Host Security Service

Guia de usuário

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 Ativação do HSS

1.1 Compra de uma cota do HSS

Você pode comprar uma cota de HSS no console.

Precauções

- A cota só pode ser usada na região onde você a comprou.
- Uma cota pode ser vinculada a um servidor para protegê-lo, com a condição de que o agente no servidor esteja on-line.
- Atualmente, o HSS só pode proteger containers Docker e Containerd. Verifique seu tipo de containers antes de comprar a edição de container.
- O HSS deve ser implementado em todos os seus servidores para que, se um vírus infectar um deles, ele não possa se espalhar para outros e danificar toda a sua rede.
- Depois de comprar a cota, acesse a página **Servers & Quota** para ativar o HSS.
- A edição premium é fornecida gratuitamente se você tiver comprado a edição WTP.

AVISO

- É aconselhável implementar o HSS em todos os seus servidores para que, se um vírus infectar um deles, ele não possa se espalhar para outros e danificar toda a sua rede.
- No modo **Pay-per-use**, a edição empresarial do HSS para de cobrar se os servidores que ela protege forem interrompidos.

Regiões

Tabela 1-1 Escolher uma região para comprar HSS

Servidor	Região do servidor	Região
ECS BMS HECS Espaço de trabalho da Huawei Cloud	Regiões onde o HSS está disponível	Regiões onde seus ECSs/BMSs/HECSs/Espaços de trabalho estão implementados O HSS não pode ser usado entre regiões. Se o servidor e sua cota de proteção estiverem em regiões diferentes, cancele a assinatura da cota e compre uma cota na região em que o servidor está implementado.
Servidor de nuvem de terceiros	-	Compre cota de proteção na região CN South-Guangzhou, CN-Hong Kong ou AP-Singapore. Para instalar o agente, execute o procedimento de instalação para servidores não da Huawei Cloud.
Servidor off-line	-	

Pré-requisitos

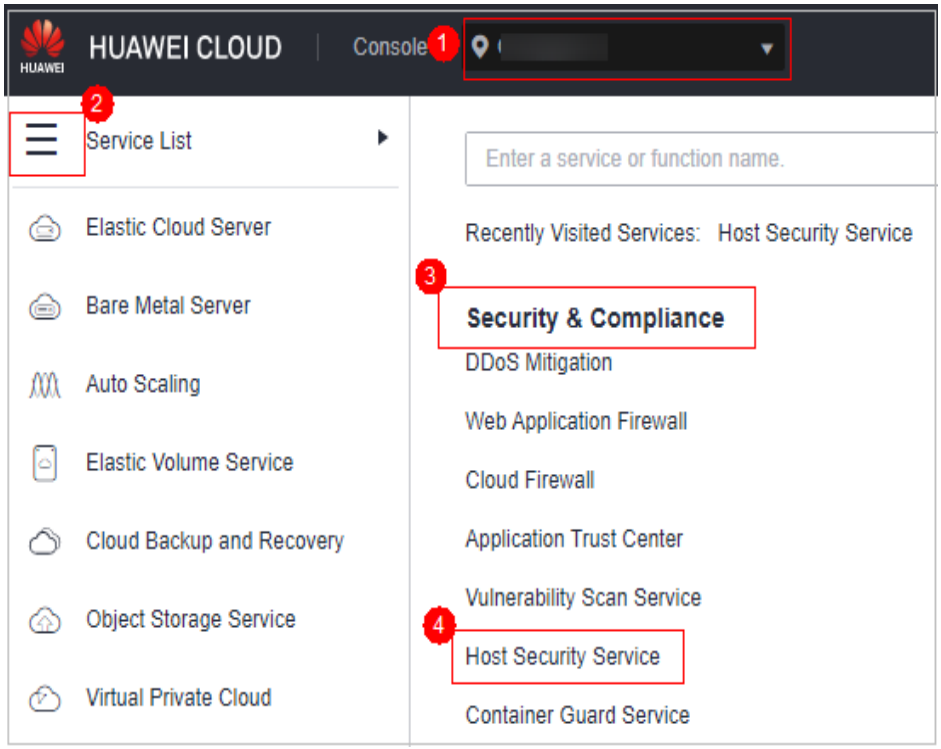
A conta deve ter as permissões **BSS Administrator** e **HSS Administrator**. Se a conta não tiver as permissões, use uma conta principal para comprar cotas ou autorize contas de membros a comprar cotas.

Procedimento

Passo 1 **Efetue 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 1-1 Acessar o HSS



Passo 3 No canto superior direito da página **Dashboard**, clique em **Buy HSS**.

Passo 4 Na página **Buy HSS**, defina as especificações da cota.

Tabela 1-2 Parâmetros para compra de HSS

Parâmetro	Descrição	Exemplo de valor
Billing Mode	Selecione o modo de cobrança **Yearly/Monthly** ou **Pay-per-use** com base em suas necessidades. ● Yearly/Monthly: você pode selecionar a edição básica, profissional, empresarial, premium, WTP ou de container. Você pode comprar a edição por um período fixo de tempo. A taxa é 30% menor do que a do pagamento por uso. Se você usar a edição por um longo tempo, você é aconselhado a comprar pacotes anuais/mensais. ● Pay-per-use: somente a edição empresarial pode ser comprada. Você precisa ativar esta edição na lista de servidores. Você paga pelo tempo de uso dos recursos. Os preços são calculados por hora, e nenhuma taxa mínima é necessária. **NOTA** Procedimento para ativar a cota de pagamento por uso: 1. Na página de compra, selecione **Pay-per-use**. A edição **Enterprise** será selecionada automaticamente. No canto inferior direito, clique em **Enable Now**. Você será redirecionado para a lista de servidores. 2. Na lista de servidores, clique em **Enable** na coluna **Operation**. Defina o **Billing Mode** para **Pay-per-use** e **Edition** para **Enterprise**. 3. Confirme as informações e clique em **OK**.	Yearly/ Monthly
Region	● Para minimizar os problemas de conexão, compre a cota na região de seus servidores.	CN-Hong Kong
Edition	As edições básica, profissional, empresarial, premium, WTP e de container são suportadas. Para detalhes sobre as diferenças entre as edições, consulte **Edições**. **AVISO** ● Se você ativar a edição básica do HSS pela primeira vez, poderá aproveitar o teste gratuito por 30 dias e comprá-lo após o teste. ● Se você comprou a edição básica, empresarial ou premium, ative-a na página **Asset Management** > **Servers & Quota**. ● Se você comprou a edição WTP, ative-a na lista de servidores na página **Prevention** > **Web Tamper Protection**. ● Se você comprou a edição de container, escolha **Asset Management** > **Containers & Quota** e ative a proteção na guia **Container Nodes**.	Enterprise

Parâmetro	Descrição	Exemplo de valor
Enterprise Project	Essa opção só está disponível quando você estiver conectado usando uma conta empresarial ou quando tiver ativado projetos empresariais. Para ativar essa função, entre em contato com seu gerente de clientes. Um projeto empresarial fornece um modo de gerenciamento de recursos de nuvem, no qual os recursos e os membros da nuvem são gerenciados centralmente pelo projeto. Selecione um projeto empresarial na lista suspensa. **NOTA** ● Os recursos e as despesas incorridas são gerenciados sob o projeto empresarial selecionado. ● Valor **default** indica o projeto empresarial padrão. Os recursos que não estão alocados a nenhum projeto empresarial na sua conta são exibidos no projeto empresarial padrão. ● A opção **default** está disponível na lista suspensa **Enterprise Project** somente depois que você comprou o HSS com sua Huawei ID.	default
Required duration	● Selecione uma duração com base em suas necessidades. No modo **Pay-per-use**, você não precisa selecionar uma duração. ● 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
Server Quota	Insira o número de cotas de HSS a serem compradas. No modo **Pay-per-use**, você não precisa configurar essa opção. **AVISO** ● Todos os seus servidores devem ser protegidos, de modo que, se um vírus (como ransomware ou um programa de mineração) infectar um deles, ele não será capaz de se espalhar para outros e danificar toda a sua rede. ● Não é possível modificar a cota de uma edição após a conclusão da compra. Você pode cancelar a assinatura e comprar novamente.	20
Tag	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). Para usar essa função, sua conta deve ter a permissão **TMS administrator**. Sem essa permissão, você não pode adicionar tags às cotas de proteção e a mensagem de erro "permission error" será exibida. Você não precisa definir este parâmetro no modo de pagamento por uso.	data

Passo 5 No canto inferior direito da página, clique em **Next**.

