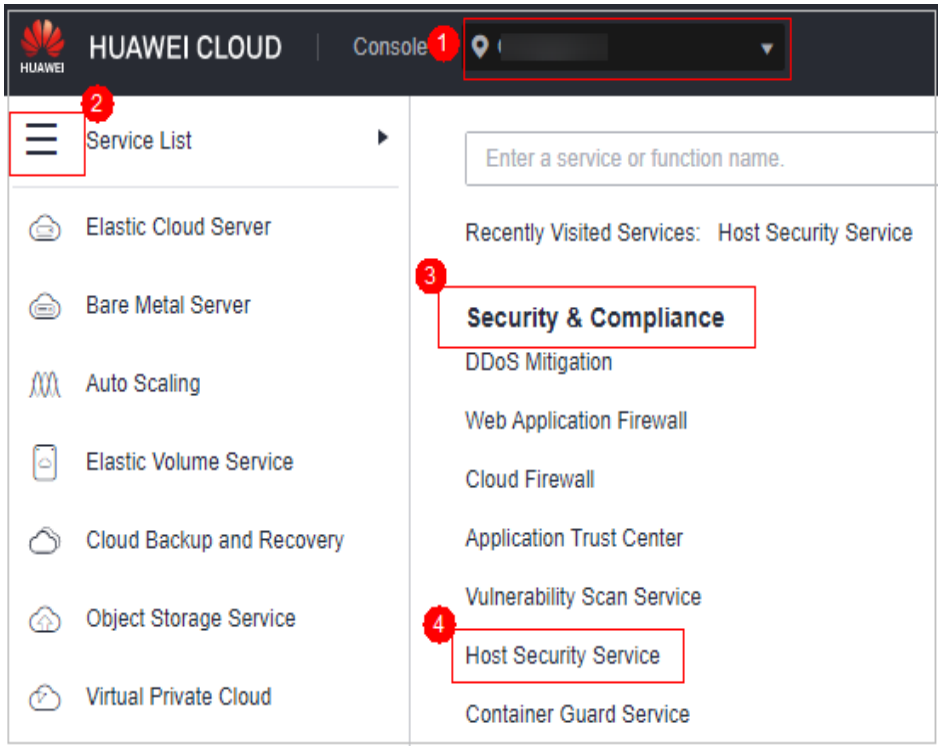
Para obter detalhes, consulte **Ativação de WTP**.

9.2 Como modificar um diretório protegido?

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em  e escolha **Security & Compliance** > **Host Security Service**.

Figura 9-1 Acessar o HSS



Passo 3 No painel de navegação, escolha **Prevention** > **Web Tamper Protection**.

Passo 4 Localize o servidor de destino e clique em **Configure Protection** na coluna **Operation**.

Passo 5 Clique em **Settings**. Na página **Protected Directory Settings** à direita, selecione o diretório a ser editado e clique em **Edit** na coluna **Operation**.

NOTA

- Se você precisar modificar arquivos no diretório protegido, interrompa primeiro a proteção para o diretório protegido.
- Depois que os arquivos são modificados, retome a proteção do diretório em tempo hábil.

Passo 6 Na caixa de diálogo **Edit Protected Directory**, modifique as configurações e clique em **OK**.

----Fim

9.3 O que devo fazer se a WTP não puder ser ativada?

As causas desse problema variam de acordo com os cenários.

Cota insuficiente

- **Sintoma**

  A cota de WTP na região selecionada é insuficiente.

Status do agente está anormal

- **Sintoma**

O status do agente é **Offline** ou **Not installed** na **lista de servidores** na página **Web Tamper Protection**.

- **Solução**

  Corrija a falha seguindo as instruções fornecidas em **Como corrigir um agente anormal**. Certifique-se de que **Agent Status** na lista de servidores esteja **Online**.

HSS de edição básica ou empresarial foi ativado

- **Sintoma**

  Protection Status está **Enabled** na **lista de servidores** no console do HSS.

- **Solução**

  Desative o HSS e, em seguida, **ative a WTP**.

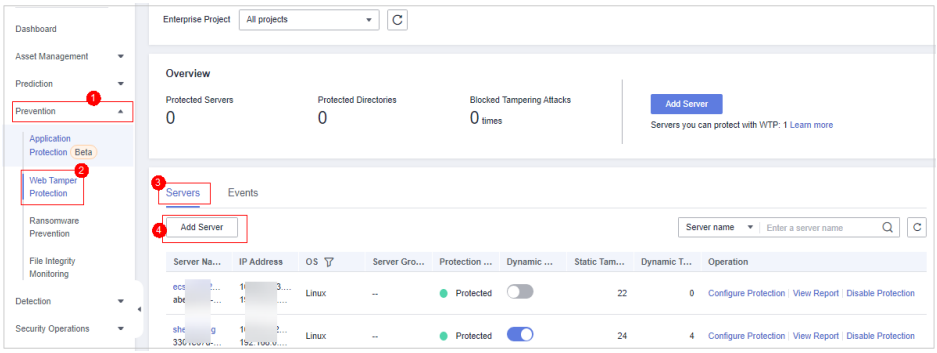
  NOTA

  As edições do HSS incluem as edições básica, empresarial, premium e WTP. Antes de ativar a WTP para um servidor, verifique se o HSS das edições básica, empresarial e premium foi desativado para o servidor.

A proteção foi ativada na página errada

Para ativar a WTP, escolha **Web Tamper Protection** > **Servers**.

Figura 9-2 Adicionar servidores protegidos



NOTA

Se você tiver comprado a edição WTP, poderá usar todas as funções da edição premium e ativar a proteção do servidor somente em **Web Tamper Protection**. Depois que a WTP é ativada, a proteção do servidor da edição premium também é ativada.

9.4 Como modificar um arquivo depois que a WTP é ativada?

Diretórios protegidos são somente leitura. Para modificar arquivos ou atualizar o site, execute qualquer uma das seguintes operações.

Desativação temporária da WTP

Desative a WTP enquanto você modifica arquivos em diretórios protegidos.

Seu site não está protegido contra adulteração enquanto a WTP estiver desativada. Ative-a imediatamente após a atualização do seu site.

Configuração da proteção programada

Você pode definir a WTP estática periódica e atualizar sites enquanto a WTP é desativada automaticamente.

Tenha cuidado ao definir os períodos para desabilitar a WTP, pois os arquivos não estarão protegidos nesses períodos.

9.5 O que posso fazer se eu tiver ativado a WTP dinâmica, mas seu status estiver ativado enquanto não estiver em vigor?

A WTP dinâmica protege suas aplicações de Tomcat.

Para que esta função entre em vigor, certifique-se de que:

- Existem aplicações de Tomcat em execução em seus servidores.
- Seus servidores executam o sistema operacional Linux.
- O arquivo **setenv.sh** foi gerado automaticamente no diretório **tomcat/bin** (normalmente 20 minutos após a ativação da WTP dinâmica). Se o arquivo existir, reinicie o Tomcat para fazer com que a WTP dinâmica tenha efeito.

Se o status da WTP dinâmica estiver **Enabled but not in effect** depois de ativá-lo, execute as seguintes operações:

- Verifique se o arquivo **setenv.sh** foi gerado no diretório **tomcat/bin**.
- Se o arquivo **setenv.sh** existir, verifique se o Tomcat foi reiniciado.

9.6 Quais são as diferenças entre as funções de proteção contra adulteração na Web do HSS e do WAF?

A função de proteção contra adulteração na Web do HSS monitora os diretórios do site em tempo real, faz backup de arquivos e restaura arquivos adulterados usando o backup, protegendo os sites contra adulteração. Essa função é útil para governos, instituições educacionais e empresas.

A WAF protege os dados do usuário na camada de aplicação. Suporta configuração de cache em páginas de Web estáticas. Quando um usuário acessa uma página da Web, o sistema retorna uma página em cache para o usuário e verifica aleatoriamente se a página foi adulterada.

Diferenças entre as funções de proteção contra adulteração na Web do HSS e do WAF

A tabela a seguir descreve as diferenças entre HSS e WAF.

Tabela 9-1 Diferenças entre as funções de proteção contra adulteração na Web do HSS e do WAF

Item	HSS	WAF
Proteção estática de páginas da Web	● Bloqueio de arquivos de driver e arquivos da Web Bloqueia arquivos nos diretórios de drivers e arquivos da Web para evitar que invasores os adulterem. ● Gerenciamento de processos privilegiados Permite que processos privilegiados modifiquem páginas da Web.	● Páginas da Web estáticas podem ser armazenadas em cache em servidores. ● O gerenciamento de processos privilegiados não é suportado.
Proteção dinâmica de páginas da Web	Protege seus dados enquanto o Tomcat está em execução, detectando adulteração dinâmica de dados em bancos de dados.	Não
Backup e restauração	● Backup e restauração ativos Se a WTP detectar que um arquivo no diretório de proteção foi adulterado, ela usará imediatamente o arquivo de backup no host local para restaurar o arquivo. ● Backup e restauração remotos Se um diretório de arquivo ou diretório de backup no servidor local se tornar inválido, você pode usar o serviço de backup remoto para restaurar a página da Web adulterada.	Não
Adequado para	Sites que possuem altos requisitos de segurança e difíceis de serem recuperados manualmente	Sites que exigem apenas proteção de camada de aplicação

Sugestão de compra

Site	Serviço
Sites comuns	Proteção contra adulteração na Web do WAF + HSS de edição empresarial
Sites que exigem uma forte proteção e recursos anti-adulteração	Proteção contra adulteração na Web do WAF + WTP do HSS

10 Container Guard Service

10.1 Como desativar a proteção de nó?

Antes de começar

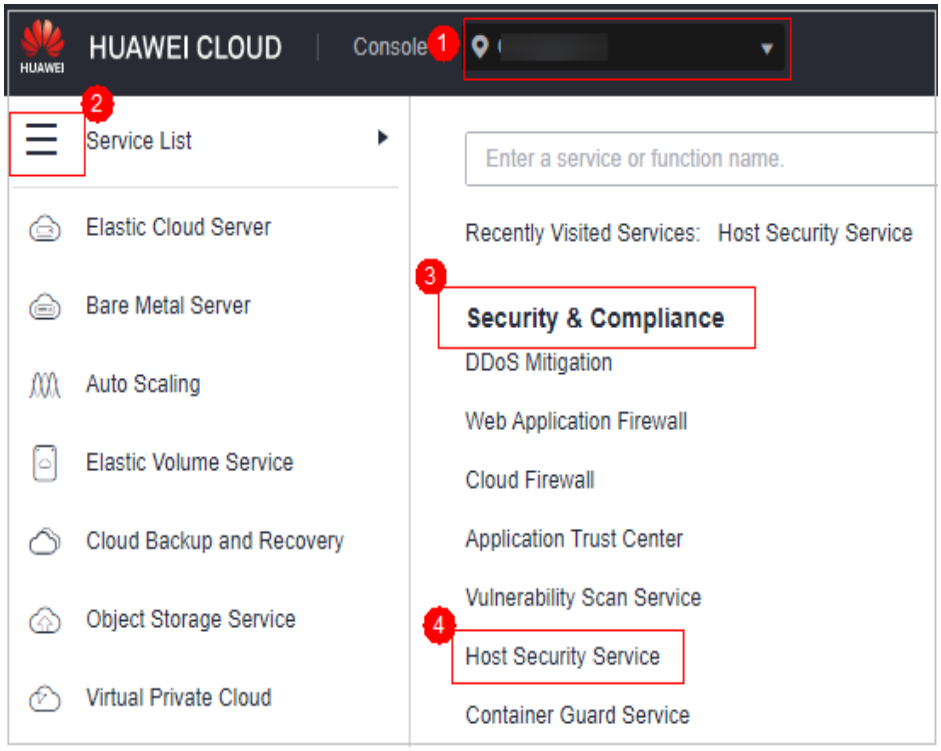
- Desativar a proteção não afeta os serviços, mas aumentará os riscos de segurança. É aconselhável manter seus servidores protegidos.
- Para cancelar a assinatura da cota de pagamento por uso da edição de container, você só precisa desativar a proteção.

Procedimento

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 10-1 Acessar o HSS



Passo 3 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

NOTA

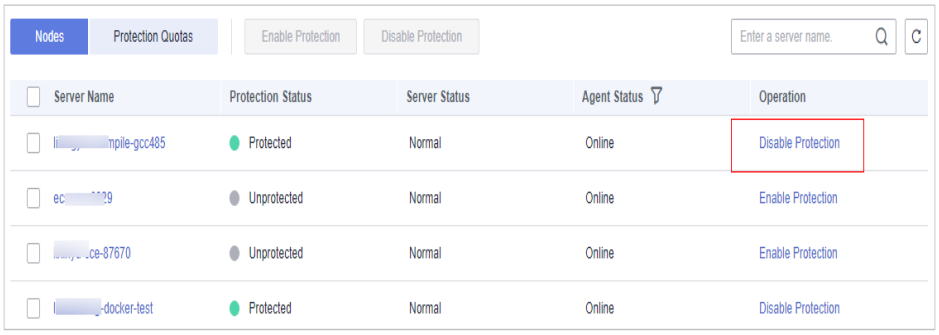
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Passo 4 Desative a proteção para um ou vários servidores.

- **Desativar a proteção para um servidor**

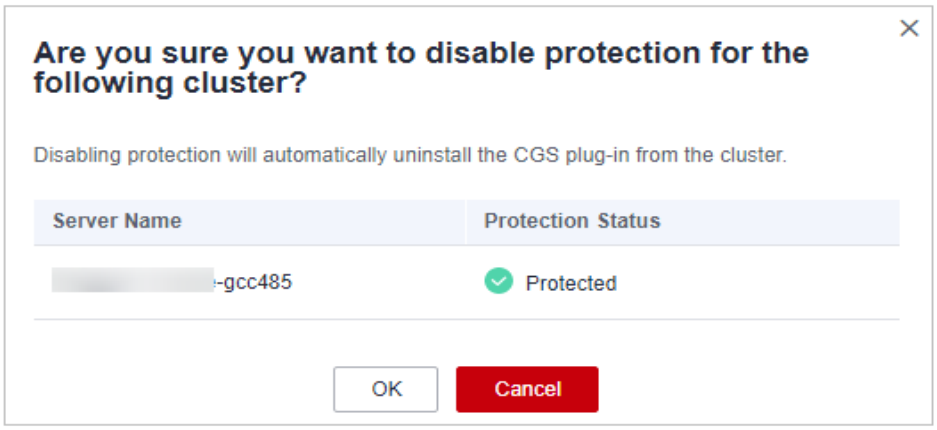
  a. Na lista de nós, clique em **Disable Protection** na coluna **Operation** de um servidor.

  Figura 10-2 Desativar a proteção do container



  b. Na caixa de diálogo exibida, confirme as informações e clique em **OK**.

Figura 10-3 Confirmar informações sobre a desativação da edição de container



c. Escolha **Asset Management** > **Containers & Quota** e clique na guia **Container Nodes**. Verifique o status da proteção na lista de servidores. Se estiver **Unprotected**, a proteção foi desativada.

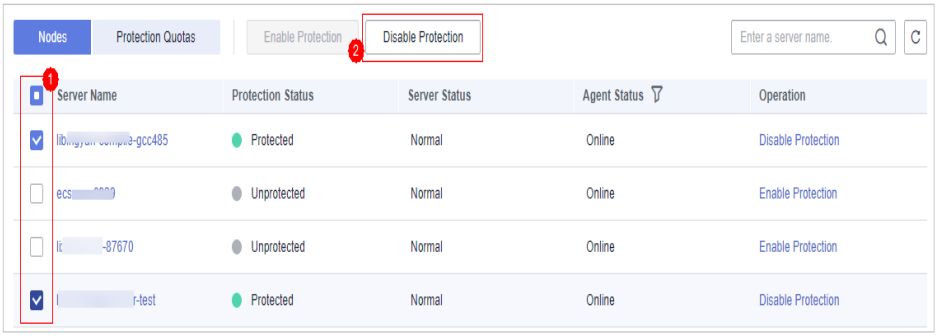
CUIDADO

Desativar a proteção não afeta os serviços, mas aumentará os riscos de segurança. É aconselhável manter seus servidores protegidos.

- **Desativar a proteção em lotes**

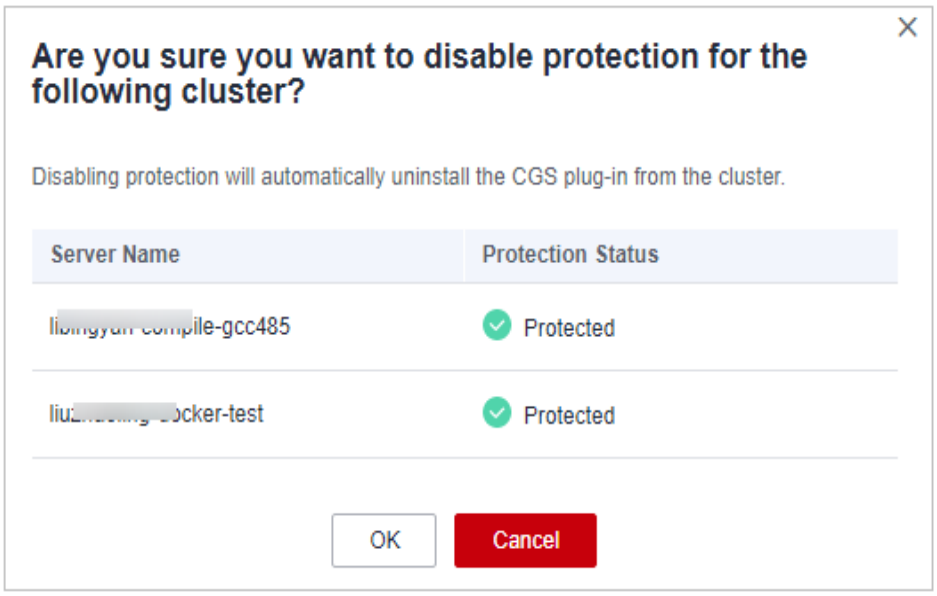
a. Na lista de nós, selecione servidores e clique em **Disable Protection** acima da lista.

Figura 10-4 Selecionar servidores



b. Na caixa de diálogo exibida, confirme as informações e clique em **OK**.

Figura 10-5 Confirmar informações sobre a desativação da edição de container em lotes



c. Escolha **Asset Management** > **Containers & Quota** e clique na guia **Container Nodes**. Verifique o status da proteção na lista de servidores. Se estiver **Unprotected**, a proteção foi desativada.

CUIDADO

Desativar a proteção não afeta os serviços, mas aumentará os riscos de segurança. É aconselhável manter seus servidores protegidos.

----Fim

10.2 Qual é o mecanismo de processamento de logs do CGS?

O CGS atualiza os logs em seu arquivo de log a cada 10 minutos. Se o arquivo exceder 30 MB, o CGS fará backup dos logs mais recentes de 30 MB em um arquivo de backup e limpará o conteúdo do arquivo de log.

O nome do arquivo de log de backup é o nome do arquivo de log mais a extensão **.last**. Por exemplo, o arquivo de backup de **shield.log** é **shield.log.last**.

10.3 Como mudar de CGS para console de HSS?

Você pode integrar o CGS no console do HSS para gerenciar centralmente os servidores e usar as novas funções.

Funções do CGS novo e anterior

Atualmente, o CGS foi integrado ao console do HSS para gerenciamento unificado. As funções existentes foram otimizadas e algumas novas funções foram adicionadas.