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

Passo 6 Depois de confirmar o pedido, selecione **I have read and agree to the Host Security Service Disclaimer** e clique em **Pay Now**.

Passo 7 Clique em **Pay Now** e conclua o pagamento.

----Fim

Procedimento de acompanhamento

Se você comprou HSS na edição ou região errada, você pode primeiro cancelar a assinatura e, em seguida, comprar a cota correta.

1.2 Instalação de um agente

1.2.1 Instalação de um agente no Linux

Para ativar a proteção da carga de trabalho para servidores em nuvem, instale o agente primeiro.

Este tópico descreve como instalar o agente em um servidor executando Linux. Para obter detalhes sobre como instalar um agente no Windows, consulte **Instalação de um agente no Windows**.

NOTA

O CentOS 6.x não é mais atualizado ou mantido no site oficial do Linux, e o HSS não suporta mais o CentOS 6.x ou anterior.

Limitações e restrições

O HSS pode proteger tanto os servidores da Huawei Cloud como os servidores não da Huawei Cloud.

- Servidor da Huawei Cloud
  - Você pode gerenciar servidores em nuvem comprados no console da Huawei Cloud.
  - Somente servidores em nuvem de 64-bit são suportados.
  - O HSS comprado deve estar na mesma região que seus servidores e ser instalado usando o pacote de instalação ou o comando de instalação fornecido para essa região.
- Servidor não da Huawei Cloud
  - Você pode gerenciar servidores comprados fora do console da Huawei Cloud ou os servidores da Huawei Cloud que não estão em sua região.
  - Somente servidores em nuvem de 64-bit são suportados.
  - Depois que o agente é instalado, você pode procurar um servidor na lista de servidores protegidos pelo EIP do servidor.

AVISO

- Para uma melhor compatibilidade e experiência de serviço, é aconselhável usar os servidores da Huawei Cloud.
- Antes de instalar o agente, limpe os processos e configurações da aplicação que possam interferir na instalação nos servidores para evitar falhas na instalação.
- Atualmente, você pode instalar agentes em servidores não da Huawei Cloud apenas nas regiões Beijing 1, Beijing 4, Shanghai 1, Shanghai 2, Guangzhou, Singapore e Hong Kong.

Caminho de instalação padrão

O caminho de instalação do agente em servidores que executam o SO Linux não pode ser personalizado. O caminho padrão é:

/usr/local/hostguard/

Tipos de servidores

Você pode instalar o HSS em servidores da Huawei Cloud e não da Huawei Cloud. Para mais detalhes, consulte **Tabela 1-3**.

Tabela 1-3 Instalação do HSS para diferentes servidores

Tipo de servidores	Método de instalação do agente
ECS BMS HECS	Se o servidor e a cota do HSS estiverem na mesma região, use o método para instalar agentes nos servidores da Huawei Cloud descritos acima.
	Se o servidor e a cota do HSS estiverem em regiões diferentes, cancele a assinatura da cota e compre uma cota na região em que o servidor está implementado.
Espaço de trabalho da Huawei Cloud	O agente do HSS será instalado automaticamente na cota comprada.
Servidor de nuvem de terceiros	Use o método para instalar agentes em servidores não da Huawei Cloud descritos acima. ● Atualmente, você pode instalar agentes em servidores não da Huawei Cloud apenas nas regiões Beijing 1, Beijing 4, Shanghai 1, Shanghai 2, Guangzhou, Singapore e Hong Kong. ● Depois que o agente for instalado em um servidor, o servidor será exibido no console. Você pode encontrá-lo pesquisando seu endereço IP.
Servidor off-line	

Pré-requisitos

- Para instalar o agente em um servidor em outra nuvem, certifique-se de que o servidor execute o Linux e possa acessar a Internet.

- O firewall de SELinux (Linux com segurança aprimorada) foi desativado. O firewall afeta a instalação do agente e deve permanecer desativado até que o agente seja instalado.

Precauções da instalação

- Para obter detalhes sobre os SOs suportados pelo agente, consulte **SOs suportados**.
- Certifique-se de que a regra de saída de seu grupo de segurança permita o acesso à porta 10180 no segmento de rede 100.125.0.0/16. (Esta é a configuração padrão.)
- Para uma melhor compatibilidade e experiência de serviço, é aconselhável usar os servidores da Huawei Cloud.
- Se algum software de segurança de terceiros tiver sido instalado no servidor, o agente do HSS pode falhar ao ser instalado. Nesse caso, desative ou desinstale o software antes de instalar o agente.
- A capacidade disponível do disco em que o agente está instalado deve ser maior que 300 MB. Caso contrário, a instalação do agente poderá falhar.
- Após a instalação, leva de 5 a 10 minutos para atualizar o status do agente. Você pode verificá-lo na guia "Servers" da página "Asset Management > Servers & Quota".
- Se esta é a primeira vez que você instala o agente, configure as notificações de alarme após a instalação.

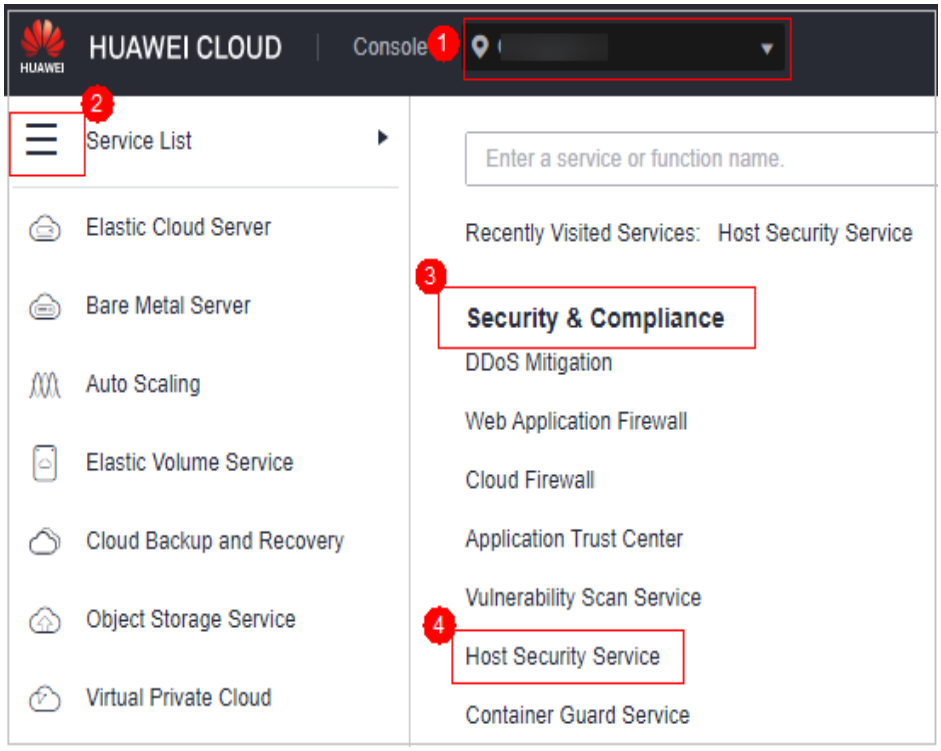
Instalação de um agente usando comandos

Este procedimento envolve o logon no servidor e a execução de comandos. Leva de 3 a 5 minutos para que o console atualize o status do agente após a instalação 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**.