Tabela 10-1 Funções do CGS novo e anterior

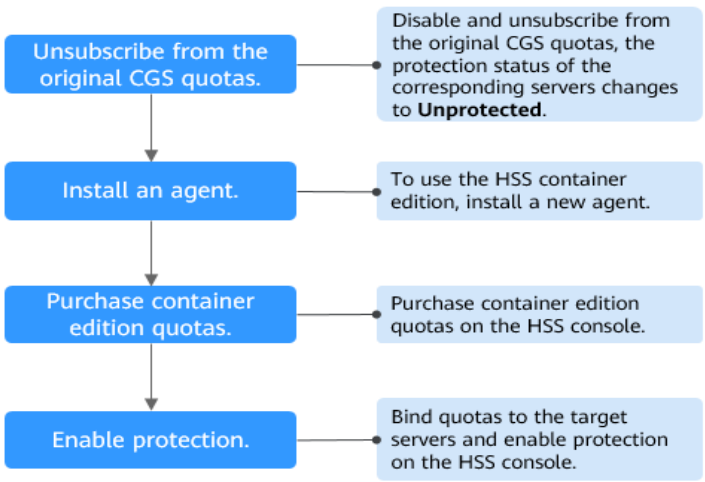
Função	CGS anterior	Novo CGS (novo HSS)
Gerenciamento de impressões digitais de ativos de container	×	√
Gerenciamento de nó de container	√	√
Gerenciamento de imagens privadas	√	√
Gerenciamento de imagens locais	√	√
Gerenciamento de imagens oficiais	√	×
Gerenciamento de imagens compartilhadas	×	√
Detecção de vulnerabilidade de imagem	√	√
Detecção de arquivo de imagem malicioso	√	√
Verificação da linha de base da imagem	√	√
Detecção de escape de vulnerabilidade	√	√
Detecção de escape de arquivo	√	√
Detecção de processo de container anormal	√	√
Detecção de configuração de container anormal	√	√
Detecção de inicialização de container anormal	√	√
Detecção de programa de container malicioso	√	√

Função	CGS anterior	Novo CGS (novo HSS)
Detecção de chamadas do sistema de alto risco	√	√
Detecção de acesso a arquivos sensíveis	√	√
Verificação de informações de software de container	√	√
Verificação de informações do arquivo de container	√	√
Gerenciamento de listas brancas	√	√
Gerenciamento de política de containers	√	√

Processo de alternância

Para mudar de CGS para HSS, cancele a assinatura do CGS, compre a edição de container do HSS e ative a proteção.

Figura 10-6 Procedimento de alternância do CGS



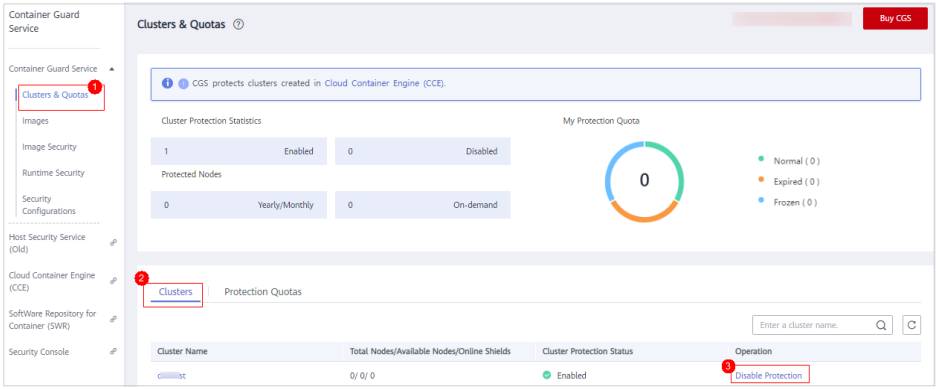
Passo 1: cancelar a assinatura das cotas originais do CGS

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Container Guard Service**. O console do **Container Guard Service** é exibido.

Passo 3 Escolha **Clusters & Quotas** em **Container Guard Service** para exibir a lista de proteção de cluster.

Figura 10-7 Visualizar o status de proteção de um cluster de containers



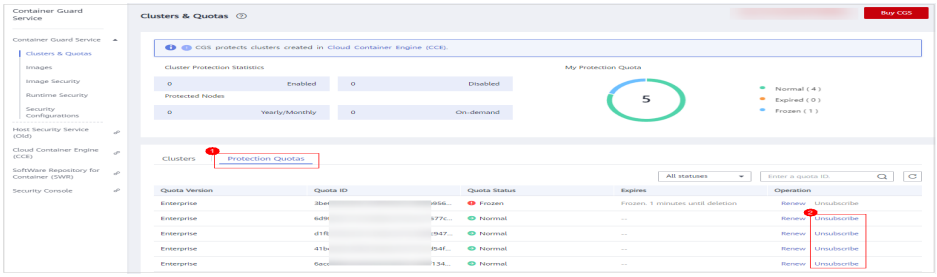
Passo 4 Clique em **Disable Protection** na coluna **Operation** do cluster de destino.

NOTA

Para facilitar o gerenciamento, é aconselhável desativar a proteção para todos os clusters.

Passo 5 Depois de desativar a proteção para todos os clusters, clique na guia **Protection Quotas**. Na coluna **Operation** das cotas, clique em **More** > **Unsubscribe** para cancelar a assinatura delas uma a uma.

Figura 10-8 Cancelamento da assinatura de cotas de edição de containers



NOTA

Se o modo de cobrança de cota original for pagamento por uso, a cobrança será interrompida quando você desativar a proteção.

----Fim

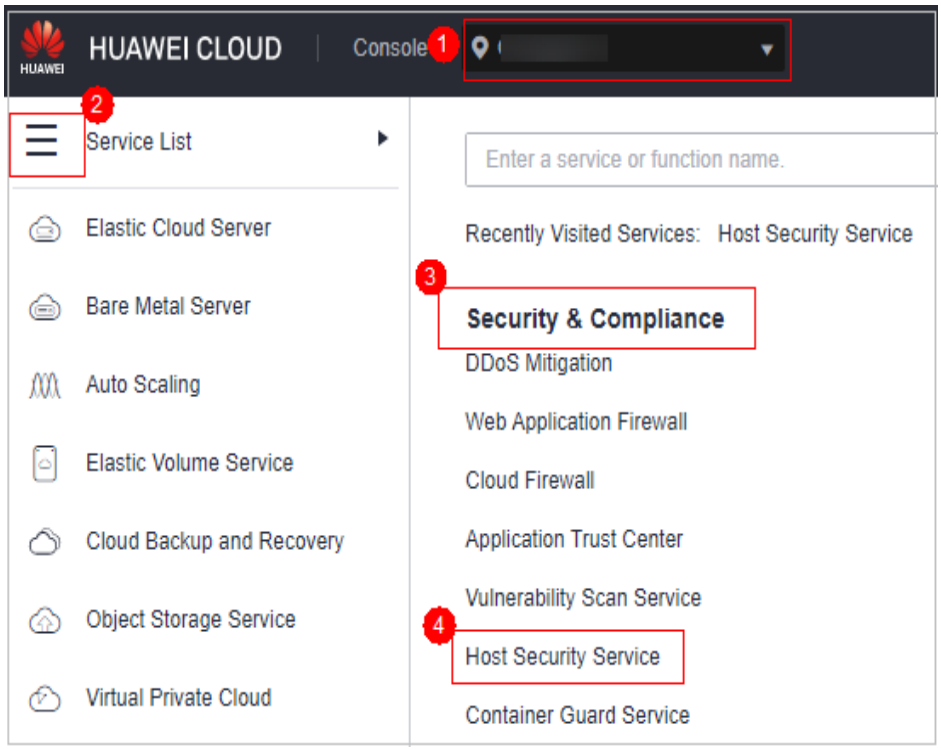
Passo 2: instalar um agente

CGS (anterior) e HSS (novo) são independentes um do outro. Para usar a edição de container do HSS, instale um novo agente.

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 10-9 Acessar o HSS



Passo 3 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 4 Clique em **Nodes** para verificar se os nós cuja proteção foi desativada existem na lista de nós.

AVISO

- Se os nós forem exibidos no console do HSS (novo), você não precisará instalar o agente.
- Se os nós não forem exibidos no console do HSS (novo), será necessário **instalar um agente**.

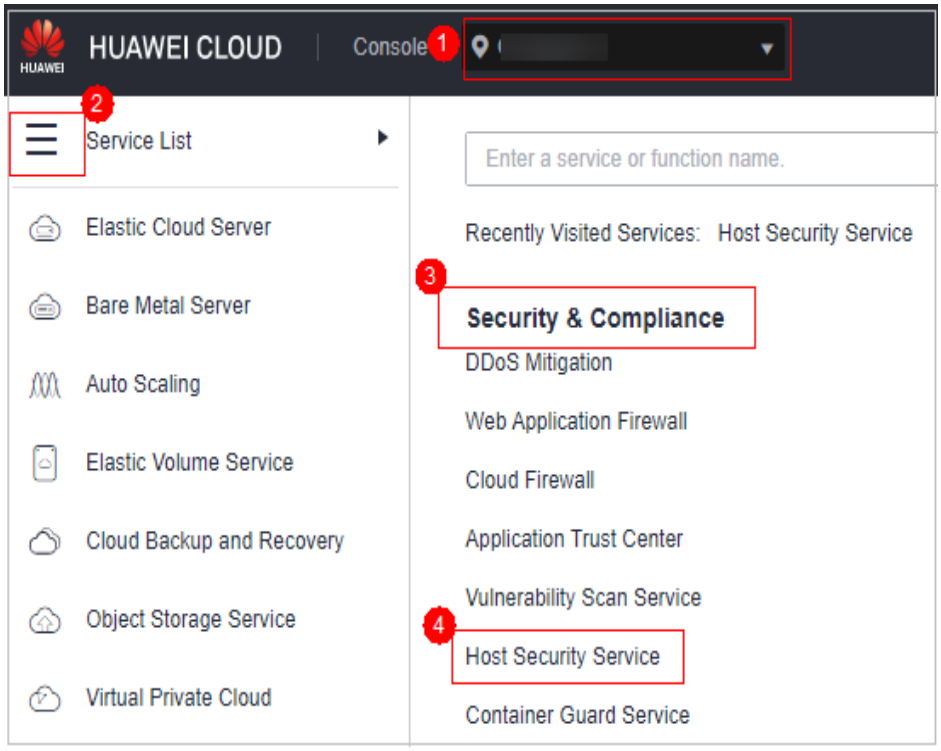
----Fim

Passo 3: comprar cotas de edição de containers no console do HSS

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 10-10 Acessar o HSS



Passo 3 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 4 Clique em **Buy CGS**.

Passo 5 Configure especificações do CGS.

Tabela 10-2 Parâmetros para compra de HSS

Parâmetro	Descrição	Exemplo de valor
Billing Mode	Apenas o modo de cobrança **Yearly/Monthly** é suportado.	Yearly/ Monthly
Region	● Para minimizar os problemas de conexão, compre a cota na região de seus servidores.	CN-Hong Kong
Edition	Selecione **Container**. Para obter detalhes sobre como ativar o modo de cobrança de pagamento por uso, consulte **Ativação da proteção do nó do container**.	Container
Node Quantity	Número de cotas de edição de containers compradas	10

Parâmetro	Descrição	Exemplo de valor
Required Duration	● Selecione uma duração conforme necessário. ● É aconselhável selecionar **Auto-renew** para garantir que seus servidores estejam sempre protegidos. ● Se você selecionar **Auto-renew**, o sistema renovará automaticamente sua assinatura, desde que o saldo da sua conta seja suficiente. O período de renovação é o mesmo que a duração exigida. ● Se você não selecionar **Auto-renew**, renove manualmente o serviço antes que ele expire.	1 year
Tags	Você pode colocar tags em recursos de nuvem do mesmo tipo para ajudá-lo a pesquisar rapidamente os recursos.	cgs-data

Passo 6 No canto inferior direito da página, clique em **Next**.

Para obter detalhes sobre preços, consulte **Detalhes de preços do produto**.

Passo 7 Depois de confirmar o pedido, selecione **I have read and agree to the Host Security Service Disclaimer** e clique em **Pay Now**.

Passo 8 Clique em **Pay Now** e conclua o pagamento.

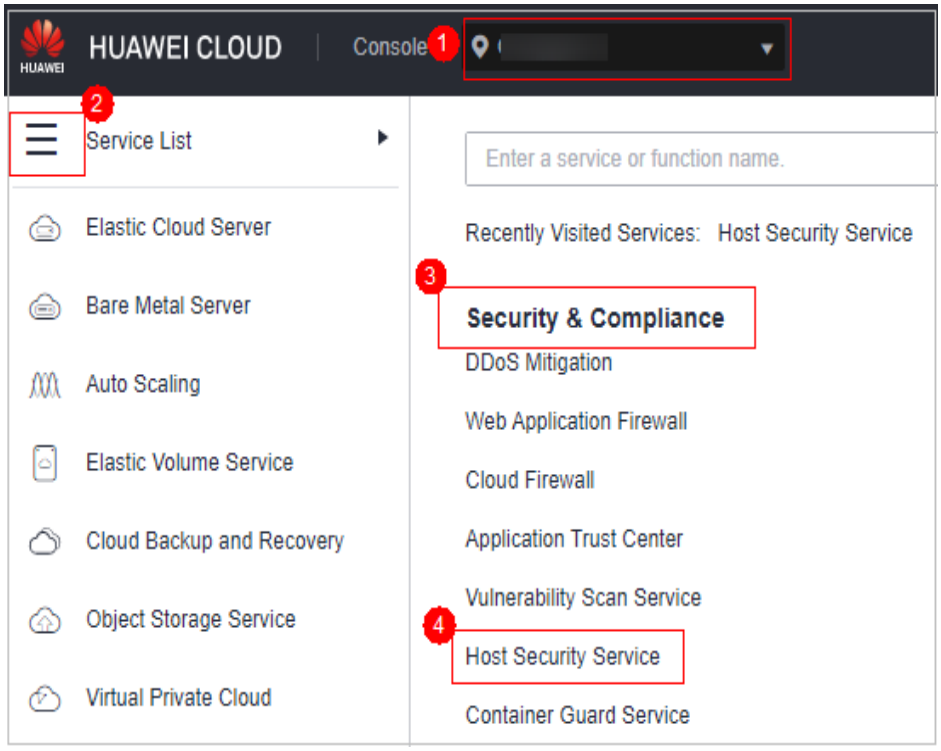
----Fim

Passo 4: ativar a proteção

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em  e escolha **Security & Compliance** > **Host Security Service**.

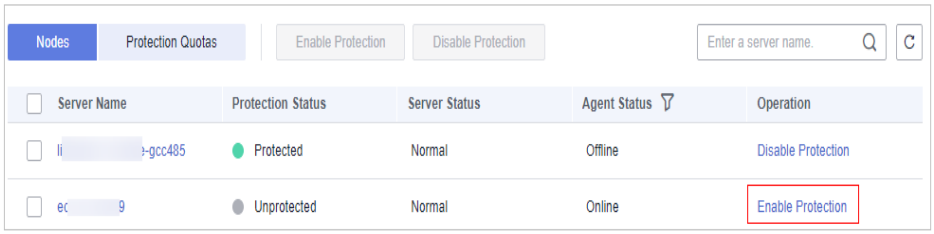
Figura 10-11 Acessar o HSS



Passo 3 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 4 Na coluna **Operation** da lista de nós, clique em **Enable Protection**.

Figura 10-12 Ativar a proteção do container

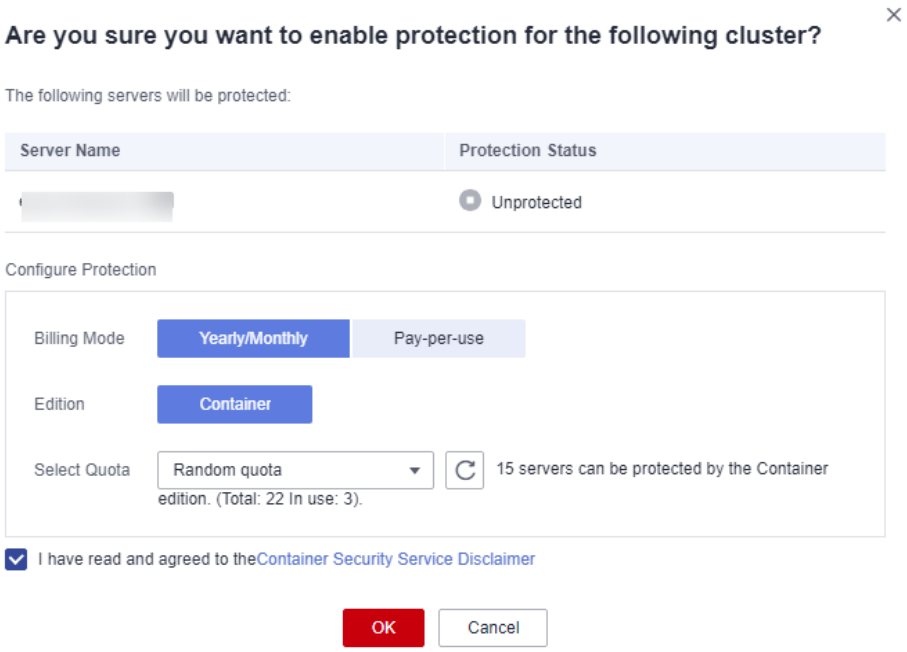


Passo 5 Você pode comprar cotas no modo de pagamento por uso ou anual/mensal.

- **Anual/Mensal**

  Na caixa de diálogo exibida, selecione **Yearly/Monthly**, leia o *Aviso de isenção de responsabilidade do Container Guard Service* e selecione **I have read and agreed to Container Guard Service Disclaimer**.

Figura 10-13 Ativar proteção anual/mensal



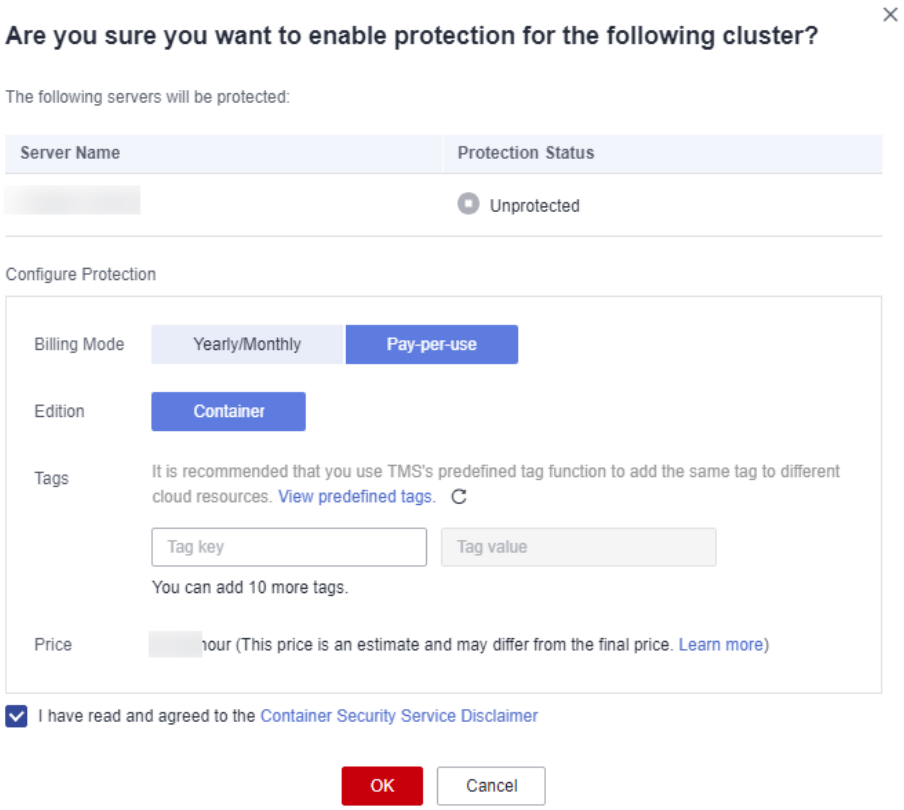
A cota pode ser alocada das seguintes maneiras:

- Selecione **Random quota** para permitir que o sistema aloque a cota com a validade restante mais longa para o servidor.
- Selecione um ID de cota e aloque-o a um servidor.