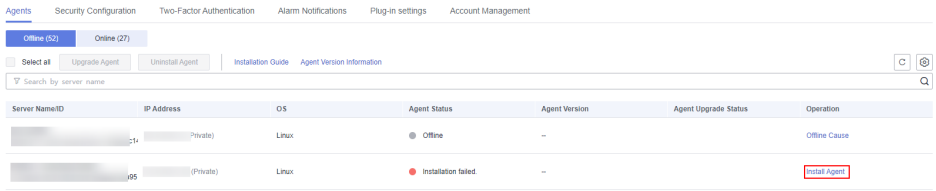
Figura 1-2 Acessar o HSS



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

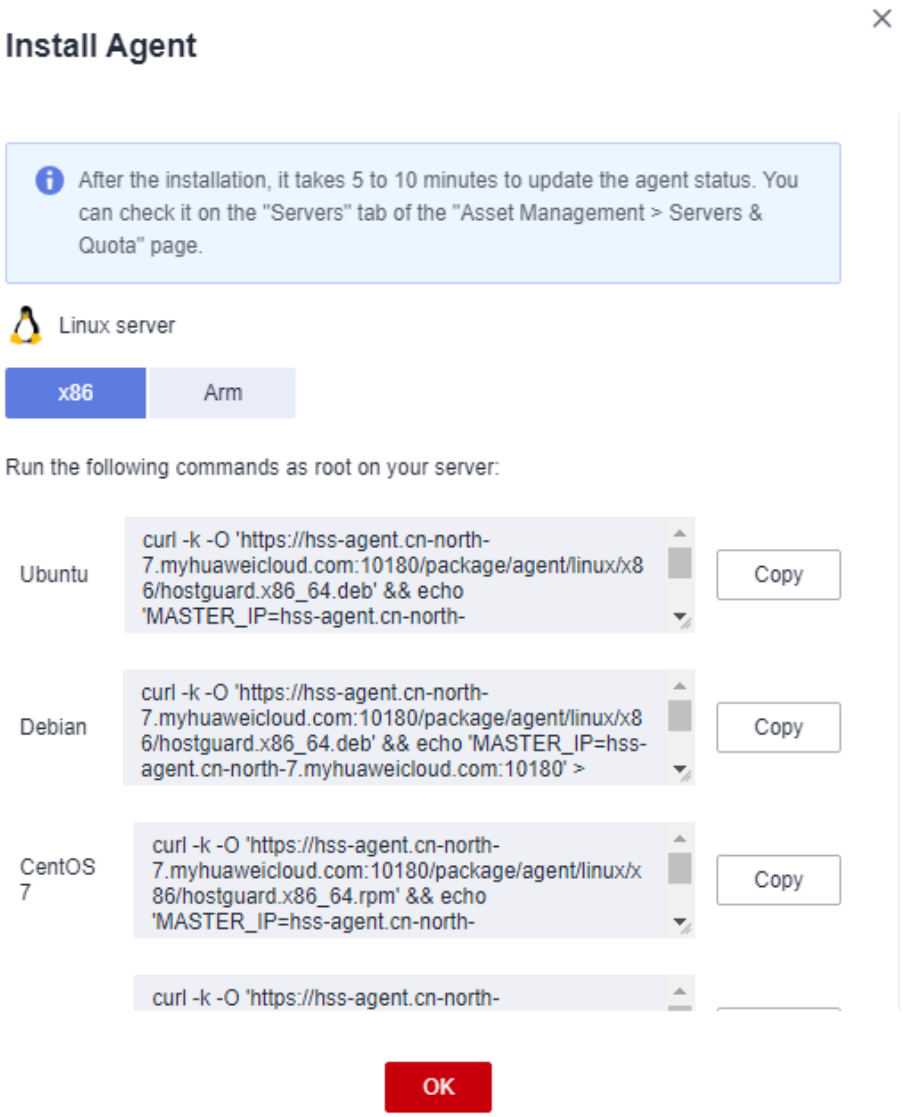
Passo 4 Clique na guia **Agents**. Clique em **Offline**. Na coluna **Operation** de um servidor, clique em **Install Agent**.

Figura 1-3 Selecionar um servidor do Linux



Passo 5 Na caixa de diálogo exibida, copie o comando adequado para a arquitetura do sistema e o SO.

Figura 1-4 Copiar o comando para instalar o agente



Passo 6 Faça logon remotamente no servidor em que o agente será instalado.

- **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 7 Cole o comando de instalação copiado e execute-o como usuário **root** para instalar o agente no servidor.

> **NOTA**
>
> - Se o pacote de instalação não puder ser baixado, verifique se o DNS pode resolver o nome de domínio no comando de instalação.
> - Para instalar o agente em um servidor não da Huawei Cloud, verifique se o ID da organização no comando existe. Caso contrário, o status do agente poderá ser exibido como **Not installed**, mesmo que a instalação tenha sido bem-sucedida.

Se forem exibidas informações semelhantes às seguintes, o agente foi instalado com sucesso:

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

Passo 8 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
```

----Fim

Pergunta frequente

- Para obter detalhes sobre o status do agente e a solução de problemas, consulte **O que devo fazer quando o status de execução do agente estiver anormal?**
- Para obter detalhes sobre como lidar com falhas de instalação do agente, consulte **O que devo fazer se a instalação do agente falhar?**
- Para obter detalhes sobre a desinstalação do agente, consulte **Como desinstalar o agente?**

1.2.2 Instalação de um agente no Windows

Para ativar a proteção da carga de trabalho para servidores em nuvem, instale o agente primeiro.

Este tópico descreve como instalar o agente em um servidor executando um SO Windows. Para obter detalhes sobre como instalar um agente no SO Linux, consulte **Instalação de um agente no Linux**.

> **NOTA**
>
> O CentOS 6.x não é mais atualizado ou mantido no site oficial do Linux, e o HSS não suporta mais o CentOS 6.x ou anterior.

Limitações e restrições

O HSS pode proteger tanto os servidores da Huawei Cloud como os servidores não da Huawei Cloud.

- **Servidor da Huawei Cloud**
  - Você pode gerenciar servidores em nuvem comprados no console da Huawei Cloud.
  - Somente servidores em nuvem de 64-bit são suportados.
  - Verifique se você comprou o HSS na região do servidor e usou o pacote de instalação ou o comando de instalação na região para instalar agentes do HSS nos servidores.

- **Servidor não da Huawei Cloud**
  - Você pode gerenciar servidores comprados fora do console da Huawei Cloud ou os servidores da Huawei Cloud que não estão em sua região.
  - Somente servidores em nuvem de 64-bit são suportados.
  - Depois que o agente é instalado, você pode procurar um servidor na lista de servidores protegidos pelo EIP do servidor.

AVISO

- Para uma melhor compatibilidade e experiência de serviço, é aconselhável usar os servidores da Huawei Cloud.
- Antes de instalar o agente, limpe os processos e configurações da aplicação que possam interferir na instalação nos servidores para evitar falhas na instalação.
- Atualmente, você pode instalar agentes em servidores não da Huawei Cloud apenas nas regiões Beijing1, Beijing 4, Shanghai 1, Shanghai 2, Guangzhou, Singapore e Hong Kong.

Caminho de instalação padrão

O caminho de instalação do agente em servidores que executam o SO Windows não pode ser personalizado. O caminho padrão é:

C:\Program Files\HostGuard

Tipos de servidores

Você pode instalar o HSS em servidores da Huawei Cloud e não da Huawei Cloud. Para mais detalhes, consulte **Tabela 1-4**.

Tabela 1-4 Métodos de instalação

Tipo de servidores	Método de instalação do agente
ECS BMS HECS	Se o servidor e a cota do HSS estiverem na mesma região, use o método para instalar agentes nos servidores da Huawei Cloud descritos acima.
	Se o servidor e a cota do HSS estiverem em regiões diferentes, cancele a assinatura da cota e compre uma cota na região em que o servidor está implementado.
Espaço de trabalho da Huawei Cloud	O agente do HSS será instalado automaticamente na cota comprada.

Tipo de servidores	Método de instalação do agente
Servidor de nuvem de terceiros	Use o método para instalar agentes em servidores não da Huawei Cloud descritos acima. ● Atualmente, você pode instalar agentes em servidores não da Huawei Cloud apenas nas regiões Beijing1, Beijing 4, Shanghai 1, Shanghai 2, Guangzhou, Singapore e Hong Kong. ● Depois que o agente for instalado em um servidor, o servidor será exibido no console. Você pode encontrá-lo pesquisando seu endereço IP.
Servidor local	

Pré-requisitos

- (Para servidores não da Huawei Cloud) Certifique-se de que o servidor execute o SO Windows e possa acessar a Internet.
- Uma ferramenta de gerenciamento remoto, como mstsc e RDP, foi instalada no seu PC.

Precauções da instalação

- Para obter detalhes sobre os SOs suportados pelo agente, consulte **SOs suportados**.
- Para uma melhor compatibilidade e experiência de serviço, é aconselhável usar os servidores da Huawei Cloud.
- Para um servidor do Windows, o agente pode ser baixado somente depois que o endereço do servidor DNS privado é configurado. Para obter mais informações, consulte **O que são os endereços de servidor DNS privado da Huawei Cloud?**