- **Sob demanda**

  Na caixa de diálogo exibida, selecione **Pay-per-use**, leia o *Aviso de isenção de responsabilidade do Container Guard Service* e selecione **I have read and agreed to Container Guard Service Disclaimer**.

Figura 10-14 Ativar a proteção de pagamento por uso



Passo 6 Clique em **OK**. Se o **Protection Status** do servidor for alterado para **Protected**, a proteção foi ativada.

NOTA

- Uma cota do CGS protege um nó de cluster.

----Fim

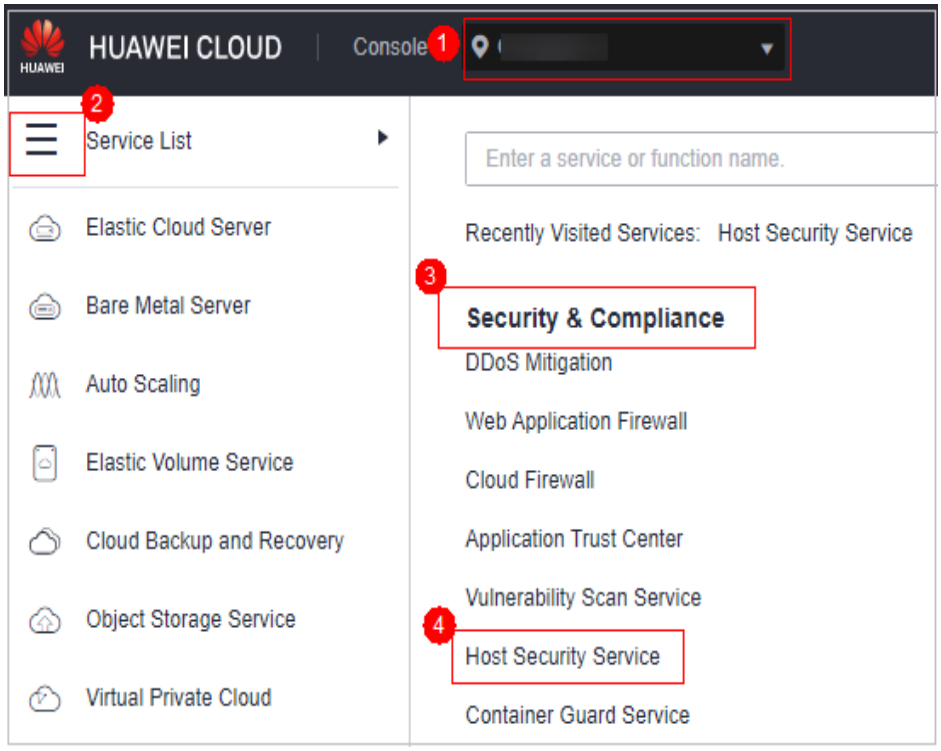
10.4 Como ativar a proteção de nó?

Quando você ativa a proteção do nó, o sistema instala automaticamente o plug-in de CGS no nó.

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 10-15 Acessar o HSS



Passo 3 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 4 Na coluna **Operation** de um nó, clique em **Enable Protection**.

Passo 5 Na caixa de diálogo exibida, leia e selecione **I have read and agree to the Container Guard Service Disclaimer**.

Passo 6 Clique em **OK** para ativar a proteção para o nó. Se **Protection Status** do nó for **Protected**, a proteção será ativada para o nó.

NOTA

- Se você ativar a proteção para nós que excedam sua cota de proteção comprada, os nós em excesso serão cobrados em uma base de pagamento por uso. Para obter detalhes sobre o modo de cobrança de pagamento por uso do Host Security Service (HSS), consulte **Quando e como o CGS será cobrado por uso?**
- Uma cota de HSS protege um nó do cluster.

----Fim

10.5 Como ativar a auditoria do servidor de API para um container do Kubernetes local?

Cenário

Os containers de Kubernetes locais são usados.

Pré-requisitos

- A proteção de container foi ativada. Para obter detalhes, consulte **Ativação da proteção de nós de containers**.
- A auditoria do servidor da API está desativada. Execute as seguintes etapas para verificar seu status:
  a. Efetue logon no nó onde o kube-apiserver está localizado.
  b. Verifique o arquivo **kube-apiserver.yaml** ou o processo de kube-apiserver iniciado.
     - Vá para o diretório **/etc/kubernetes/manifest** e verifique se **--audit-log-path** e **--audit-policy-file** existem em **kube-apiserver.yaml**. Se eles não existirem, a auditoria do servidor da API será desativada.
     - Execute o comando **ps** para verificar se **--audit-log-path** e **--audit-policy-file** existem nas linhas de comando do processo de kube-apiserver. Se eles não existirem, a função de auditoria do processo de kube-apiserver é desativada.

Ativação da auditoria do servidor da API

Passo 1 Copie o seguinte conteúdo YAML e salve-o em um arquivo TXT:

Esse arquivo YAML é o arquivo de configuração da função de auditoria do Kubernetes. Você pode usar diretamente o arquivo ou compilá-lo conforme necessário.

```
apiVersion: audit.k8s.io/v1 # This is required.
kind: Policy
# Don't generate audit events for all requests in RequestReceived stage.
omitStages:
  - "RequestReceived"
rules:
  # The following requests were manually identified as high-volume and low-risk,
  # so drop them.
  # Kube-Proxy running on each node will watch services and endpoint objects in
real time
  - level: None
    users: ["system:kube-proxy"]
    verbs: ["watch"]
    resources:
      - group: "" # core
        resources: ["endpoints", "services"]
  # Some health checks
  - level: None
    users: ["kubelet"] # legacy kubelet identity
    verbs: ["get"]
    resources:
      - group: "" # core
        resources: ["nodes"]
  - level: None
    userGroups: ["system:nodes"]
    verbs: ["get"]
    resources:
      - group: "" # core
        resources: ["nodes"]
  - level: None
    users: ["system:apiserver"]
    verbs: ["get"]
    resources:
      - group: "" # core
        resources: ["namespaces"]
  # Some system component certificates reuse the master user, which cannot be
accurately distinguished from user behavior,
  # considering that subsequent new functions may continue to add system
operations under kube-system, the cost of targeted configuration is relatively
high,
  # in terms of the overall strategy, it is not recommended (allowed) for users
```



```
to operate under the kube-system,
  # so overall drop has no direct impact on user experience
  - level: None
    verbs: ["get", "update"]
    namespaces: ["kube-system"]
  # Don't log these read-only URLs.
  - level: None
    nonResourceURLs:
      - /healthz*
      - /version
      - /swagger*
  # Don't log events requests.
  - level: None
    resources:
      - group: "" # core
        resources: ["events"]
  # Don't log leases requests
  - level: None
    verbs: [ "get", "update" ]
    resources:
      - group: "coordination.k8s.io"
        resources: ["leases"]
  # Secrets, ConfigMaps, and TokenReviews can contain sensitive & binary data,
  # so only log at the Metadata level.
  - level: Metadata
    resources:
      - group: "" # core
        resources: ["secrets", "configmaps"]
      - group: authentication.k8s.io
        resources: ["tokenreviews"]
  # Get repsonses can be large; skip them.
  - level: Request
    verbs: ["get", "list", "watch"]
    resources:
      - group: "" # core
      - group: "admissionregistration.k8s.io"
      - group: "apps"
      - group: "authentication.k8s.io"
      - group: "authorization.k8s.io"
      - group: "autoscaling"
      - group: "batch"
      - group: "certificates.k8s.io"
      - group: "extensions"
      - group: "networking.k8s.io"
      - group: "policy"
      - group: "rbac.authorization.k8s.io"
      - group: "settings.k8s.io"
      - group: "storage.k8s.io"
  # Default level for known APIs
  - level: RequestResponse
    resources:
      - group: "" # core
      - group: "admissionregistration.k8s.io"
      - group: "apps"
      - group: "authentication.k8s.io"
      - group: "authorization.k8s.io"
      - group: "autoscaling"
      - group: "batch"
      - group: "certificates.k8s.io"
      - group: "extensions"
      - group: "networking.k8s.io"
      - group: "policy"
      - group: "rbac.authorization.k8s.io"
      - group: "settings.k8s.io"
      - group: "storage.k8s.io"
  # Default level for all other requests.
  - level: Metadata
```

Passo 2 Faça o upload do arquivo TXT para o nó onde o kube-apiserver está implementado.

Passo 3 Vá para o diretório **/etc/kubernetes/manifest** e adicione o seguinte conteúdo ao arquivo **kube-apiserver.yaml** para ativar a auditoria do servidor da API:

```
--audit-policy-file=/etc/kubernetes/audit-policy.yaml \
--audit-log-path=/var/log/kubernetes/audit/audit.log \
--audit-log-maxsize=100 \
--audit-log-maxage=1  \
--audit-log-maxbackup=10
```

NOTA

--audit-policy-file: arquivo de configuração usado pela função de auditoria.

--audit-log-path: caminho do arquivo de log onde os eventos de auditoria são gravados. Se esse sinalizador não for especificado, o back-end de registro será desativado.

--audit-log-maxsize: tamanho máximo (em MB) de um arquivo de log de auditoria antes de rotação.

--audit-log-maxage: número máximo de dias para armazenar arquivos de log de auditoria anteriores.

--audit-log-maxbackup: número máximo de arquivos de log de auditoria retidos.

Passo 4 (Opcional) Se o seu kube-apiserver for executado como um pod, execute as seguintes etapas para persistir os logs no servidor:

1. Localize o campo **volumeMounts** em **kube-apiserver.yaml** e configure a montagem do volume da seguinte maneira:

```
volumeMounts:
  - mountPath: /etc/kubernetes/audit-policy.yaml
    name: audit
    readOnly: true
  - mountPath: /var/log/kubernetes/audit/
    name: audit-log
    readOnly: false
```

2. Localize o campo **volumes** em **kube-apiserver.yaml** e configure-o da seguinte forma:

```
volumes:
- name: audit
  hostPath:
    path: /etc/kubernetes/audit-policy.yaml
    type: File
- name: audit-log
  hostPath:
    path: /var/log/kubernetes/audit/
    type: DirectoryOrCreate
```

----Fim

10.6 O que devo fazer se o plug-in de proteção de cluster de container falhar ao ser desinstalado?

Possíveis causas

Se a rede do cluster estiver anormal ou o plug-in estiver em execução, a desinstalação do plug-in no console do HSS poderá falhar.

Solução

Execute as seguintes etapas para desinstalar manualmente o plug-in:

Passo 1 Faça logon no servidor de nuvem.

Passo 2 Crie o arquivo **plugin.yaml** no diretório **/tmp** e copie o seguinte conteúdo do script para o arquivo:


```
apiVersion: v1
kind: Namespace
metadata:
  labels:
    admission.gatekeeper.sh/ignore: no-self-managing
    control-plane: controller-manager
    gatekeeper.sh/system: "yes"
    pod-security.kubernetes.io/audit: restricted
    pod-security.kubernetes.io/audit-version: latest
    pod-security.kubernetes.io/enforce: restricted
    pod-security.kubernetes.io/enforce-version: v1.24
    pod-security.kubernetes.io/warn: restricted
    pod-security.kubernetes.io/warn-version: latest
  name: gatekeeper-system
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: assign.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: assignimage.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: assignmetadata.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: configs.config.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: constraintpodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: constrainttemplatepodstatuses.status.gatekeeper.sh
---
```



```
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.11.3
  labels:
    gatekeeper.sh/system: "yes"
  name: constrainttemplates.templates.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: expansiontemplate.expansion.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: expansiontemplatepodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: modifyset.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: mutatorpodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.11.3
  labels:
    gatekeeper.sh/system: "yes"
  name: providers.externaldata.gatekeeper.sh
---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  creationTimestamp: null
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-role
  namespace: gatekeeper-system
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  creationTimestamp: null
  labels:
    gatekeeper.sh/system: "yes"
```



```
  name: gatekeeper-manager-role
---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-rolebinding
  namespace: gatekeeper-system
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: gatekeeper-manager-role
subjects:
- kind: ServiceAccount
  name: gatekeeper-admin
  namespace: gatekeeper-system
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-rolebinding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: gatekeeper-manager-role
subjects:
- kind: ServiceAccount
  name: gatekeeper-admin
  namespace: gatekeeper-system
---
apiVersion: admissionregistration.k8s.io/v1
kind: MutatingWebhookConfiguration
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-mutating-webhook-configuration
---
apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingWebhookConfiguration
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-validating-webhook-configuration
```

Passo 3 Crie o arquivo **uninstall.sh** no diretório **/tmp** e copie o seguinte conteúdo de script para o arquivo:

```
#!/bin/bash
kubectl delete -f /tmp/plugin.yaml
kubectl delete ns cgs-provider
```

Passo 4 Execute o seguinte comando para desinstalar o plug-in de proteção de cluster de container:

```
bash /tmp/uninstall.sh
```

Se forem exibidas informações semelhantes às seguintes, o plug-in foi desinstalado.


```
namespace "gatekeeper-system" deleted
resourcequota "gatekeeper-critical-pods" deleted
customresourcedefinition.apiextensions.k8s.io "assign.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "assignimage.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "assignmetadata.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "configs.config.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constraintpodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constrainttemplatepodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constrainttemplates.templates.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "expansiontemplate.expansion.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "expansiontemplatepodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "modifyset.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "mutatorpodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "providers.externaldata.gatekeeper.sh" deleted
serviceaccount "gatekeeper-admin" deleted
role.rbac.authorization.k8s.io "gatekeeper-manager-role" deleted
clusterrole.rbac.authorization.k8s.io "gatekeeper-manager-role" deleted
rolebinding.rbac.authorization.k8s.io "gatekeeper-manager-rolebinding" deleted
clusterrolebinding.rbac.authorization.k8s.io "gatekeeper-manager-rolebinding" deleted
secret "gatekeeper-webhook-server-cert" deleted
service "gatekeeper-webhook-service" deleted
deployment.apps "gatekeeper-audit" deleted
deployment.apps "gatekeeper-controller-manager" deleted
poddisruptionbudget.policy "gatekeeper-controller-manager" deleted
mutatingwebhookconfiguration.admissionregistration.k8s.io "gatekeeper-mutating-webhook-configuration" deleted
validatingwebhookconfiguration.admissionregistration.k8s.io "gatekeeper-validating-webhook-configuration" deleted
```

----Fim

11 Proteção contra ransomware

11.1 Quais são as diferenças entre backup de proteção contra ransomware e backup em nuvem?

O backup da proteção contra ransomware de HSS depende do Cloud Backup and Recovery (CBR). A política de backup do servidor só entra em vigor após a compra do CBR.

Não há diferença entre os dois em termos de mecanismo de backup e gerenciamento. A única diferença é que o backup de ransomware gera uma biblioteca de backup de ransomware dedicada.

O mecanismo de backup da proteção contra ransomware herda o do CBR (Cloud Backup and Restoration). Os arquivos de backup da proteção contra ransomware podem ser gerenciados e visualizados de forma centralizada no CBR. Para obter detalhes sobre o mecanismo de CBR, consulte **O que é CBR**.

12 Região e AZ

12.1 O que são regiões e AZs?

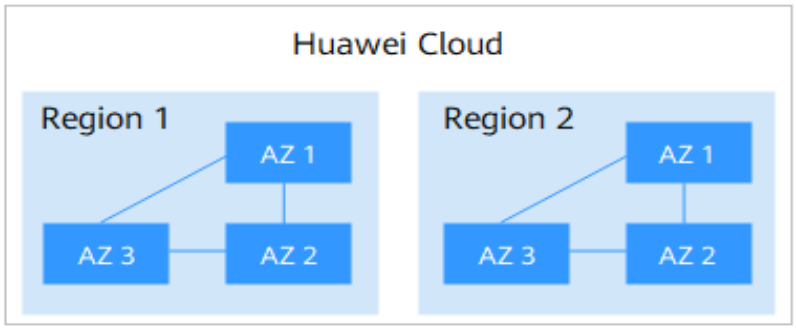
Conceitos

Uma região e uma zona de disponibilidade (AZ) identificam a localização de um data center. Você pode criar recursos em uma região e AZ específicas.

- **Regions** são definidas em termos de localização geográfica e latência da rede. Cada região tem seus próprios serviços públicos compartilhados (ECS, EVS, OBS, VPC, EIP e IMS). As regiões são comuns ou dedicadas. Uma região comum fornece serviços de nuvem comuns disponíveis para todos os locatários. Uma região dedicada fornece serviços de um tipo específico ou apenas para locatários específicos.
- Uma **AZ** contém um ou mais data centers físicos. Cada AZ tem instalações independentes de resfriamento, extinção de incêndio, antiumidade e eletricidade. A computação, rede, armazenamento e outros recursos em uma AZ são logicamente divididos em vários clusters. As AZs em uma região são interconectadas por meio de fibra óptica de alta velocidade, para que os sistemas implementados nas AZs possam alcançar maior disponibilidade.

Figura 12-1 mostra a relação entre as regiões e as AZs.

Figura 12-1 Região e AZ



HUAWEI CLOUD fornece serviços em muitas regiões do mundo. Você pode selecionar uma região e uma AZ conforme necessário.

Qual região devo escolher?

Ao selecionar uma região, considere o seguinte:

- Localização

  É recomendável selecionar uma região mais próxima dos usuários-alvo. Isso reduz a latência da rede e melhora a taxa de acesso. No entanto, as regiões da China continental fornecem a mesma infraestrutura, qualidade de rede BGP e operações e configurações em recursos. Portanto, se seus usuários-alvo estiverem na China continental, não será necessário considerar as diferenças de latência da rede ao selecionar uma região.

  – Se seus usuários-alvo estiverem em Pacífico Asiático (excluindo a China continental), selecione a região **CN-Hong Kong**, **AP-Bangkok** ou **AP-Singapore**.

  – Se você ou seus usuários-alvo estiverem na África, selecione a região **AF-Johannesburg**.

  – Se você ou seus usuários-alvo estiverem na Europa, selecione a região **EU-Paris**.

- Preço do recurso

  Os preços dos recursos podem variar em diferentes regiões. Para obter detalhes, consulte **Detalhes de preço do produto**.

Qual AZ devo escolher?

Considere seus requisitos de DR e latência de rede ao selecionar uma AZ:

- Para obter maior capacidade de DR, implemente recursos em diferentes AZs na mesma região.
- Para reduzir a latência, implemente recursos na mesma AZ.

Regiões e pontos de extremidade

Antes de usar uma API para chamar recursos, especifique sua região e ponto de extremidade. Para obter mais detalhes, consulte **Regiões e pontos de extremidade**.

12.2 Onde o HSS está disponível?

Atualmente, você pode acessar servidores não da Huawei Cloud apenas nas seguintes regiões:

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

Se o seu servidor não for um servidor da Huawei Cloud, compre HSS em uma das regiões anteriores e conecte o servidor à região executando o procedimento de instalação para servidores não da Huawei Cloud.

13 Configurações de segurança

13.1 Como limpar a lista branca de endereços IP de logon SSH configurada no HSS?

Os métodos para limpar a lista branca variam de acordo com seus estados de cota do HSS.