- Se algum software de segurança de terceiros tiver sido instalado no servidor, o agente do HSS pode falhar ao ser instalado. Nesse caso, desative ou desinstale o software antes de instalar o agente.
- A capacidade disponível do disco em que o agente está instalado deve ser maior que 300 MB. Caso contrário, a instalação do agente poderá falhar.
- Após a instalação, leva de 5 a 10 minutos para atualizar o status do agente. Você pode verificá-lo na guia "Servers" da página "Asset Management > Servers & Quota".
- Se esta é a primeira vez que você instala o agente, configure as notificações de alarme após a instalação.

Procedimento

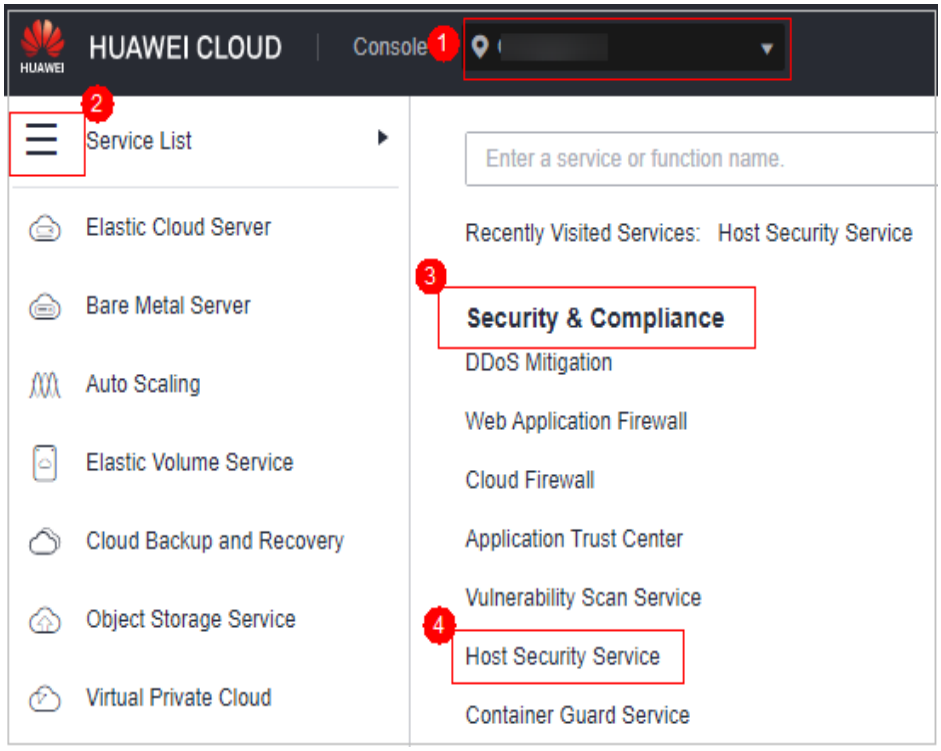
Há duas maneiras de instalar um agente. Esta seção descreve a primeira.

- Método 1: faça download do pacote de instalação do agente, carregue-o no servidor onde o agente será instalado e execute o comando de instalação no servidor para instalar o agente.
- Método 2: efetue logon em um servidor, efetue logon no console de gerenciamento a partir do servidor, faça download e instale o 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**.

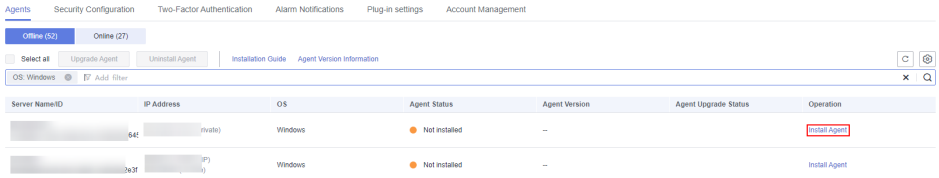
Figura 1-5 Acessar o HSS



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

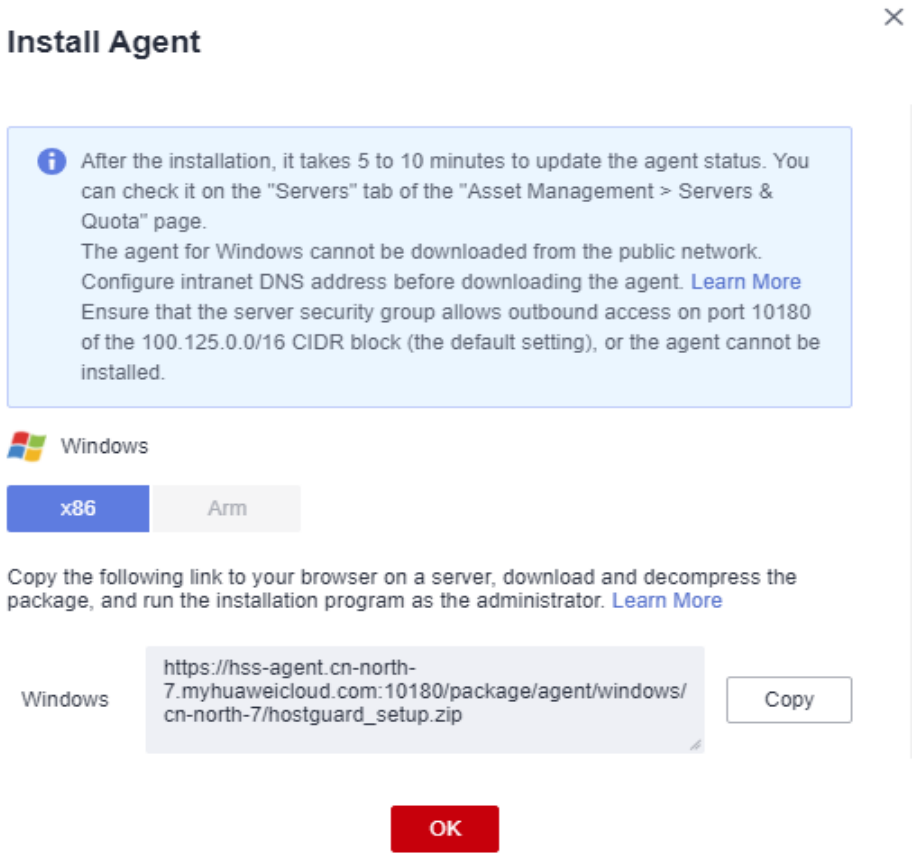
Passo 4 Clique na guia **Agents**. Clique em **Offline**. Na coluna **Operation** de um servidor, clique em **Install Agent**.

Figura 1-6 Selecionar um servidor do Windows



Passo 5 Na caixa de diálogo exibida, copie o link de download do agente adequado para a arquitetura do sistema e o SO.

Figura 1-7 Copiar o comando para instalar o agente do Windows



Passo 6 Efetue logon remotamente no servidor onde o agente será instalado.

- 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 7 No servidor em que o agente 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.

NOTA

- Para instalar o agente em um servidor não da Huawei Cloud, verifique se o ID da organização no comando está correto. Caso contrário, o status do agente poderá ser exibido como **Not installed**, mesmo que a instalação tenha sido bem-sucedida.

Passo 8 Execute o programa de instalação do agente como um administrador.

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

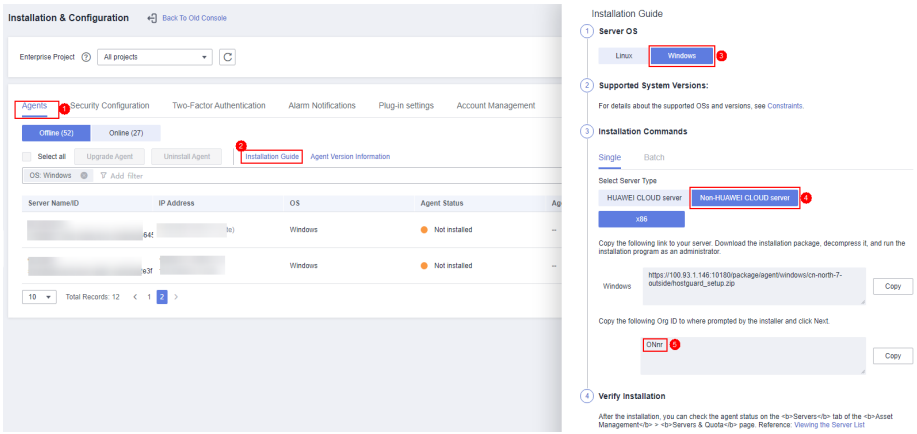
- Servidor da Huawei Cloud: selecione **Huawei Cloud Host**.
- Servidor não da Huawei Cloud: selecione **Other Cloud Host**.

Copie o ID da organização da página de instalação do agente, conforme mostrado em **Figura 1-8**. Digite o ID da organização e 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 1-8 Obtenção do ID da organização (para um servidor não da Huawei Cloud)



Passo 9 Verifique os processos **HostGuard.exe** e **HostWatch.exe** no Gerenciador de Tarefas do Windows.

Se os processos não existirem, a instalação do agente falhará. Nesse caso, reinstale o agente.

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

----Fim

Pergunta frequente

- Para obter detalhes sobre o status do agente e a solução de problemas, consulte **Como corrigir um agente anormal?**
- Para obter detalhes sobre como lidar com falhas de instalação do agente, consulte **O que devo fazer se a instalação do agente falhar?**
- Para obter detalhes sobre a desinstalação do agente, consulte **Como desinstalar o agente?**

1.3 Habilitação de HSS

1.3.1 Ativação da edição básica/profissional/empresarial/premium

Antes de ativar a proteção em servidores, você precisa alocar cota para um servidor especificado. Se a proteção for desativada ou o servidor for excluído, a cota poderá ser alocada para outros servidores.

Para a edição WTP, escolha **Prevention** > **Web Tamper Protection** > **Server Protection** e, em seguida, ative-a. Para obter detalhes, consulte **Habilitação da edição WTP**.

NOTA

Para ativar a edição WTP, escolha **Prevention** > **Web Tamper Protection** > **Server Protection** e clique na guia **Servers**. Todas as funções da edição premium estão incluídas na edição WTP.

Modo de verificação

O HSS realiza uma verificação completa no início da manhã todos os dias.

Depois de ativar a proteção do servidor, pode visualizar os resultados da verificação após a verificação automática na manhã seguinte ou executar uma **verificação manual** imediatamente.

Pré-requisitos

- O status do agente do servidor a ser protegido é **Online**. Para verificar o status, escolha **Host Security Service** > **Asset Management** > **Servers & Quota**.