Normal/Expirada

Cotas normais e expiradas podem ser usadas. Para excluir o endereço IP de logon SSH, desative-o ou exclua-o no console de gerenciamento.

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Passo 3 Escolha **Installation and Configuration**, clique em **Security Configuration** e clique em **SSH IP Whitelist**.

Passo 4 Localize a linha que contém o endereço IP de destino na lista branca e clique em **Disable** ou **Delete** na coluna **Operation**.

----Fim

Congelado ou excluído após o período de congelamento expirar

Se o status da cota for **Frozen** ou se a cota for excluída após o período de congelamento expirar, o HSS não protegerá mais seus servidores. Não é possível limpar a lista branca de endereços IP de logon SSH por meio do console de gerenciamento.

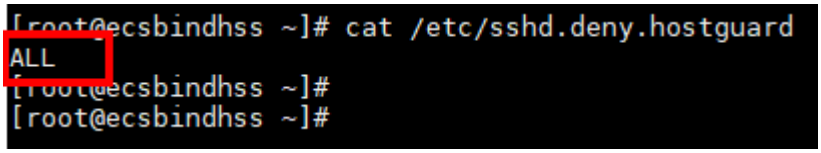
Execute as seguintes etapas para limpar a lista branca de endereços IP de logon SSH configurada:

Passo 1 Faça logon no servidor cuja lista branca de endereços IP de logon SSH precisa ser limpa.

Passo 2 Execute o seguinte comando para visualizar o arquivo **/etc/sshd.deny.hostguard**, conforme mostrado em **Figura 13-1**.

cat /etc/sshd.deny.hostguard

Figura 13-1 Visualização do conteúdo do arquivo



Passo 3 Execute o seguinte comando para abrir o arquivo **/etc/sshd.deny.hostguard**:

vim /etc/sshd.deny.hostguard

Passo 4 Pressione **i** para entrar no modo de edição e exclua **ALL**.

Passo 5 Pressione **Esc** para sair do modo de edição e execute o comando **:wq** para salvar a modificação e sair.

----Fim

13.2 O que posso fazer se eu não posso fazer logon remotamente em um servidor via SSH?

Sintomas

Você pode fazer logon em um servidor por meio de console da Huawei Cloud, mas não via SSH.

Possíveis causas

- Um servidor será bloqueado se for considerado um servidor suspeito que esteja realizando ataques de força bruta (por exemplo, o número de tentativas de senhas incorretas chega a 5 em 30 segundos).
- A **lista branca de IPs de logon SSH** está ativada. Seus endereços IP de logon não foram adicionados à lista branca de logon.

  Se você ativar a lista branca de endereços IP de logon SSH, os logons SSH serão permitidos apenas a partir de endereços IP na lista branca.

Solução

Passo 1 Verifique se o seu endereço IP de logon foi bloqueado porque foi considerado uma fonte de ataques de força bruta.

- Se o seu endereço IP de logon foi bloqueado como fonte de ataque, vá para a página **Events**, clique em **Blocked IP Addresses** e desbloqueie seu endereço IP.
- Se o seu endereço IP de logon não foi bloqueado por esse motivo, vá para **Passo 2**.

Passo 2 Verifique se o seu endereço IP de logon está bloqueado porque não está na lista branca e a lista branca de IP de logon SSH está ativada.

- Se o seu endereço IP de logon não foi bloqueado por esse motivo, adicione o endereço IP à **lista branca de endereços IP de logon SSH**.

- Se o seu endereço IP de logon não foi bloqueado por esse motivo, entre em contato com o suporte técnico.

----Fim

Procedimento de acompanhamento

- **O que devo fazer se não conseguir fazer logon no meu ECS de Linux?**
- **O que devo fazer se não conseguir fazer logon no meu ECS de Windows?**

13.3 Como usar a 2FA?

Esta seção de perguntas frequentes mostra como usar a 2FA.

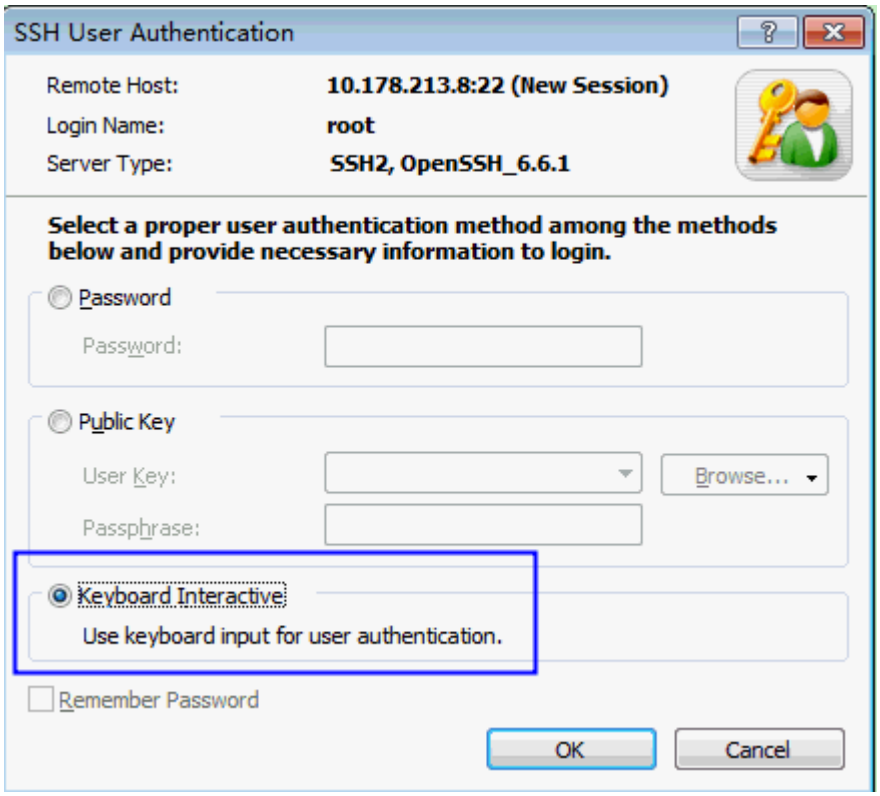
Ativar a 2FA

Para obter detalhes, consulte **Ativação da autenticação de dois fatores**.

Fazer logon e passar autenticação 2FA

- Efetuar logon em um servidor do Linux
  a. Use PuTTY ou Xshell para fazer logon no servidor.
     Selecione **Keyboard Interactive** e insira as informações de identidade do usuário.
     - PuTTY
       Defina o modo de autenticação para **Keyboard Interactive** e clique em **OK**.

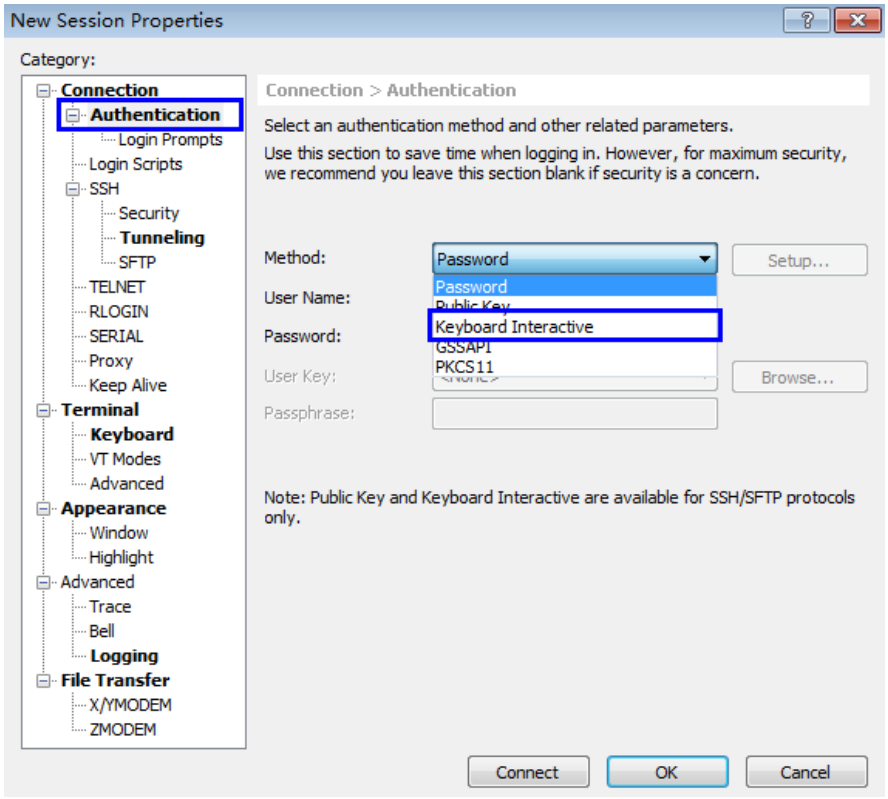
       Figura 13-2 Método de interação do teclado (1)



- Xshell

  Na caixa de diálogo **New Session Properties**, escolha **Connection > Authentication > Method**, escolha **Keyboard Interactive** na lista suspensa de **Method** e clique em **OK**.

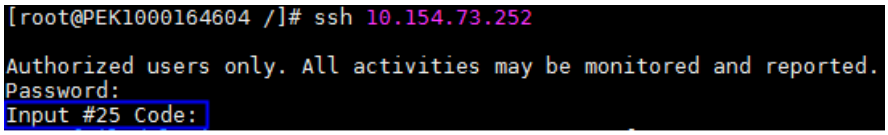
  Figura 13-3 Método de interação do teclado (2)



b. Digite a conta e a senha do servidor.

c. Digite o código de verificação 2FA enviado ao seu terminal.

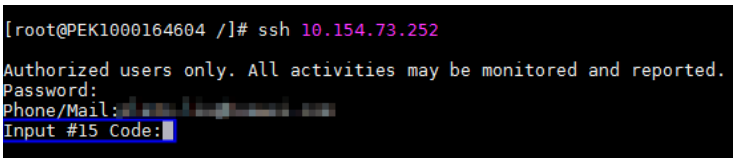
Figura 13-4 Digitar um código de verificação



NOTA

- O telefone celular ou caixa de e-mail inscrito em um tópico de notificação receberá uma mensagem: **[HUAWEI CLOUD] Login verification code #** *XX* para o seu ECS (*xxxx-yyyy*): *XXXXXX*.
- Se você não receber o código de verificação, verifique se o firewall do SELinux está desativado e tente novamente.
- Se o HSS detectar que um servidor pode estar sob um ataque de força bruta, ele solicitará que você insira informações detalhadas sobre o terminal de assinatura (como o número de celular ou o endereço de e-mail) antes de enviar um código de verificação, conforme mostrado em **Figura 13-5**.

Figura 13-5 Digitar um número de celular ou endereço de e-mail



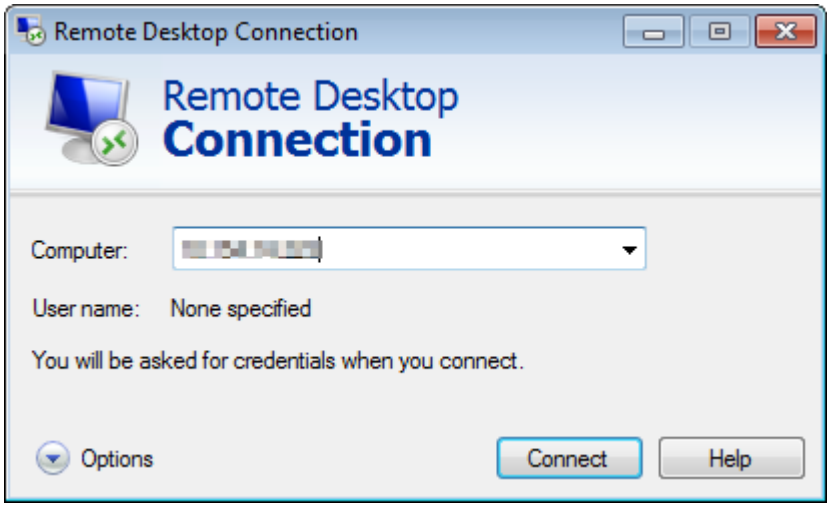
- Você pode adicionar até 10 números de celular e endereços de e-mail por vez. Um tópico pode ter até 10.000 números de celular e endereços de e-mail.

- Efetuar logon em um servidor do Windows

  a. Clique em **Start**, insira **Remote Desktop Connection** na caixa de pesquisa e pressione **Enter** para abrir a conexão de área de trabalho remota.

  b. Digite o endereço IP do host na caixa de texto **Computer** e clique em **Connect**.

Figura 13-6 Conexão de área de trabalho remota



  c. Digite o número de celular reservado ou endereço de e-mail para receber o código de verificação 2FA.

Figura 13-7 Digitar um número de celular ou endereço de e-mail

NOTA

O telefone celular ou caixa de e-mail inscrito em um tópico de notificação receberá uma mensagem: **[HUAWEI CLOUD] Login verification code #** *XX* para o seu ECS (*xxxx-yyyy*): *XXXXXX*.

d. Digite o código de verificação, o nome da conta do servidor e a senha na página de logon e clique em  para efetuar logon no servidor.

13.4 O que devo fazer se não conseguir ativar a 2FA?

Sintomas

- Na lista de 2FA, não há servidores com a 2FA desativada.
- Depois que a 2FA é ativada, ela não tem efeito.
- Falha ao ativar a 2FA.

Possíveis causas

- A proteção do servidor não está ativada.
- As configurações de 2FA não entraram em vigor. Depois que a 2FA é ativada, leva cerca de 5 minutos para as configurações entrarem em vigor.
- Para um servidor do Linux, **Key pair** é selecionado como o modo de logon.
- A 2FA entra em conflito com G01 ou 360 Guard (edição do servidor).
- O firewall de SELinux não está desativado.

Solução

Passo 1 Verifique se o HSS foi ativado para o servidor para o qual você deseja usar a 2FA.

- Se sim, vá para **Passo 2**.
- Se não, ative o HSS primeiro.

Passo 2 Verifique se já se passaram 5 minutos desde que você ativou a 2FA.

- Se sim, vá para **Passo 3**.
- Se não, aguarde 5 minutos e verifique se a 2FA faz efeito.

Passo 3 Verifique se o seu servidor é um servidor do Linux com **Key pair** selecionado como seu modo de logon.

- Se sim, desative o modo de logon do **Key pair** e ative o modo de logon por **Password**.
- Se não, vá para **4**.

Passo 4 Verifique se o firewall do SELinux está desativado em seu servidor.

- Se sim, vá para **Passo 6**.
- Se não, execute um dos seguintes comandos para desativá-lo.
  - Para desativar temporariamente o firewall do SELinux, execute o seguinte comando:

    setenfore 0 #Temporarily disable
  - Para desativar permanentemente o firewall do SELinux, execute o seguinte comando:

    vi /etc/selinux config

    selinux=disabled #Permanently disable

Passo 5 Verifique se você interrompeu o G01 e o 360 Guard (edição do servidor) (se houver) em seu servidor.

- Se sim, vá para **Passo 6**.
- Se não, interrompa o software.

Passo 6 Entre em contato com o suporte técnico.

----Fim

13.5 Por que não consigo receber um código de verificação depois que a 2FA é ativada?

- A função de autenticação de dois fatores não entra em vigor imediatamente após ser ativada.

  Aguarde 5 minutos e tente novamente.
- Para habilitar a autenticação de dois fatores, você precisa desabilitar o firewall do SELinux.

  Desative o firewall do SELinux e tente novamente.
- Os servidores Linux exigem senhas de usuário para logon.

  Para alternar do modo de logon de chave para o modo de logon de senha, execute as seguintes etapas:

  a. Use a chave para fazer logon no ECS de Linux e definir a senha do usuário **root**.

     sudo passwd root

     Se o arquivo de chave for perdido ou danificado, redefina a senha do usuário **root**.

  b. Modifique o arquivo de configuração SSH no ECS como usuário **root**.

     su root

     vi /etc/ssh/sshd_config

     Modifique as seguintes configurações:

     - Altere **PasswordAuthentication no** para **PasswordAuthentication yes**.

Como alternativa, exclua a tag de comentário (#) antes do **PasswordAuthentication yes**.

- Altere **PermitRootLogin no** para **PermitRootLogin yes**.

  Como alternativa, exclua a tag de comentário (#) antes do **PermitRootLogin yes**.

c. Reinicie o sshd para que a modificação tenha efeito.

service sshd restart

d. Reinicie o ECS. Em seguida, você pode fazer logon no ECS como usuário **root** usando a senha.

NOTA

Para impedir que usuários não autorizados usem o arquivo de chave para acessar o ECS do Linux, exclua o arquivo **/root/.ssh/authorized_keys** ou limpe o arquivo **authorized_keys**.

13.6 Por que meu logon falha depois de ativar a 2FA?

O logon falhou provavelmente porque as configurações de arquivo ou o modo de logon estavam incorretos.

Corrigir configurações de arquivo

Verifique se o arquivo de configuração está correto.

Caminho do arquivo de configuração: **/etc/ssh/sshd_config**

Itens de configuração:

PermitEmptyPasswords no

UsePAM yes

ChallengeResponseAuthentication yes

AVISO

Se você usar a conta **root** para logon, o seguinte item de configuração é necessário:

PermitRootLogin yes

Corrigir o modo de logon

Se você tentar fazer logon em uma das seguintes maneiras, seu logon falhará.

- Usou o CloudShell para fazer logon em um ECS.
- Tentativa de fazer logon em um servidor Linux por meio de uma instância de CBH.

Causa da falha: a 2FA é implementada por meio de um módulo integrado, que não pode ser exibido se você fizer logon das maneiras anteriores. Como resultado, a autenticação de logon falha.

Solução: execute a autenticação de logon consultando **Como usar a 2FA?**

NOTA

Para obter detalhes sobre os pré-requisitos, restrições e limitações para ativar a 2FA, consulte "Ativação de 2FA" em **Configuração de segurança**.

13.7 Como adicionar um número de telefone celular ou endereço de e-mail para receber notificações de verificação de 2FA?

Você pode definir o seu número de telefone celular somente se tiver selecionado **SMS/Email** para **Method**. Defina o seu número de telefone celular no tópico de SMN que escolher.

Na lista suspensa **SMN Topic**, apenas os tópicos de SMN com assinaturas confirmadas são exibidos.

- Você pode clicar em **View** para ir para o console do SMN e criar um tópico. Clique em **Add Subscription** e digite um número de telefone celular ou endereço de e-mail.
- Você também pode adicionar ou modificar o número de telefone celular ou endereço de e-mail sob um tópico existente.
  - Adicionar um número de telefone celular ou endereço de e-mail

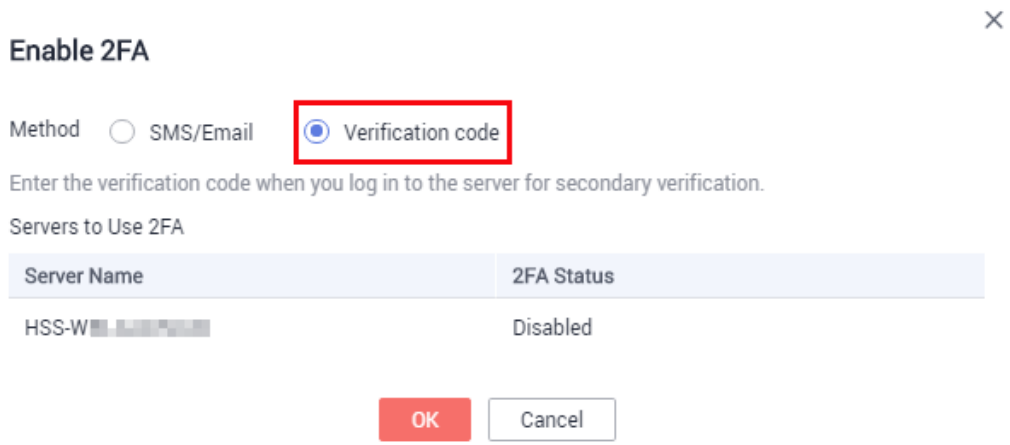
    Clique em **View Topics**. Clique em **Add Subscription** e digite um número de telefone celular ou endereço de e-mail.
  - Excluir um número de telefone celular ou endereço de e-mail

    Clique em **View Topics**. Clique no nome de um tópico para ir para a página de detalhes. Clique na guia **Subscriptions** e exclua um ou mais pontos de extremidade de destino.