- Você comprou cotas de edição necessárias em sua região.
- Para proteger melhor seus containers, é aconselhável definir configurações de segurança.

Restrições

- SO Linux

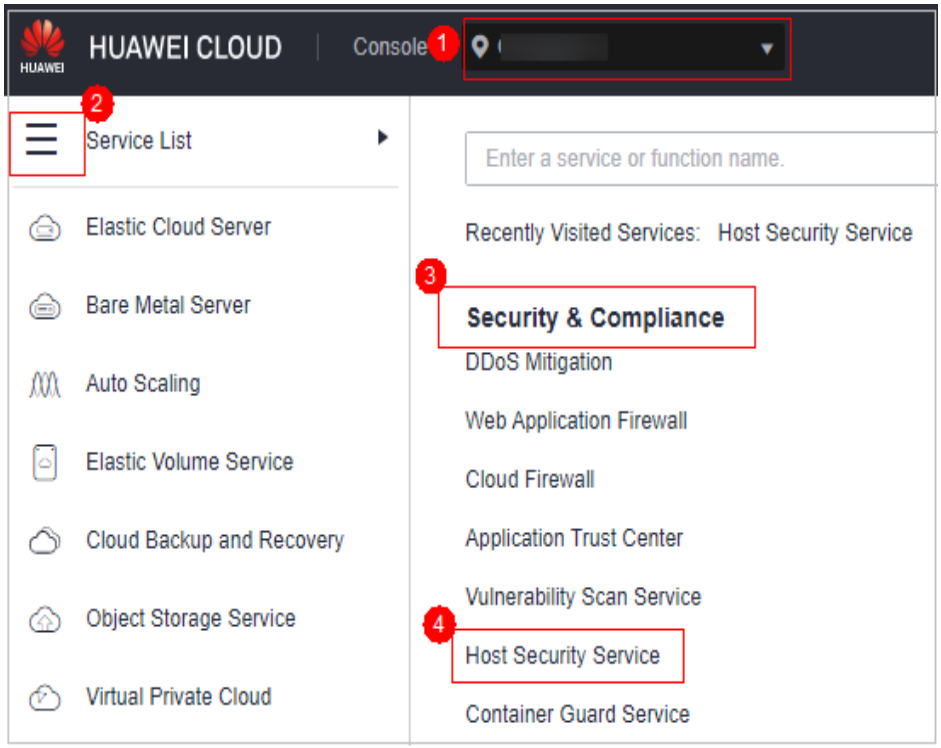
  Em servidores que executam o EulerOS com ARM, o HSS não bloqueia os endereços IP suspeitos de ataques de força bruta de SSH, mas apenas gera alarmes.
- SO Windows
  - Autorize o firewall do Windows quando ativar a proteção para um servidor do Windows. Não desative o firewall do Windows durante o período 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.

Ativação da 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 1-9 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 Selecione o servidor de destino e clique em **Enable**.

Você pode comprar HSS no modo de pagamento por uso ou modo anual/mensal.

NOTA

- Somente a edição empresarial suporta o modo de pagamento por uso.
- Se a cota for insuficiente ao selecionar o modo anual/mensal, você precisa comprar cotas de HSS.
- A prevenção de ransomware é ativada automaticamente com a edição premium. Para aprimorar a prevenção de ransomware, você pode configurar diretórios protegidos e ativar a proteção dinâmica de honeypot conforme necessário. Você também é aconselhado a ativar o backup para que você possa restaurar os dados no caso de um ataque de ransomware para minimizar as perdas. Para obter detalhes, consulte **Modificação de uma política de proteção** e **Habilitação de backup de ransomware**.

- **Yearly/Monthly**

  Na caixa de diálogo exibida, selecione uma edição, selecione o modo **Yearly/Monthly**, aloque a cota do HSS e selecione **I have read and agree to the Host Security Service Disclaimer**.

  As cotas podem ser atribuídas das seguintes formas:

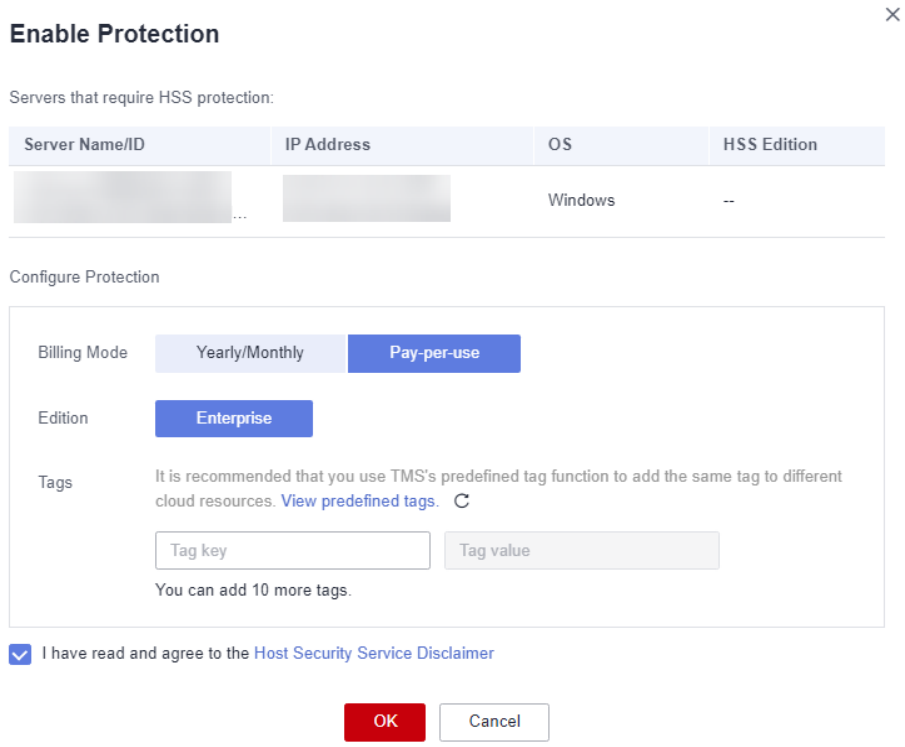
  – Selecione **Random quota** para permitir que o sistema aloque a cota com a validade restante mais longa para o servidor.

– Selecione um ID de cota e atribua-o a um servidor.

- **Pay-per-use**

  Na caixa de diálogo exibida, selecione o modo **Pay-per-use**, selecione a edição e selecione **I have read and agree to the Host Security Service Disclaimer**.

  Figura 1-10 Habilitação de HSS de pagamento por uso



  NOTA

  A edição básica pode ser usada gratuitamente por 30 dias. O modo anual/mensal da edição básica só pode ser usado após a compra.

Passo 5 Clique em **OK**. Visualize o status de proteção do servidor na lista de servidores.

Se o **Protection Status** do servidor de destino estiver **Enabled**, a edição básica, profissional, empresarial ou premium foi ativada.

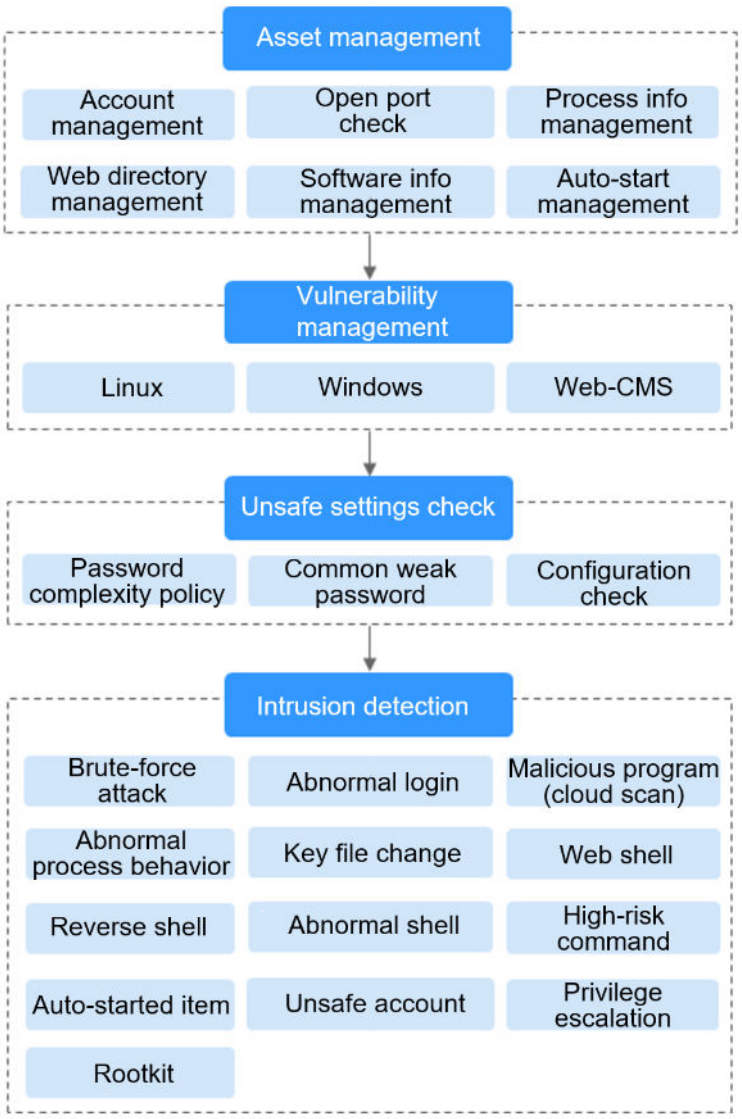
NOTA

- Como alternativa, na guia **Quotas** da página **Servers & Quota**, clique em **Bind Server** na coluna **Operation** para vincular uma cota a um servidor. O HSS ativará automaticamente a proteção para o servidor.
- Uma cota pode ser vinculada a um servidor para protegê-lo, com a condição de que o agente no servidor esteja on-line.

Depois que o HSS for ativado, ele verificará seus servidores em busca de problemas de segurança. Os itens de verificação variam de acordo com a edição que você ativou.

Para obter detalhes sobre as diferenças entre as edições, consulte **Edições**.

Figura 1-11 Itens de verificação de segurança automática



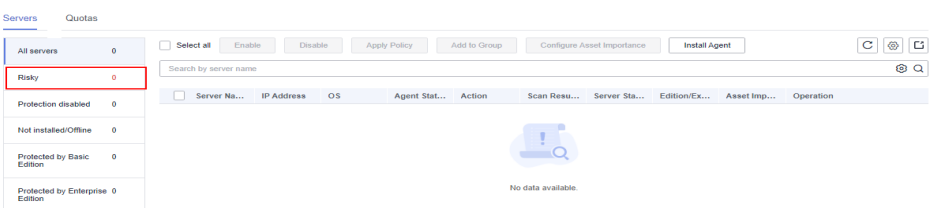
----Fim

Visualização de detalhes da detecção

Depois que a proteção do servidor estiver ativada, o HSS executará imediatamente uma detecção abrangente no servidor. A detecção pode levar muito tempo.

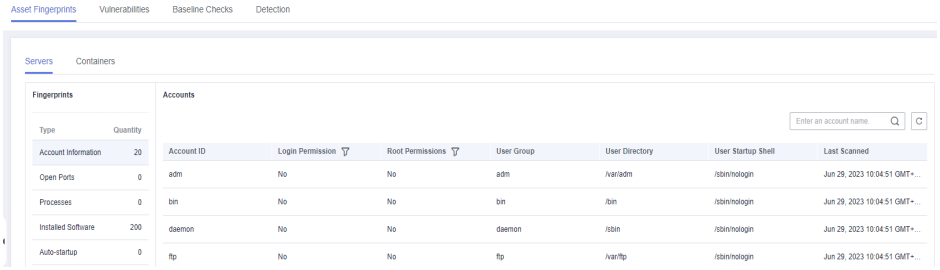
À esquerda da lista de proteção, clique em **Risky**.

Figura 1-12 Visualização de itens arriscados



Clique em um nome de servidor para ir para a página de detalhes. Nesta página, você pode verificar rapidamente as informações detectadas e os riscos do servidor.

Figura 1-13 Visualizar o resultado da detecção



Operação de acompanhamento

Você pode configurar manualmente os itens de verificação. Os itens configuráveis variam de acordo com a edição que você ativou.

Para obter detalhes sobre as diferenças entre as edições, consulte **Edições**.

Figura 1-14 Itens de verificação manual

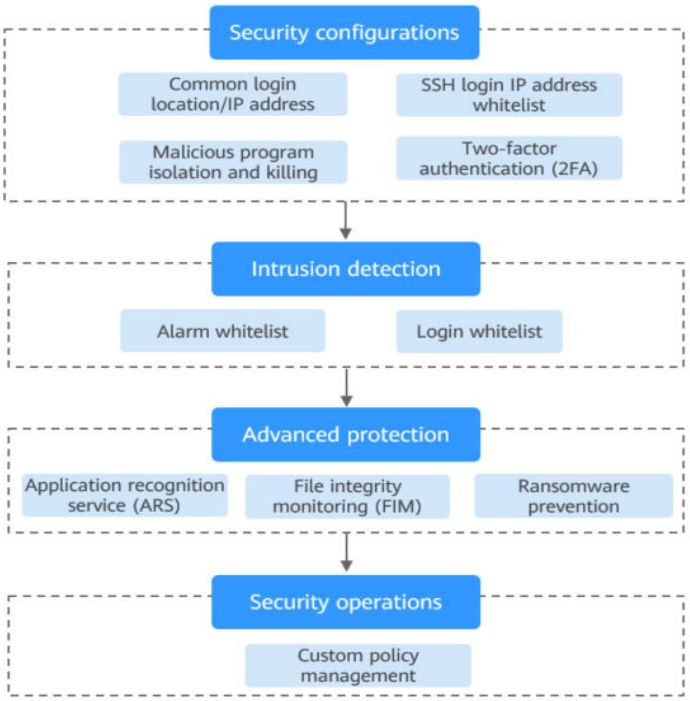


Tabela 1-5 Itens de verificação manual

Função	Item de verificação	Referência
Instalação e configuração	● Localização de logon comum/ endereço IP ● Lista branca de endereços IP de logon SSH ● Isolar e eliminar programas maliciosos	**Instalação e configuração**
Detecção de intrusão	● Lista branca do alarme ● Lista branca de logon	**Detecção de intrusão**
Defesa proativa	● Proteção da aplicação ● Prevenção de ransomware ● Monitoramento de integridade de arquivos (FIM)	**Prevenção**
Operações de segurança	● Gerenciamento de políticas	**Operações de segurança**
Relatório de segurança	● Assinar os relatórios de segurança	**Assinatura de um relatório de segurança**

Procedimento de acompanhamento

Desativar o HSS

Na guia **Servers** da página **Servers & Quotas**, clique em **Disable** na coluna **Operation** de um servidor.

Se o HSS estiver desativado, o status da cota do HSS mudará de ocupado para ocioso. Você pode alocar as cotas ociosas para outros servidores ou cancelar a assinatura das cotas desnecessárias para evitar o desperdício de cotas.

AVISO

- Antes de desativar a proteção, execute uma detecção abrangente no servidor, lide com os riscos conhecidos e registre as informações da operação para evitar erros de O&M e ataques ao servidor.
- Após a desativação da proteção, limpe dados importantes no servidor, interrompa aplicações importantes no servidor e desconecte o servidor da rede externa para evitar perdas desnecessárias causadas por ataques.

Desvincular a cota

Escolha **Asset Management** > **Servers & Quota** e clique na guia **Quotas**. Clique em **Unbind** na coluna **Operation**. O status de uso da cota não vinculada mudará de **In use** para **Idle**. O HSS desativará automaticamente a proteção para o servidor desvinculado da cota.

Você pode alocar as cotas ociosas para outros servidores ou cancelar a assinatura das cotas desnecessárias para evitar o desperdício de cotas.

1.3.2 Habilitação da edição WTP

Antes de habilitar a WTP, você precisa alocar uma cota para um servidor especificado. Se o serviço for desabilitado ou o servidor for excluído, a cota poderá ser alocada a outros servidores.

A edição premium será habilitada quando você habilitar a WTP.

Como a WTP impede a adulteração de páginas da Web

Tabela 1-6 Mecanismos de proteção

Tipo	Mecanismo
Proteção estática de páginas da Web	1. Bloqueio de diretório local A WTP bloqueia arquivos em um diretório de arquivos da Web em uma unidade para impedir que invasores os modifiquem. Os administradores do site podem atualizar o conteúdo do site usando processos privilegiados. 2. Backup e restauração ativos Se a WTP detectar que um arquivo em um diretório protegido foi adulterado, ela usará imediatamente o arquivo de backup no host local para restaurar o arquivo. 3. Backup e restauração remotos Se um diretório de arquivos ou um diretório de backup no host local for inválido, você poderá usar o serviço de backup remoto para restaurar a página da Web adulterada.
Proteção dinâmica de páginas da Web	Fornece autoproteção de aplicações em tempo de execução (RASP) para aplicações de Tomcat das seguintes maneiras: 1. Filtragem de comportamento malicioso baseada em RASP A autoproteção de aplicações em tempo de execução (RASP), exclusiva da Huawei, detecta comportamentos de programas de aplicações, impedindo que os invasores adulterem páginas da Web por meio de programas de aplicações. 2. Controle de acesso a arquivos de disco de rede A WTP implementa um gerenciamento refinado para controlar as permissões para adicionar, modificar e consultar o conteúdo do arquivo em discos de rede, evitando adulterações sem afetar a liberação do conteúdo do site.

Pré-requisitos

- Escolha **Prevention** > **Web Tamper Protection**. Clique na guia **Servers**. O **Protection Status** do servidor é **Unprotected**.
- Escolha **Asset Management** > **Servers & Quota**. O **Agent Status** de um servidor é **Online** e o **Protection Status** do servidor é **Unprotected**.

Configuração de diretórios protegidos

Você pode definir:

- Diretórios

  Você pode adicionar um máximo de 50 diretórios protegidos a um host. Para obter detalhes, consulte **Adição de um diretório protegido**.

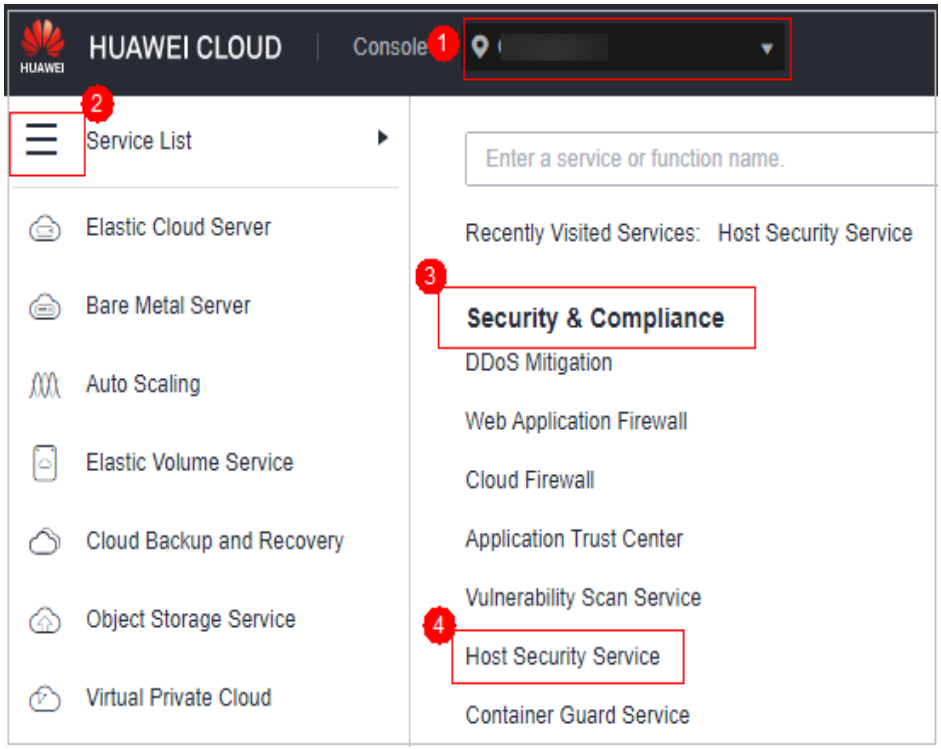
  Para registrar o status de execução do servidor em tempo real, exclua os arquivos de log no diretório protegido. Você pode conceder altas permissões de leitura e gravação para arquivos de log para impedir que invasores visualizem ou adulterem os arquivos de log.

Habilitação de WTP