13.8 Se optar por usar o código de verificação para 2FA, como obter o código?

Se quiser ativar a 2FA, mas não puder receber mensagens por telefone celular ou e-mail, defina **Method** como **Verification code**. Toda vez que você fizer logon em um ECS, o HSS enviará um código de verificação aleatório para sua página de logon. Você só precisa digitar o código para fazer logon.

Figura 13-8 Configuração do método para código de verificação



13.9 Serei cobrado por notificações de alarme e SMS?

Sim. Simple Message Notification (SMN) é um serviço pago. Para obter detalhes sobre preços, consulte **Detalhes do preço de SMN**.

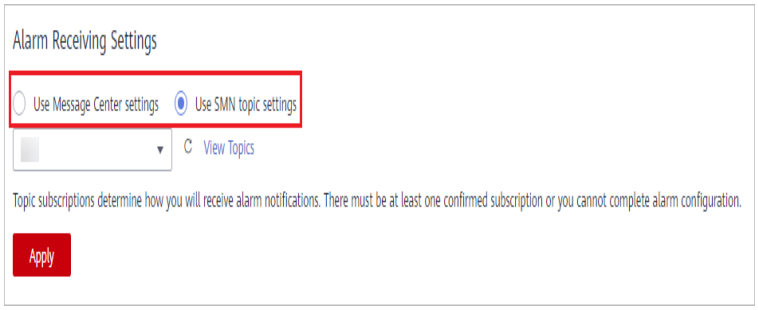
13.10 Como modificar destinatários de notificação de alarme?

Os destinatários podem receber notificações de alarme via SMS ou e-mail.

Você pode configurar as informações do destinatário em:

- **Configurações da Central de mensagens**
- **Tópicos de SMN**

Figura 13-9 Configurações de recepção de alarme



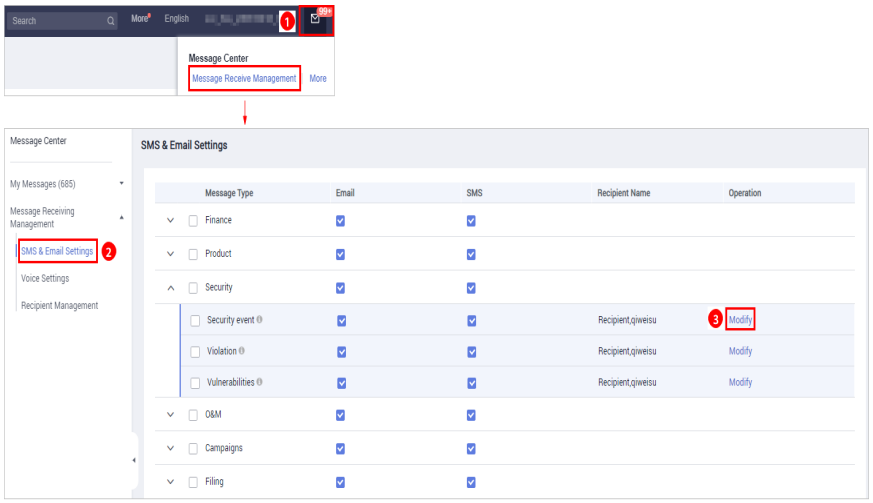
Configurações da Central de mensagens

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 Vá para a Central de mensagens. Adicione ou altere o endereço de e-mail e o número de celular do destinatário na Central de mensagens.

Vá para a Central de mensagens e escolha **Message Receiving Management** > **SMS & Email Settings**. Na área **Security**, clique em **Modify** na linha onde reside **Security event**.

Figura 13-10 Adicionar ou modificar um destinatário de notificação de alarme



Passo 3 Na caixa de diálogo **Modify Recipient**, selecione ou desmarque os contatos e clique em **OK**.

----Fim

Tópicos de SMN

Para alterar um ponto de extremidade de assinatura (um endereço de e-mail ou número de celular), exclua-o e adicione um novo.

O procedimento a seguir altera **test@example.com** para outro endereço no tópico de **HSS-warning**.

Pré-requisito

Você obteve a permissão de administrador de SMN.

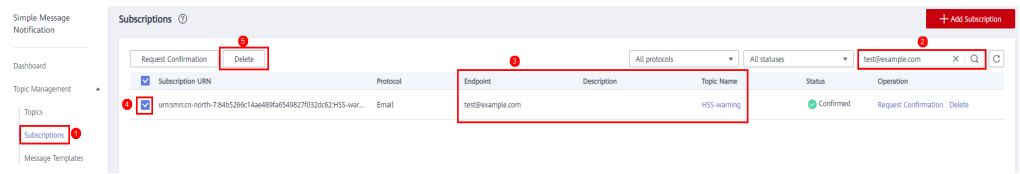
Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

Passo 2 No canto superior esquerdo, clique em ☰ e escolha **Application** > **Simple Message Notification**.

Passo 3 Escolha **Topic Management** > **Subscriptions** no painel de navegação. Digite o ponto de extremidade da assinatura na caixa de pesquisa, conforme mostrado na **Figura 13-11**.

Figura 13-11 Pesquisar o ponto de extremidade de assinatura anterior



Passo 4 Confirme que o ponto de extremidade da assinatura recebe notificações de alarme de HSS enviadas de SMN.

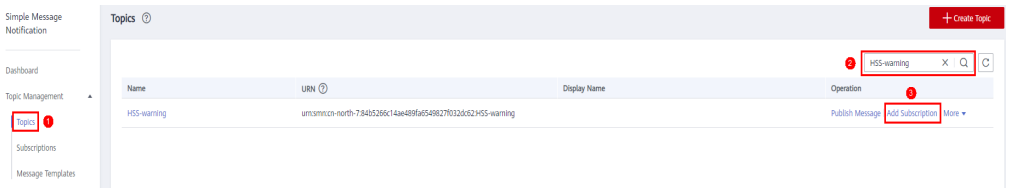
Passo 5 Clique em **Delete**.

NOTA

Depois que uma assinatura é excluída, o ponto de extremidade não recebe mais notificações de alarme de HSS. Tenha cuidado ao realizar esta operação.

Passo 6 Escolha **Topics**, pesquise o tópico desejado e adicione uma assinatura para ele. Para obter detalhes, consulte **Adição de uma assinatura** e **Solicitação de confirmação de assinatura**.

Figura 13-12 Adição de uma assinatura



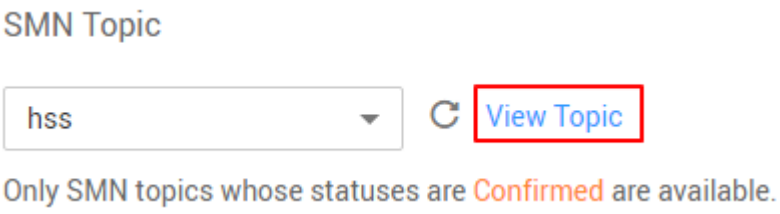
----Fim

13.11 Por que não há tópicos disponíveis para eu escolher quando configuro as notificações de alarme?

Nenhum tópico criado

Na página **Alarm Notifications**, clique em **View Topics** para acessar o console de SMN e criar um tópico. Para obter detalhes, consulte **Criação de um tópico**.

Figura 13-13 Exibição de tópicos de SMN



Nenhum tópico assinado

Depois de criar um tópico, você precisa adicionar uma ou mais assinaturas ao tópico e confirmar as assinaturas conforme solicitado. Para obter detalhes, consulte **Adição de uma assinatura**.

13.12 Posso desativar as notificações de alarme de HSS?

Sim.

Se você não ativar as notificações de alarme, o HSS não poderá enviar notificações de alarme para você em tempo hábil. Para exibir os riscos de segurança do host, você só pode fazer logon no console de gerenciamento.

Configurar notificações de alarme

Depois de habilitar o HSS, execute as seguintes operações para configurar as notificações de alarme:

1. Faça logon no console de HSS.
2. Escolha **Installation and Configuration** > **Alarm Notifications**. Configure notificações de alarme.

Desativação de notificações de alarme

Se você não quiser receber notificações de alarme do HSS depois que o HSS for ativado, você pode desabilitar a notificação. Depois de desabilitado, você precisa fazer logon no console de gerenciamento para visualizar os alarmes.

Utilize um dos seguintes métodos para desativar a notificação de alarme do HSS:

- Exclua o tópico de SMN.

  Depois de excluir o tópico, suas configurações de notificação de alarme não terão efeito.
- Exclua a assinatura do tópico de SMN.

  Depois de excluir a assinatura, você não receberá mais notificações de alarme.
- Cancele ou desative a assinatura do tópico de SMN.

  Depois de cancelar a assinatura, você não receberá mais notificações de alarme.

13.13 Como modificar itens de notificação de alarme?

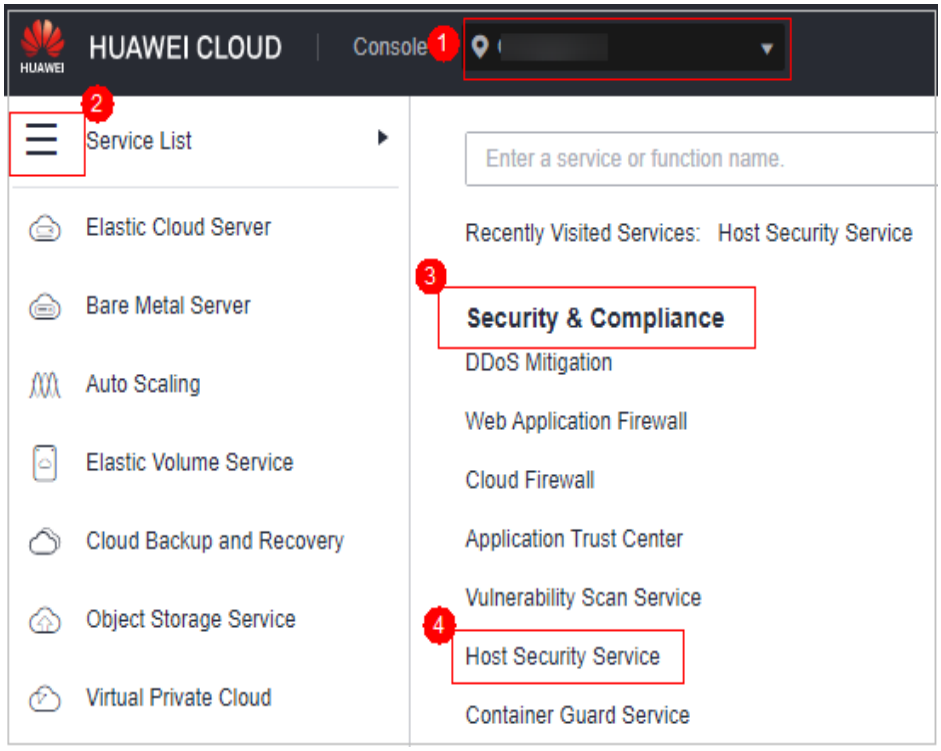
Se você não quiser receber determinadas notificações de alarme do HSS depois que o HSS estiver ativado, você pode desativar os itens de notificação. Depois de desativado, é necessário efetuar logon no console de gerenciamento para visualizar os alarmes.

Procedimento

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 13-14 Acessar o HSS



Passo 3 No painel de navegação, escolha **Installation and Configuration**.

Passo 4 Na página exibida, clique na guia **Alarm Notifications**.

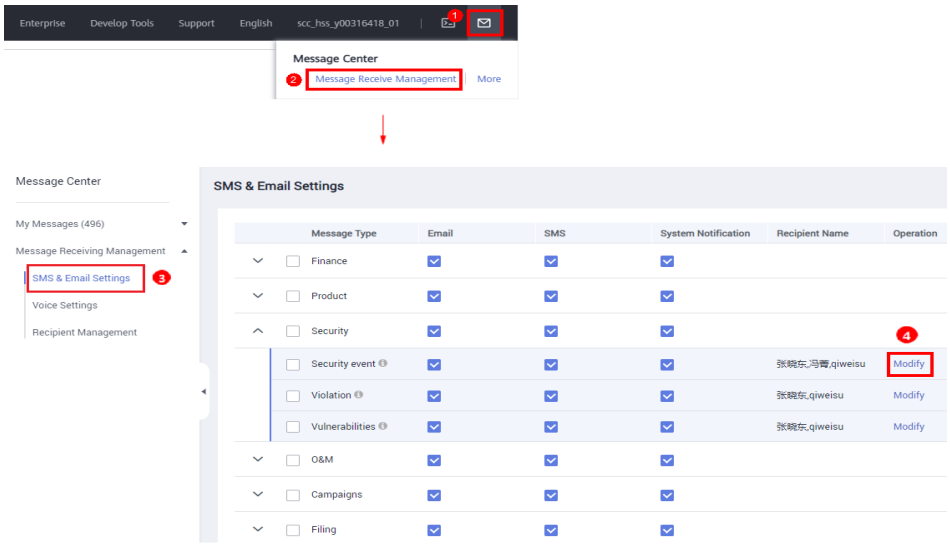
Passo 5 Selecione os eventos cujas notificações de alarme devem ser mascaradas. Para obter mais informações, consulte **Ativação da notificação de alarme**.

Passo 6 Clique em **Use Message Center settings** ou **Use SMN topic settings**.

- Se você clicar em **Use Message Center settings**,

  Vá para a Central de mensagens e escolha **Message Receiving Management** > **SMS & Email Settings**. Na área **Security**, clique em **Modify** na linha onde reside **Security event**.

Figura 13-15 Adição ou modificação de destinatários



- Se você clicar em **Use SMN topic settings**, selecione um tópico na lista suspensa.

Passo 7 Clique em **Apply**. Será exibida uma mensagem indicando que a notificação de alarme foi definida com sucesso.

Para modificar vários tópicos de notificação, repita as etapas de **Passo 5** a **Passo 7**.

----Fim

13.14 Como desativar o firewall do SELinux?

O SELinux (Linux com segurança aprimorada) é um módulo do kernel e subsistema de segurança do Linux.

O SELinux minimiza os recursos que podem ser acessados pelos processos de serviço no sistema (o princípio do mínimo privilégio).

Descrição do fechamento

- Depois que o SELinux é desativado, os serviços não são afetados.
- O SELinux pode ser desativado temporária ou permanentemente, conforme necessário.

Cenário

Para usar a função de autenticação de dois fatores do HSS, você precisa desativar permanentemente o firewall do SELinux.

Procedimento

Passo 1 Efetue logon remotamente no servidor de destino.

- **Servidor da Huawei Cloud**
  - Efetue logon no console do ECS, localize o servidor de destino e clique em **Remote Login** na coluna **Operation** para efetuar logon no servidor. Para obter detalhes, consulte **Fazer logon usando VNC**.

- **Servidor não da Huawei Cloud**

  Use uma ferramenta de gerenciamento remoto (como PuTTY ou Xshell) para se conectar ao EIP de seu servidor e fazer logon remotamente em seu servidor.

Passo 2 Execute o comando de desligamento na janela de comando.

- **Desativar temporariamente o SELinux**

  Execute o seguinte comando na CLI para desativar temporariamente o SELinux:

  ```
  setenforce 0
  ```

  NOTA

  Depois que o sistema for reiniciado, o SELinux será ativado novamente.

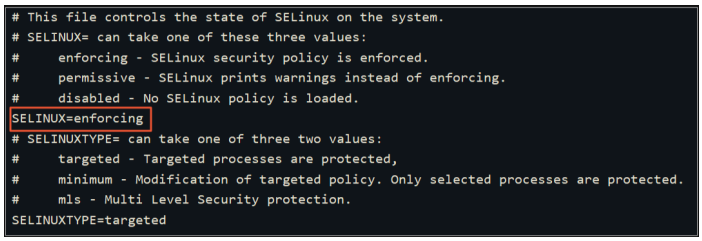
- **Desativar permanentemente o SELinux**

  a. Execute o seguinte comando na janela do diretório para editar o arquivo **config** do SELinux:

  ```
  vi /etc/selinux/config
  ```

  b. Localize **SELINUX=enforcing**, pressione **i** para entrar no modo de edição e altere o parâmetro para **SELINUX=disabled**.

  Figura 13-16 Editar o status do SELinux

  c. Após a modificação, pressione **Esc** e execute o seguinte comando para salvar o arquivo e sair:

  ```
  :wq
  ```

Passo 3 Execute o comando de desligamento permanente, salve as configurações e saia. Execute o seguinte comando para reiniciar o servidor imediatamente:

```
shutdown -r now
```

NOTA

O comando de desligamento permanente só tem efeito depois que o servidor é reiniciado.

Passo 4 Após a reinicialização, execute o seguinte comando para verificar se o SELinux está desativado:

```
getenforce
```

----Fim

14 Cotas

14.1 Como estender o período de validade das cotas do HSS?

A maneira de aumentar a cota de HSS varia de acordo com o modo de cobrança.

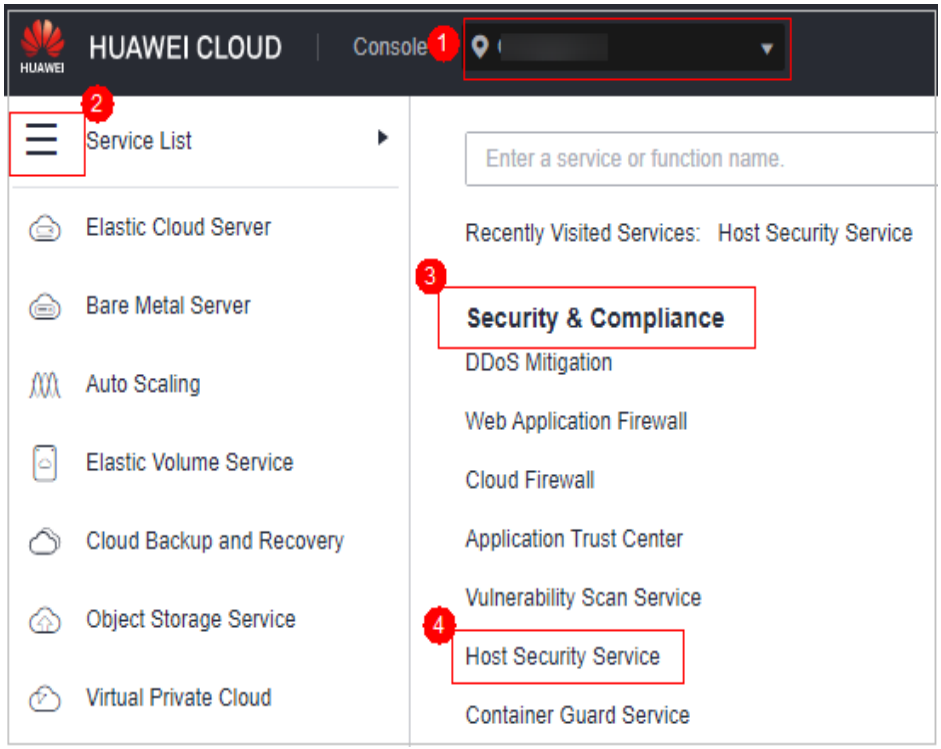
- No modo de pagamento por uso, você não precisa estender o período de validade. Você pode usar quantos recursos do HSS forem necessários por qualquer período e será cobrado por uso.
- No modo anual/mensal, sua cota tem um determinado período de validade. Antes que a cota expire, você pode **renovar** a cota.

14.2 Como filtrar servidores desprotegidos?

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

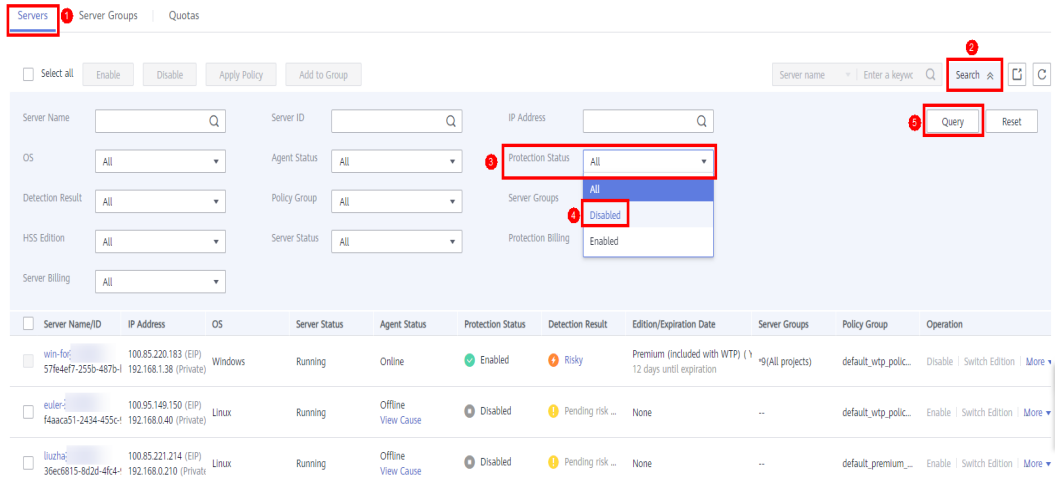
Figura 14-1 Acessar o HSS



Passo 3 No painel de navegação, selecione **Servers**.

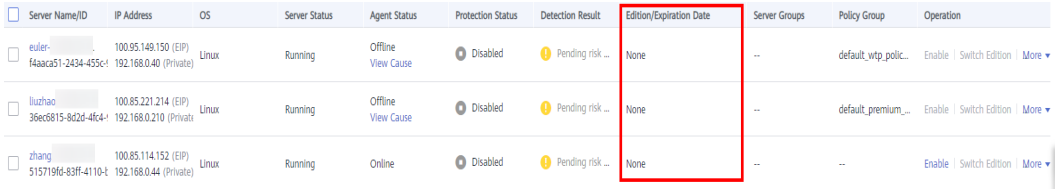
Passo 4 Na guia **Servers**, filtre servidores desprotegidos.

Figura 14-2 Filtragem de servidores desprotegidos



Passo 5 Verifique os servidores desprotegidos.

Figura 14-3 Servidores desprotegidos



----Fim

14.3 Por que não consigo encontrar os servidores que comprei no console?

Você provavelmente está na região errada. Somente os seguintes servidores são exibidos no console:

- Servidores da Huawei Cloud comprados na região selecionada
- Servidores não da Huawei Cloud que foram adicionados à região selecionada

Solução:

Alterne para a região correta antes de procurar seus servidores. Se as funções de projeto empresarial tiverem sido ativadas para sua conta, você também precisará garantir que tenha alternado para o projeto correto.

14.4 O que devo fazer se minhas cotas forem insuficientes e eu falhar em ativar a proteção?

Nenhuma cota comprada

Se você não tiver cotas suficientes, compre cotas na região em que os servidores estão implementados. Para obter detalhes, consulte **Compra de cotas de HSS**.

Verificar sua região

Sua cota está disponível apenas na região onde você a comprou. Se você comprou cotas, mas não consegue encontrar nenhuma no console, mude para a região correta antes de ativar a proteção.

Verificar sua página

- Para ativar o HSS da edição básica, empresarial ou premium, escolha **Host Security Service** > **Servers** e ative-o na guia **Servers**.
- Se você comprou a edição WTP, no console do HSS, escolha **Prevention** > **Web Tamper Protection** e clique na guia **Server**.
- Se você comprou a edição de container, no console do HSS, escolha **Containers & Quota** e clique na guia **Servers**.

Verificar seu projeto

Se as funções de projeto empresarial tiverem sido ativadas para sua conta, sua cota estará disponível somente no projeto em que você a comprou. Se você comprou cotas, mas não consegue encontrar nenhuma no console, mude para o projeto correto antes de ativar a proteção.

14.5 Como alocar minha cota?

A cota pode ser alocada das seguintes maneiras:

- Selecione **Select a quota randomly.** para permitir que o sistema aloque a cota com a validade restante mais longa para o servidor.
- Selecione um ID de cota e atribua-o a um servidor.
- Habilite proteção para servidores em lotes. O sistema alocará automaticamente cotas para eles.

NOTA

Geralmente, você pode deixar o HSS selecionar aleatoriamente uma cota.

14.6 Se eu mudar o SO de um servidor protegido, isso afetará minha cota de HSS?

Não. Mas antes de alterar o SO do servidor, você precisa verificar se o agente do HSS suporta o novo SO. Para obter uma melhor experiência de serviço HSS, é aconselhável instalar ou atualizar para uma versão do SO suportada pelo agente.

Os agentes do HSS podem ser executados em servidores do Linux, como CentOS e EulerOS; e servidores do Windows, como Windows 2012 e 2016.

AVISO

O agente é provavelmente incompatível com as versões de Linux ou Windows que atingiram o fim da vida útil. Para obter uma melhor experiência de serviço HSS, é aconselhável instalar ou atualizar para uma versão do SO suportada pelo agente.

Tabela 14-1 SOs suportados

Tipo de SO	Arquitetura do sistema	Versão do SO suportada	Suporte para verificação de vulnerabilidades
Windows	X86	Windows 10 (64-bit) **NOTA** Somente o Huawei Cloud Workspace pode usar este sistema operacional.	×

Tipo de SO	Arquitetura do sistema	Versão do SO suportada	Suporte para verificação de vulnerabilidades
		Windows 11 (64-bit) **NOTA** Somente o Huawei Cloud Workspace pode usar este sistema operacional.	×
		Windows Server 2012 R2 Standard 64-bit English (40 GB)	√
		Windows Server 2012 R2 Standard 64-bit Chinese (40 GB)	√
		Windows Server 2012 R2 Datacenter 64-bit English (40 GB)	√
		Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB)	√
		Windows Server 2016 Standard 64-bit English (40 GB)	√
		Windows Server 2016 Standard 64-bit Chinese (40 GB)	√
		Windows Server 2016 Datacenter 64-bit English (40 GB)	√
		Windows Server 2016 Datacenter 64-bit Chinese (40 GB)	√
		Windows Server 2019 Datacenter 64-bit English (40 GB)	√
		Windows Server 2019 Datacenter 64-bit Chinese (40 GB)	√
Linux	X86	CentOS 7.4 (64-bit)	√
		CentOS 7.5 (64-bit)	√
		CentOS 7.6 (64-bit)	√
		CentOS 7.7 (64-bit)	√
		CentOS 7.8 (64-bit)	√
		CentOS 7.9 (64-bit)	√
		CentOS 8.0 (64-bit)	×
		CentOS 8.1 (64-bit)	×
		CentOS 8.2 (64-bit)	×

Tipo de SO	Arquitetura do sistema	Versão do SO suportada	Suporte para verificação de vulnerabilidades
		CentOS 8 (64-bit)	×
		CentOS 9 (64-bit)	×
		Debian 9 (64-bit)	√
		Debian 10 (64-bit)	√
		Debian 11.0.0 (64-bit)	√
		Debian 11.1.0 (64-bit)	√
		EulerOS 2.2 (64-bit)	√
		EulerOS 2.3 (64-bit)	√
		EulerOS 2.5 (64-bit)	√
		EulerOS 2.7 (64-bit)	×
		EulerOS 2.9 (64-bit)	√
		Fedora 28 (64-bit)	×
		Ubuntu 16.04 (64-bit)	√
		Ubuntu 18.04 (64-bit)	√
		Ubuntu 20.03 (64-bit)	×
		Ubuntu 20.04 (64-bit)	√
		Ubuntu 22.04 (64-bit)	×
		Red Hat 7.4 (64-bit)	×
		Red Hat 7.6 (64-bit)	×
		Red Hat 8.0 (64-bit)	×
		Red Hat 8.7 (64-bit)	×
		OpenEuler 20.03 LTS (64-bit)	×
		OpenEuler 22.03 SP3 (64-bit)	×
		OpenEuler 22.03 (64-bit)	×
		AlmaLinux 9.0 (64-bit)	×
		Rocky Linux 8.4 (64-bit)	×
		Rocky Linux 8.5 (64-bit)	×
		Rocky Linux 9.0 (64-bit)	×

Tipo de SO	Arquitetura do sistema	Versão do SO suportada	Suporte para verificação de vulnerabilidades
		HCE 2.0 (64-bit)	×
		SUSE 12 SP5 (64-bit)	√
		SUSE 15 SP2 (64-bit)	√
		SUSE 15.5 (64-bit)	√
	ARM	CentOS 7.4 (64-bit)	√
		CentOS 7.5 (64-bit)	√
		CentOS 7.6 (64-bit)	√
		CentOS 7.7 (64-bit)	√
		CentOS 7.8 (64-bit)	√
		CentOS 7.9 (64-bit)	√
		CentOS 8.0 (64-bit)	×
		CentOS 8.1 (64-bit)	×
		CentOS 8.2 (64-bit)	×
		CentOS 9 (64-bit)	×
		EulerOS 2.8 (64-bit)	√
		EulerOS 2.9 (64-bit)	√
		Fedora 29 (64-bit)	×
		Ubuntu 18 (64-bit)	×
		Kylin V7 (64-bit)	×
		Kylin V10 (64-bit)	√
		HCE 2.0 (64-bit)	×
		UnionTech OS V20 (64-bit)	√ (Edições E e D do servidor UOS V20)

14.7 Por que uma edição de HSS não entra em vigor após a compra?

Depois de comprar o HSS, você precisa executar as seguintes operações para que o HSS entre em vigor:

1. Instale um agente no servidor de destino. Após a instalação, o HSS pode monitorar o servidor e relatar alarmes. Se você instalou o agente, pule esta etapa. Para obter detalhes sobre como instalar agentes, consulte **Instalação de um agente**.
2. Vincule a cota de edição comprada ao servidor de destino. Após a vinculação, os recursos da edição serão ativados no servidor de destino. Para obter detalhes sobre como vincular uma cota para ativar o HSS, consulte **Ativação do HSS**. Para obter detalhes sobre como ativar a proteção de nó de container, consulte **Ativação da proteção do nó do container**.

Depois que a proteção estiver ativada, é aconselhável ativar a notificação de alarme, para que você possa receber notificações assim que os alarmes forem relatados. Você também é aconselhado a configurar os parâmetros de segurança para seus servidores.

14.8 Como alterar a edição da cota de proteção vinculada a um servidor?

Precauções

Você pode alternar para a edição empresarial, básica, profissional ou premium.

Para usar a WTP ou a edição de container, compre uma cota dessa edição e ative-a. Para obter detalhes, consulte **Compra de uma cota de HSS**.

Pré-requisitos

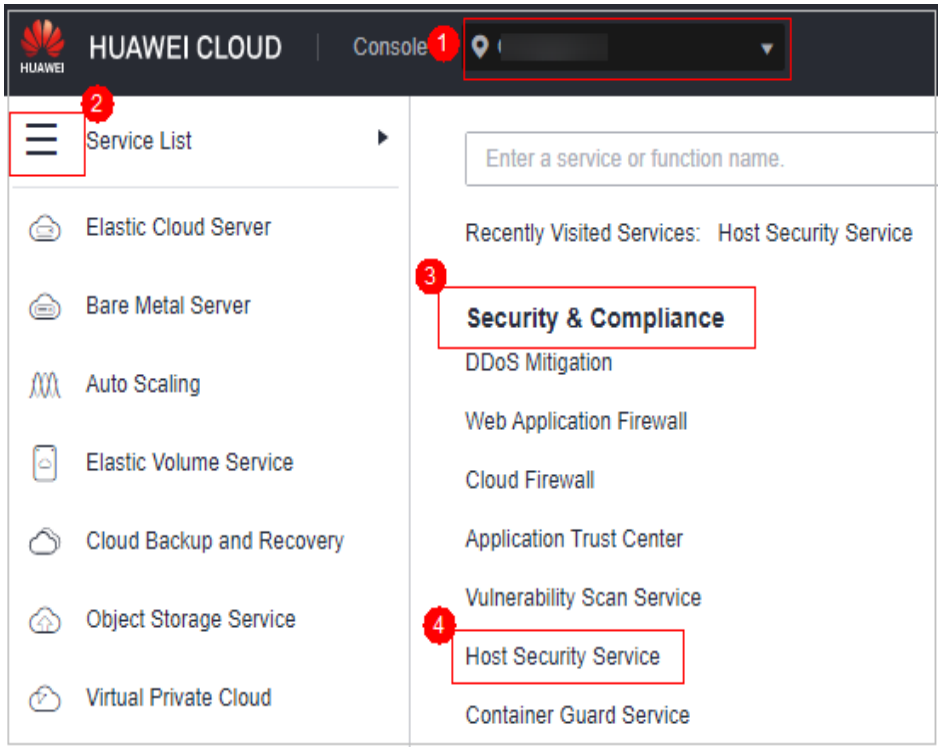
- O servidor cuja cota de proteção deve ser alterada está no estado **Protected**.
- Antes de mudar para uma quota no modo de cobrança anual/mensal, certifique-se de que a quota foi comprada e está disponível. Para obter detalhes, consulte **Compra de uma cota de HSS**.
- Antes de mudar para uma edição inferior, verifique o servidor, lide com os riscos conhecidos e registre as informações de operação para evitar erros e ataques de O&M.

Procedimento

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 14-4 Acessar o HSS



Passo 3 No painel de navegação, escolha **Asset Management** > **Servers & Quota**. Clique na guia **Servers**.

NOTA

A lista de servidores exibe o status de proteção somente dos seguintes servidores:

- Servidores da Huawei Cloud comprados na região selecionada
- Servidores não da Huawei Cloud que foram adicionados à região selecionada

Passo 4 Você pode alternar as edições de cota para um ou vários servidores.

- Alternação da edição de cota para um único servidor
  a. Na coluna **Operation** de um servidor, clique em **Switch Edition**.
  b. Na área **Configure Protection**, selecione um modo de cobrança, uma edição e uma cota. Para obter mais informações, consulte **Tabela 14-2**. Para obter detalhes sobre as edições que podem ser alteradas, consulte **Tabela 14-3**.

Tabela 14-2 Parâmetros para alternância de edições

Parâmetro	Descrição
Billing Mode	Modo de cobrança de uma cota. ■ Anual/Mensal ■ Pagamento por uso

Parâmetro	Descrição
Edition	Selecione uma edição de cota. ■ Edição básica: ela protege servidores de teste ou servidores de usuários individuais. **Ela pode proteger qualquer número de servidores, mas apenas parte dos recursos de verificação de segurança estão disponíveis**. **Esta edição não fornece recursos de proteção, nem fornece suporte para a certificação DJCP Multi-level Protection Scheme (MLPS)**. A edição básica é gratuita por 30 dias se tiver sido ativada pela primeira vez. ■ Edição profissional: esta edição é superior à edição básica, mas inferior à edição empresarial. Seus recursos incluem detecção de alteração de diretório de arquivos, detecção de shell anormal e gerenciamento de políticas. ■ Edição empresarial: ela fornece assistência para a certificação DJCP MLPS. Os principais recursos incluem gerenciamento de impressões digitais de ativos, gerenciamento de vulnerabilidades, detecção de programas maliciosos, detecção de shell da Web e detecção de comportamento anormal de processos. ■ Edição premium: ela ajuda você com a certificação DJCP MLPS e fornece recursos avançados, incluindo proteção de aplicações, prevenção de ransomware, detecção de comandos de alto risco, detecção de escalonamento de privilégios e detecção de shell anormal. Para obter mais informações, consulte **Edições e recursos**.
Select Quota	Se você selecionar **Yearly/Monthly**, será necessário selecionar uma cota de proteção para o servidor. ■ **Select a quota randomly**: uma cota aleatória é alocada ao servidor. ■ ID da cota: a cota especificada é vinculada ao servidor. Quando você alterna a edição para vários servidores por vez, a cota selecionada só pode ser vinculada a um deles. O resto dos servidores serão aleatoriamente vinculados às cotas da edição de destino. **NOTA** Se o sistema exibir uma mensagem indicando que não há cotas disponíveis, você precisará comprar cotas primeiro.
Tags (opcional)	Se você selecionar o modo de cobrança de pagamento por uso, poderá adicionar tags às cotas de pagamento por uso. As tags são usadas para identificar os recursos em nuvem. Quando você tem muitos recursos em nuvem do mesmo tipo, pode usar tags para classificar os recursos em nuvem por dimensão (por exemplo, por uso, proprietário ou ambiente).

Tabela 14-3 Alteração de edição permitida

Modo de cobrança	Edição atual	Edição de destino permitida
Anual/ Mensal	Básica	■ Anual/mensal: edições profissional, empresarial e premium ■ Pagamento por uso: edição empresarial
	Edição profissional	■ Anual/mensal: edições básica, empresarial e premium ■ Pagamento por uso: edição empresarial
	Empresarial	Anual/mensal: edições básica, profissional e premium
	Premium	■ Anual/mensal: edições básica, profissional e empresarial ■ Pagamento por uso: edição empresarial
Pagamento por uso	Empresarial	Anual/mensal: edições básica, profissional e premium

c. Leia o *Aviso de isenção de responsabilidade do Host Security Service* e selecione **I have read and agree to the Host Security Service Disclaimer**.

- Alternação das edições de cota para vários servidores

a. Selecione vários servidores e clique em **Enable** acima da lista de servidores.

b. Na caixa de diálogo exibida, confirme as informações do servidor e selecione um modo de cobrança, uma edição e uma cota. Para obter mais informações, consulte **Tabela 14-2**.

c. Leia o *Aviso de isenção de responsabilidade do Host Security Service* e selecione **I have read and agree to the Host Security Service Disclaimer**.

Passo 5 Clique em **OK**.

As informações da edição na coluna **Edition** serão atualizadas. Se as informações de edição na coluna **Edition** forem atualizadas, a alteração de edição foi bem-sucedida.

----Fim

Procedimento de acompanhamento

- Depois que a edição é alterada, você pode alocar a cota de edição ociosa para outros servidores.
- Depois de mudar para uma edição inferior, limpe dados importantes no servidor, interrompa aplicações importantes no servidor e desconecte o servidor da rede externa para evitar perdas desnecessárias causadas por ataques.

- Depois de mudar para uma edição superior, execute uma detecção de segurança no servidor, lide com os riscos de segurança no servidor e configure as funções necessárias em tempo hábil.

15 Cobrança, renovação e cancelamento de assinatura

15.1 Se eu não renovar o HSS após ele expirar, meus serviços serão afetados?

A expiração do HSS não tem impacto direto em seus serviços.

Impacto da interrupção da renovação

HSS vai parar de proteger seus serviços se a sua assinatura do HSS expira.

Riscos depois de interromper a renovação

A edição básica do HSS não oferece funções avançadas de proteção. Se você não renovar sua assinatura, seus servidores estarão expostos aos riscos de quebra de contas, intrusões e violações de dados, o que pode causar grandes prejuízos para o seu negócio empresarial.

O HSS fornece proteção completa para servidores, incluindo prevenção pré-ataque, proteção durante ataque e alarmes em tempo real ou diários. Para obter mais informações, consulte **HSS**.

15.2 Se eu cancelar a assinatura do HSS e comprá-lo novamente, preciso instalar agentes e definir as configurações de proteção do servidor do zero?

Não.

Se você cancelar a assinatura do HSS, sua cota do HSS não estará mais disponível. O HSS não desinstala automaticamente o agente de seus servidores nem modifica ou exclui as configurações de proteção de servidor em seus servidores.

AVISO

O HSS não pode ser usado entre regiões. Certifique-se de que as novas cotas compradas estejam nas mesmas regiões que as cotas anteriores.

15.3 Como renovar o HSS?

Você pode renovar sua assinatura de uma instância do HSS cobrada anualmente/mensalmente quando ela estiver prestes a expirar. Após a renovação, você poderá continuar a usar o HSS.

- Antes que o serviço expire, o sistema enviará uma mensagem SMS ou e-mail para lembrá-lo de renová-lo.
- Se você não renovar o serviço antes que ele expire, ele entrará no período de retenção. No período de retenção, o HSS não protegerá mais seus servidores, mas as configurações relacionadas ao HSS serão mantidas. Quando o período de retenção expirar, as configurações relacionadas ao HSS serão excluídas. Para obter mais informações, consulte **Período de retenção**.

Para evitar perdas desnecessárias causadas por problemas de segurança, renove sua assinatura em tempo hábil.

NOTA

- Se você selecionou **Auto-renew** ao comprar o HSS, o sistema gera automaticamente um pedido de renovação e renova sua assinatura antes que ela expire.
- Se você usar uma conta de membro, conceda a permissão BSS Administrator a ela para que você possa renovar a assinatura expirada usando esta conta de membro.

Pré-requisito

Você obteve as permissões BSS Administrator e HSS Administrator e suas senhas.

NOTA

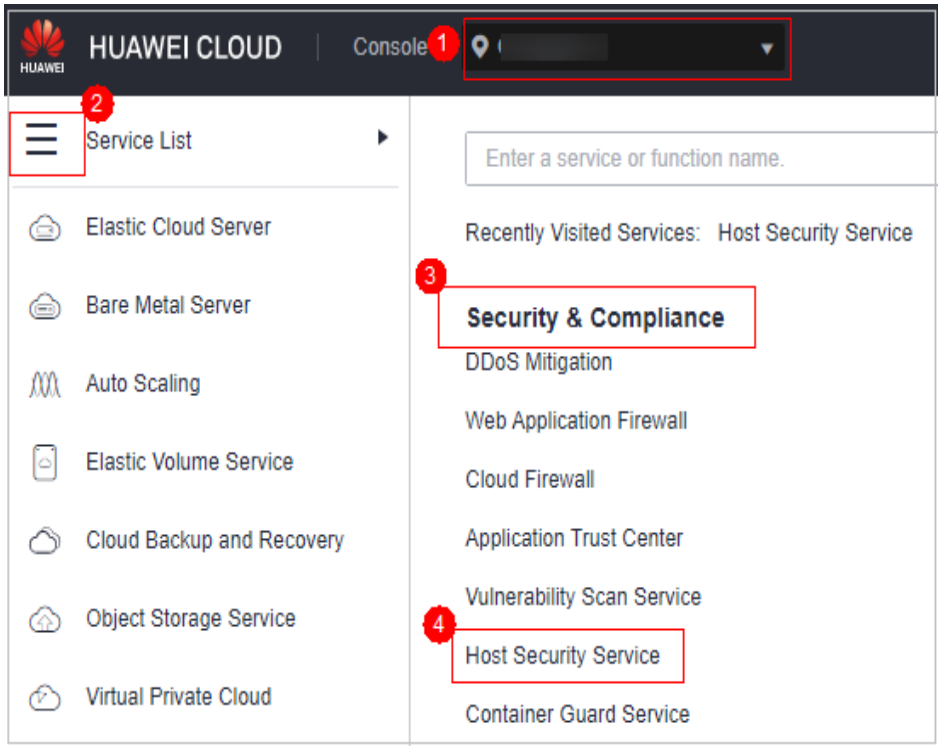
Uma conta com a permissão **BSS Administrator** pode executar qualquer operação em todos os itens de menu na central de contas, na central de cobrança e na central de recursos.

Renovação manual

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 15-1 Acessar o HSS



Passo 3 Renove cotas diferentes.

- **Renovar cotas de servidor**:
  a. No painel de navegação à esquerda, escolha **Asset Management** > **Servers & Quota**. Clique na guia **Quotas**. A página de lista de cotas de proteção é exibida.
  b. Na coluna **Operation** da cota que você deseja renovar, clique em **More** > **Renew**.
     Você também pode selecionar todas as cotas a serem renovadas e clicar em **Batch Renew** no canto superior esquerdo da lista de cotas para renová-las em lotes.
  c. Na página **Renew**, conclua a renovação conforme solicitado.
     Para obter detalhes, consulte **Renovação manual de um recurso**.
- **Renovar cotas de containers**:
  a. No painel de navegação à esquerda, escolha **Asset Management** > **Containers & Quota**. Clique na guia **Protection Quotas**. A página de lista de cotas de proteção é exibida.
  b. Na coluna **Operation** da cota que você deseja renovar, clique em **More** > **Renew**.
     Você também pode selecionar todas as cotas a serem renovadas e clicar em **Batch Renew** no canto superior esquerdo da lista de cotas para renová-las em lotes.
  c. Na página **Renew**, conclua a renovação conforme solicitado.
     Para obter detalhes, consulte **Renovação manual de um recurso**.

----Fim

Renovação automática

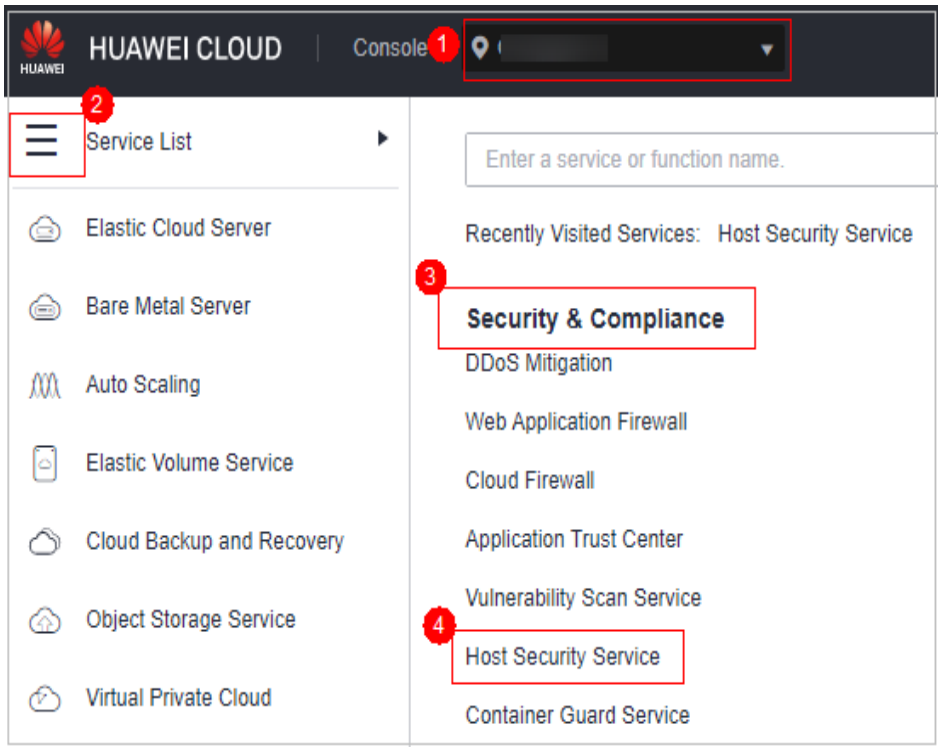
Se você selecionou **Auto-renew** ao comprar o HSS, o sistema gera automaticamente um pedido de renovação e renova sua assinatura antes que ela expire.

Se você não selecionou **Auto-renew** ao comprar o HSS, poderá executar as seguintes etapas para ativar a função de renovação automática:

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 15-2 Acessar o HSS



Passo 3 Ative a função de renovação automática para diferentes tipos de cotas.

- **Ativar a renovação automática para cotas de servidor**:
  a. No painel de navegação à esquerda, escolha **Asset Management** > **Servers & Quota**. Clique na guia **Quotas**. A página de lista de cotas de proteção é exibida.
  b. Na coluna **Operation** da cota que você deseja renovar, clique em **More** > **Enable Auto-Renewal**.

     Você também pode selecionar todas as cotas a serem renovadas e clicar em **Enable Auto-Renewal** no canto superior esquerdo da lista de cotas para ativar a renovação automática em lotes.
  c. Na página **Enable Auto-Renew**, confirme o nome da cota para a qual você deseja ativar a renovação automática e selecione a duração e o número de vezes das renovações automáticas.
  d. Clique em **OK**.
- **Ativar a renovação automática para cotas de container**:
  a. No painel de navegação à esquerda, escolha **Asset Management** > **Containers & Quota**. Clique na guia **Protection Quotas**. A página de lista de cotas de proteção é exibida.

b. Na coluna **Operation** da cota que você deseja renovar, clique em **More** > **Enable Auto-Renewal**.

   Você também pode selecionar todas as cotas a serem renovadas e clicar em **Enable Auto-Renew** no canto superior esquerdo da lista de cotas para ativar a renovação automática em lotes.

c. Na página **Enable Auto-Renew**, confirme o nome da cota para a qual você deseja ativar a renovação automática e selecione a duração e o número de vezes das renovações automáticas.

d. Clique em **OK**.

----Fim

15.4 Como cancelar a assinatura das cotas de HSS?

Se algumas de suas cotas do HSS forem desnecessárias e você quiser parar de cobrar por elas, poderá cancelar a assinatura delas.

Você pode cancelar a assinatura das cotas do HSS cobradas no modo anual/mensal. Após o cancelamento da assinatura, o valor que você não consumiu será reembolsado. Para obter detalhes, consulte **Cancelar assinatura de cotas do HSS cobradas no modo anual/mensal**.

A cota do HSS de pagamento por uso é cobrada com base na duração de uso real. Depois que o HSS for desativado, você não será cobrado. Para obter detalhes, consulte **Desativação de cotas do HSS cobradas no modo de pagamento por uso**.

NOTA

Se você usa uma conta de membro, conceda a permissão BSS Administrator a ela para que possa cancelar a assinatura do HSS usando essa conta de membro.

Cancelar assinatura de cotas do HSS cobradas no modo anual/mensal

Você pode cancelar a assinatura das cotas do HSS cobradas no modo anual/mensal.

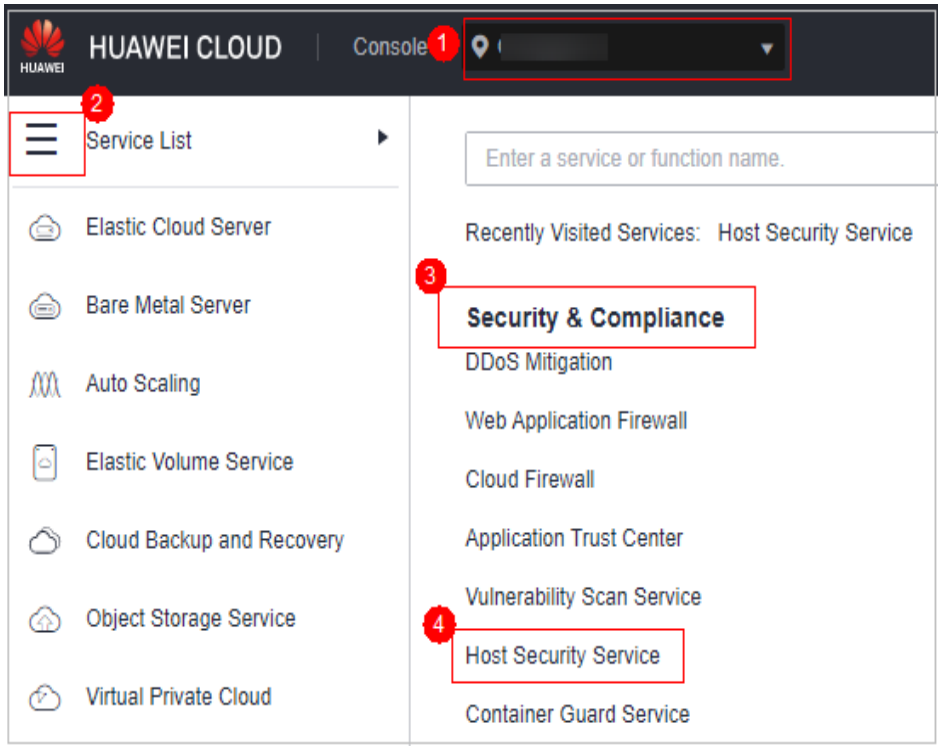
- Se você tiver cancelado a assinatura de menos de 10 recursos no ano atual, poderá obter o reembolso total ao cancelar a assinatura de uma cota comprada dentro de cinco dias (excluindo as cotas cujos pedidos não são pagos).
- Se você cancelar a assinatura de uma cota depois de cinco dias após a compra, serão cobradas as taxas de manuseio e o valor consumido. Os cupons de dinheiro e cupons de desconto usados não serão reembolsados.

Para obter mais informações, consulte **Regras de cancelamento de assinatura**.

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 15-3 Acessar o HSS



Passo 3 Cancele a assinatura de diferentes tipos de cotas.

- **Cancelar a assinatura das cotas do servidor**:
  a. No painel de navegação à esquerda, escolha **Asset Management** > **Servers & Quota**. Clique na guia **Quotas**. A página de lista de cotas de proteção é exibida.
  b. Na coluna **Operation** da cota da qual você deseja cancelar a assinatura, clique em **More** > **Unsubscribe**.
  c. Na página exibida, conclua o cancelamento da assinatura conforme solicitado.
     Para obter detalhes, consulte **Regras de cancelamento de assinatura**.
- **Cancelar a assinatura de cotas de containers**:
  a. No painel de navegação à esquerda, escolha **Asset Management** > **Containers & Quota**. Clique na guia **Protection Quotas**. A página de lista de cotas de proteção é exibida.
  b. Na coluna **Operation** da cota da qual você deseja cancelar a assinatura, clique em **More** > **Unsubscribe**.
  c. Na página exibida, conclua o cancelamento da assinatura conforme solicitado.
     Para obter detalhes, consulte **Regras de cancelamento de assinatura**.

----Fim

Desativação de cotas do HSS cobradas no modo de pagamento por uso

Para cancelar a assinatura das cotas de edição empresarial ou de container compradas no modo de pagamento por uso, você só precisa desativar a proteção.

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 Clique em ☰ no canto superior esquerdo da página, selecione uma região e escolha **Security & Compliance** > HSS para ir para o console de gerenciamento do HSS.

Passo 3 Vá para a lista de proteção.

- Lista de proteção do servidor: no painel de navegação, escolha **Asset Management** > **Servers & Quota**. Clique na guia **Servers**.
- Lista da proteção do container: no painel de navegação, escolha **Asset Management** > **Container Management**. Clique na guia **Container Nodes** e clique em **Nodes**.

Passo 4 Na coluna **Operation** de um servidor, clique em **Disable** ou **Disable Protection**.

Passo 5 Na caixa de diálogo de confirmação, clique em **OK**.

Depois que a proteção for desativada, retorne à lista de proteção. O status de proteção do servidor ou container é **Unprotected**.

----Fim

15.5 Como desativar a renovação automática?

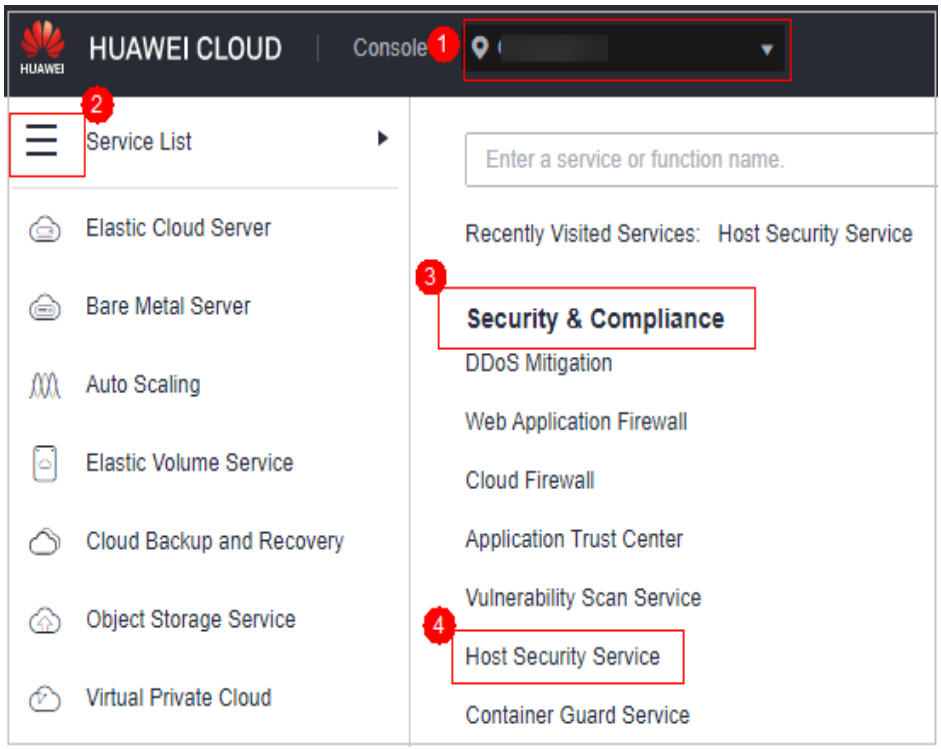
Você pode cancelar a renovação automática do HSS. Se a renovação automática for cancelada, você precisará **renovar manualmente** suas assinaturas.

Procedimento

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 15-4 Acessar o HSS



Passo 3 Cancele a renovação automática com base no tipo de cota.

- **Cancelar a renovação automática de cotas de servidor:**
  a. No painel de navegação à esquerda, escolha **Asset Management** > **Servers & Quota**. Clique na guia **Quotas**. A página de lista de cotas de proteção é exibida.
  b. Na linha de uma cota, escolha **More** > **Modify Auto-renew** na coluna **Operation**.
  c. Defina **Renewal Option** como **Manual**.
  d. Clique em **OK**.
- **Cancelar a renovação automática de cotas de containers:**
  a. No painel de navegação à esquerda, escolha **Asset Management** > **Containers & Quota**. Clique na guia **Protection Quotas**. A página de lista de cotas de proteção é exibida.
  b. Na linha de uma cota, escolha **More** > **Modify Auto-renew** na coluna **Operation**.
  c. Defina **Renewal Option** como **Manual**.
  d. Clique em **OK**.

----Fim

16 Outros

16.1 Como usar a ferramenta de conexão de área de trabalho remota do Windows para se conectar a um servidor?

Procedimento

Passo 1 No PC local, escolha **Startup** > **Running** e execute o comando **mstsc** para iniciar a Conexão de área de trabalho remota do Windows.

Passo 2 Clique em **Options** e, em seguida, clique na guia **Local Resources**. Na área **Local devices and resources**, selecione **Clipboard**.

Passo 3 Clique na guia **General**. Em **Computer**, insira o EIP do servidor no qual você deseja instalar um agente. Em **User name**, insira **Administrator**. Em seguida, clique em **Connect**.

Passo 4 Na caixa de diálogo exibida, digite a senha do usuário do servidor e clique em **OK** para se conectar ao servidor.

----Fim

16.2 Como verificar os arquivos de log do HSS?

Caminho do log

A tabela a seguir descreve os arquivos de log e seus caminhos.

SO	Diretório de log	Arquivo de log
Linux	/var/log/hostguard/	● hostwatch.log ● hostguard.log ● upgrade.log ● hostguard-service.log ● config_tool.log ● engine.log
Windows	C:\Program Files\HostGuard \log	● hostwatch.log ● hostguard.log ● upgrade.log

Retenção de log

Arquivo de log	Descrição	Tamanho máximo	Arquivo retido	Período de retenção
hostwatch.log	Registra logs gerados durante a execução de processos daemon.	10M	Últimos oito arquivos	Até que o agente do HSS seja desinstalado
hostguard.log	Registra os logs gerados durante a execução dos processos de trabalho.	10M	Últimos oito arquivos	
upgrade.log	Registra os logs gerados durante a atualização de versão.	10M	Últimos oito arquivos	
hostguard-service.log	Registra os logs (scripts) gerados quando o serviço é iniciado.	100k	Últimos dois logs	
config_tool.log	Registra os logs (programas) gerados quando o serviço é iniciado.	10M	Últimos dois logs	
engine.log	Registra os logs gerados quando o serviço é encerrado.	10M	Últimos dois logs	

16.3 Como ativar o registro em log para falhas de logon?

MySQL

A função de prevenção de invasão de contas para Linux é compatível com o MySQL 5.6 e 5.7. Execute as etapas a seguir para habilitar o log para falha de logon:

Passo 1 Efetue logon no host como o usuário **root**.

Passo 2 Execute o seguinte comando para consultar o valor **log_warnings**:

show global variables like 'log_warnings'

Passo 3 Execute o seguinte comando para alterar o valor **log_warnings**:

set global log_warnings=2

Passo 4 Modifique o arquivo de configuração.

- Para um sistema operacional Linux, modifique o arquivo **my.conf** adicionando **log_warnings=2** ao **[MySQLd]**.

----Fim

vsftp

Esta seção mostra como habilitar o registro em log para falhas de logon do vsftp.

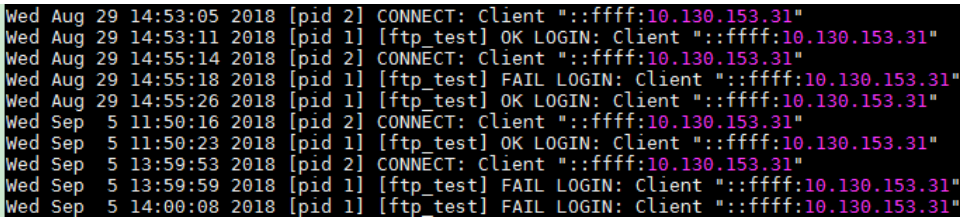
Passo 1 Modifique o arquivo de configuração (por exemplo, **/etc/vsftpd.conf**) e defina os seguintes parâmetros:

vsftpd_log_file=log/file/path

dual_log_enable=YES

Passo 2 Reinicie o serviço vsftp. Se a configuração for bem-sucedida, os registros de log mostrados nos logs mostrados em **Figura 16-1** serão retornados quando você fizer logon no vsftp.

Figura 16-1 Registros de log



----Fim

16.4 Como limpar um alarme em alterações de arquivos críticos?

Se você tiver certeza de que as alterações em seus arquivos críticos são seguras, você não precisa lidar com o alarme. Será automaticamente limpo em sete dias.

16.5 O HSS está disponível como software off-line?

Não.

16.6 Por que não consigo visualizar todos os projetos na lista suspensa do projeto empresarial?

Somente as contas com as permissões **Tenant Administrator** ou **HSS Administrator** +**Tenant Guest** podem selecionar **All projects**. Se sua conta não tiver as permissões necessárias, você não poderá visualizar todos os projetos empresariais. Para obter detalhes sobre como conceder permissões, consulte **Atribuição de permissões a um usuário do IAM**.

16.7 Como ativar a autoproteção do HSS?

A autoproteção do HSS protege arquivos, processos e software do HSS contra programas maliciosos, que podem desinstalar agentes do HSS, adulterar arquivos do HSS ou interromper processos do HSS.

Restrições

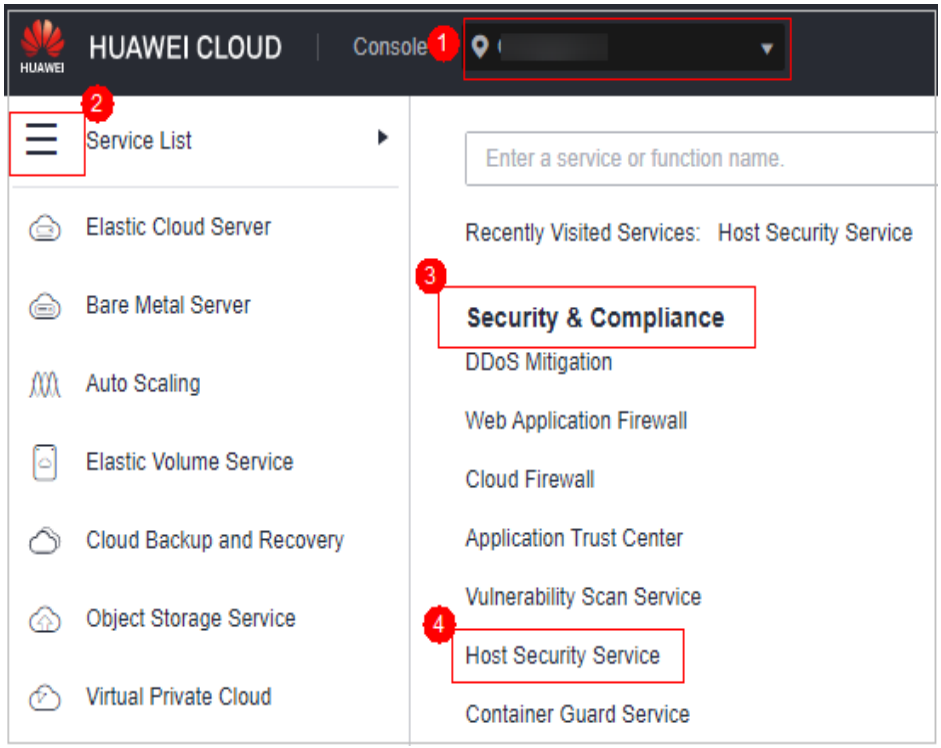
- A autoproteção do HSS é suportada apenas para servidores do Windows que ativaram a edição premium ou WTP do HSS.
- A autoproteção depende da detecção de antivírus, detecção de HIPS e proteção contra ransomware. Ela só entra em vigor quando mais de uma das três funções estiver ativada. Para mais detalhes, consulte:
  - **Ativação da prevenção contra ransomware**
  - A detecção de antivírus e a detecção de HIPS são ativadas por padrão. Se você desativar manualmente os dois itens de detecção, ative-os novamente consultando **Visualização de um grupo de políticas**.
- A ativação da política de autoproteção tem os seguintes impactos:
  - O agente do HSS não pode ser desinstalado no painel de controle de um servidor, mas pode ser desinstalado no console do HSS.
  - O processo do HSS não pode ser encerrado.
  - No caminho de instalação do agente **C:\Program Files\HostGuard**, você só pode acessar os diretórios **log** e **data** (e o diretório **upgrade**, se o seu agente tiver sido atualizado).

Procedimento

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 16-2 Acessar o HSS



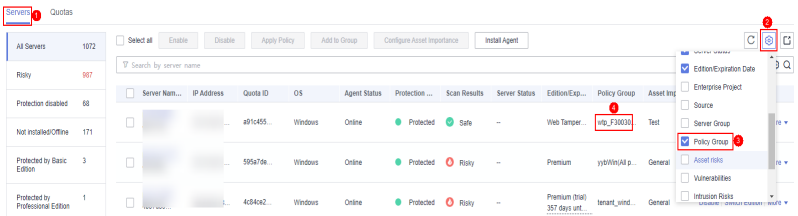
Passo 3 Na árvore de navegação à esquerda, escolha **Security Operations** > **Policies**

Passo 4 Clique no nome de um grupo de políticas da edição premium para servidores do Windows. A página de detalhes do grupo de políticas é exibida.

Selecione o grupo de políticas do servidor em que você deseja ativar a autoproteção.

- Se você não tiver criado nenhum grupo de políticas da edição premium, selecione o grupo de políticas padrão **tenant_windows_premium_default_policy_group**.
- Se você tiver criado grupos de políticas da edição premium, selecione o grupo de políticas do servidor. Realize as operações a seguir:
  a. Na árvore de navegação à esquerda, escolha **Asset Management** > **Servers & Quota**.
  b. Clique na guia **Servers** para exibir os grupos de políticas de servidores.

  Figura 16-3 Exibição dos grupos de políticas de servidores



Passo 5 Na linha que contém a política de autoproteção de destino, clique em **Enable** na coluna **Operation**.

Passo 6 Na caixa de diálogo Prompt exibida, clique em **OK**.

----Fim

Operações relacionadas

Desativar a autoproteção do HSS

Passo 1 Na linha que contém a política de autoproteção de destino, clique em **Disable** na coluna **Operation**.

Passo 2 Na caixa de diálogo exibida, clique em **OK**.

----Fim

16.8 O que fazer se a autoproteção do HSS não puder ser desativada?

Causa raiz

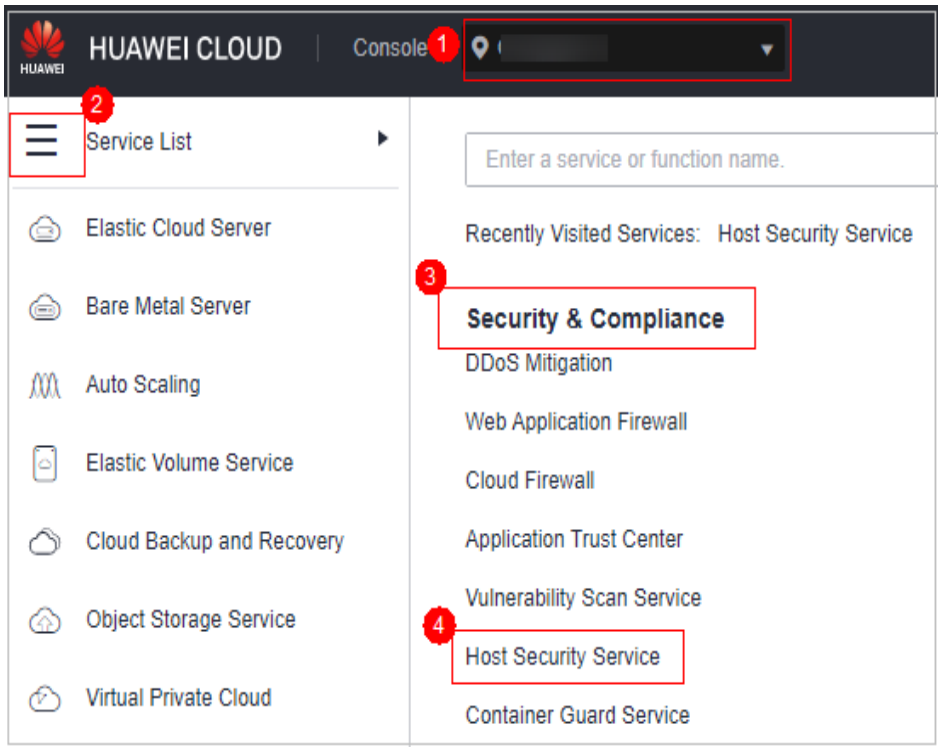
Se a rede do servidor for desconectada, os agentes não poderão receber o comando para desativar a autoproteção fornecido pelo console do HSS. Portanto, a autoproteção do HSS não pode ser desativada.

Soluções

Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

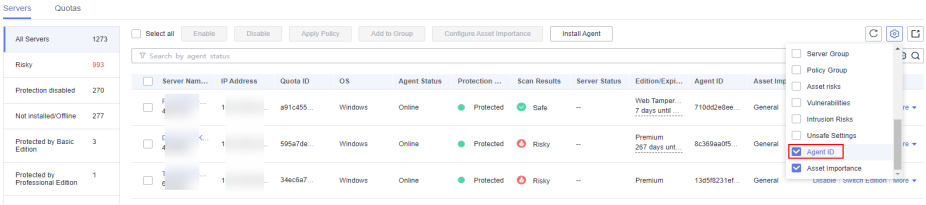
Figura 16-4 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Asset Management** > **Servers & Quota**.

Passo 4 Clique na guia **Servers**, clique em  no canto superior direito da lista de servidores e selecione **Agent ID**.

Figura 16-5 Exibição do ID do agente



Passo 5 Acima da lista de servidores, digite um nome ou ID de servidor e clique em  para procurar o servidor do Windows para o qual você deseja desativar a autoproteção do HSS.

Passo 6 Na linha do servidor do Windows de destino, copie os primeiros oito caracteres da coluna **Agent ID**.

Passo 7 Abra a CLI do servidor do Windows de destino.

Passo 8 Execute o seguinte comando para desativar a autoproteção do HSS:

"C:\Program Files\HostGuard\bin\HssClient.exe"1234abcd

NOTA

1234abcd no comando indica os primeiros oito caracteres do ID do agente. Os primeiros oito caracteres do ID do agente são usados como código de verificação quando **HSSClient.exe** é executado. É para evitar que programas maliciosos desativem a autoproteção e as operações incorretas do usuário. A autoproteção pode ser desativada somente quando os primeiros oito caracteres do ID do agente estiverem corretos.

Passo 9 Se **Disable self protect succeed.** for exibido, a autoproteção do HSS foi desativada com sucesso.

----Fim

16.9 Por que um ECS excluído ainda é exibido na lista de servidores do HSS?

Depois que um ECS é excluído, o HSS não sincroniza suas informações imediatamente. Portanto, você ainda pode ver o ECS excluído na lista de servidores do HSS.

O HSS inicia a sincronização imediatamente quando você acessa a página **Asset Management** > **Servers & Quota** e concluirá a sincronização em cerca de 10 minutos. Em seguida, você pode atualizar a página **Servers & Quota** e visualizar a lista de servidores mais recente.

A História de mudanças

Lançado em	Descrição
27/10/2023	Este é o décimo quarto lançamento oficial. Adição de: ● **Por que não consigo selecionar um servidor durante a verificação manual de vulnerabilidades?** ● **O que devo fazer se o plug-in de proteção de cluster de container falhar ao ser desinstalado?** ● **O que devo fazer se a atualização do agente falhar e a mensagem "File replacement failed" for exibida?**
27/09/2023	Este é o décimo terceiro lançamento oficial. Adição de: ● **O HSS pode ser usado entre contas?** ● **O que devo fazer se não conseguir acessar o link de download do agente do Windows?** ● **O que devo fazer se o HSS (novo) não gerar alarmes após uma atualização do HSS (anterior)?** ● **O que devo fazer se a correção da vulnerabilidade falhar?** ● **Como alterar a edição da cota de proteção vinculada a um servidor?** ● **Por que um ECS excluído ainda é exibido na lista de servidores do HSS?**
25/07/2023	Este é o décimo segundo lançamento oficial. Adição de: ● **Como ativar a autoproteção do HSS?** ● **O que fazer se a autoproteção do HSS não puder ser desativada?** ● **O que devo fazer se a porta do meu servidor remoto não for atualizada nos registros de ataques de força bruta?** ● **Como ativar a auditoria do servidor de API para um container do Kubernetes local?**

Lançado em	Descrição
19/07/2023	Este é o décimo primeiro lançamento oficial. Adição de: **Como desativar a renovação automática?** Otimização de: Adição de descrição sobre a atualização manual do agente para 2.0 em **Como atualizar o agente?**.
15/06/2023	Este é o décimo lançamento oficial. Adição de: ● **Por que não consigo visualizar todos os projetos na lista suspensa do projeto empresarial?**

Lançado em	Descrição
24/05/2023	Este é o nono lançamento oficial. Adição de: ● **O HSS está em conflito com qualquer outro software de segurança?** ● **É necessário instalar o agente do HSS após a compra do HSS?** ● **O que devo fazer se o HSS relatar alarmes de força bruta com frequência?** ● **Como lidar com alarmes sobre ataques de força bruta lançados a partir de um endereço IP da Huawei Cloud?** ● **Com que frequência o HSS detecta, isola e elimina programas maliciosos?** ● **O que devo fazer se um endereço IP for bloqueado pelo HSS?** ● **Como me defender contra ataques de ransomware?** ● **Posso verificar a vulnerabilidade e o histórico de correção de linha de base no HSS?** ● **Como desativar a proteção de nó?** ● **Como limpar a lista branca de endereços IP de logon SSH configurada no HSS?** ● **O que posso fazer se eu não posso fazer logon remotamente em um servidor via SSH?** ● **Como usar a 2FA?** ● **O que devo fazer se não conseguir ativar a 2FA?** ● **Por que não consigo receber um código de verificação depois que a 2FA é ativada?** ● **Por que meu logon falha depois de ativar a 2FA?** ● **Como adicionar um número de telefone celular ou endereço de e-mail para receber notificações de verificação de 2FA?** ● **Se optar por usar o código de verificação para 2FA, como obter o código?** ● **Como modificar destinatários de notificação de alarme?** ● **Por que não há tópicos disponíveis para eu escolher quando configuro as notificações de alarme?** ● **Posso desativar as notificações de alarme de HSS?** ● **Como modificar itens de notificação de alarme?** ● **Por que não consigo encontrar os servidores que comprei no console?** ● **O que devo fazer se minhas cotas forem insuficientes e eu falhar em ativar a proteção?** ● **Se eu não renovar o HSS após ele expirar, meus serviços serão afetados?**

Lançado em	Descrição
	● **Se eu cancelar a assinatura do HSS e comprá-lo novamente, preciso instalar agentes e definir as configurações de proteção do servidor do zero?**
27/04/2023	Esta edição é o oitavo lançamento oficial. Adição de: ● **Como renovar o HSS?** ● **Como cancelar a assinatura das cotas de HSS?**
06/03/2023	Este é o sétimo lançamento oficial. Adição de: **Como usar imagens para instalar agentes em lotes?**
18/01/2023	Este é o sexto lançamento oficial. Adição de **Por que uma edição de HSS não entra em vigor após a compra?**
15/11/2022	Este é o quinto lançamento oficial. Adição de **E se eu não fizer a atualização da versão do HSS (anterior) para a versão do HSS (novo)?**
04/11/2022	Este é o quarto lançamento oficial. Adição de **O que devo fazer se a atualização do HSS falhar?**
28/10/2022	Esta edição é o terceiro lançamento oficial. Adição das seguintes seções: **Como atualizar o agente?** **Quais são as diferenças entre backup de proteção contra ransomware e backup em nuvem?**
20/10/2022	Esta edição é o segundo lançamento oficial. Adição de todas as seções sobre problemas do agente.
31/08/2022	Esta edição é o primeiro lançamento oficial.