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

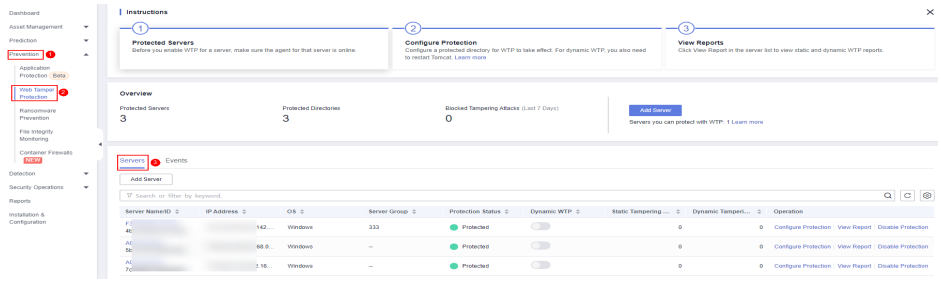
Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 1-15 Acessar o HSS



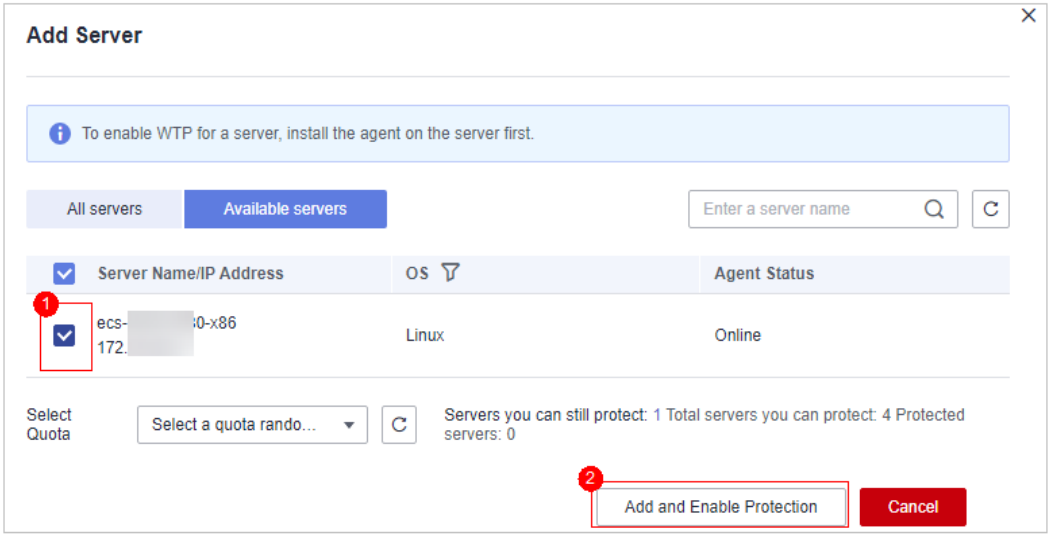
Passo 3 No painel de navegação, escolha **Prevention** > **Web Tamper Protection**. Na página **Web Tamper Protection**, clique em **Add Server**.

Figura 1-16 Adicionar um servidor protegido



Passo 4 Na página **Add Server**, selecione o servidor de destino, selecione cota na lista suspensa ou mantenha o valor padrão e clique em **Add and Enable Protection**.

Figura 1-17 Selecionar um servidor para habilitar a proteção



Passo 5 Visualize o status do servidor na página **Web Tamper Protection**.

A edição premium será habilitada quando você habilitar a WTP.

- Escolha **Prevention** > **Web Tamper Protection**. Se o **Protection Status** do servidor for **Protected**, a WTP foi habilitada.
- Escolha **Asset Management** > **Servers & Quota** e clique na guia **Servers**. Se o status de proteção do servidor de destino estiver **Enabled** e a **Edition/Expiration Date** dele for **Premium (included with WTP)**, a edição premium fornecida pela edição WTP será habilitada gratuitamente.

----Fim

AVISO

- Para habilitar a proteção WTP para um servidor, você também pode escolher **Asset Management** > **Servers & Quota**, clicar na guia **Quotas** e clicar em **Bind Server**.
- Uma cota pode ser vinculada a um servidor para protegê-lo, com a condição de que o agente no servidor esteja on-line.
- A prevenção de ransomware é ativada automaticamente com a edição WTP. Para aprimorar a prevenção de ransomware, você pode configurar diretórios protegidos e ativar a proteção dinâmica de honeypot conforme necessário. Você também é aconselhado a ativar o backup para que você possa restaurar os dados no caso de um ataque de ransomware para minimizar as perdas. Para obter detalhes, consulte **Modificação de uma política de proteção** e **Habilitação de backup de ransomware**.
- Desabilite a WTP antes de atualizar um site e habilite-a após a conclusão da atualização. Caso contrário, o site não será atualizado.
- Seu site não está protegido enquanto a WTP estiver desativada. Habilite-a imediatamente após a atualização do seu site.

Procedimento de acompanhamento

Desabilitar a WTP

Escolha **Prevention** > **Web Tamper Protection** e clique na guia **Servers**. Clique em **Disable Protection** na coluna **Operation** de um servidor.

Se a WTP estiver desabilitada, seu status de cota mudará de ocupado para ocioso. Você pode alocar as cotas ociosas para outros servidores ou cancelar a assinatura das cotas desnecessárias para evitar o desperdício de cotas.

AVISO

- Antes de desabilitar a WTP, execute uma detecção abrangente no servidor, trate os riscos conhecidos e registre as informações de operação para evitar erros de O&M e ataques ao servidor.
- Se a WTP estiver desabilitada, é mais provável que as aplicações da Web sejam adulteradas. Portanto, você precisa excluir dados importantes no servidor, interromper serviços importantes no servidor e desconectar o servidor da rede externa em tempo hábil para evitar perdas desnecessárias causadas por ataques ao servidor.
- Depois que você desabilitar a WTP, os arquivos no diretório protegido não estarão mais protegidos. É aconselhável processar arquivos no diretório protegido antes de executar essas operações.
- Se você encontrar alguns arquivos ausentes após a desabilitação da WTP, procure-os no caminho de backup local ou remoto.
- A edição premium será desabilitada quando você desabilitar a WTP.

Desvincular a cota

Escolha **Asset Management** > **Servers & Quota** e clique na guia **Quotas**. Clique em **Unbind** na coluna **Operation**. O status de uso da cota não vinculada será alterado de **In use** para **Idle**. O HSS desabilita automaticamente a WTP para servidores vinculados à cota.

Você pode alocar as cotas ociosas para outros servidores ou cancelar a assinatura das cotas desnecessárias para evitar o desperdício de cotas.

1.4 Ativação da proteção de nó de container

Antes de ativar a proteção para um nó de container, você precisa alocar cota para um nó especificado. Se a proteção for desativada ou o nó for excluído, a cota poderá ser alocada para outros nós.

Frequência de verificação

O HSS realiza uma verificação completa no início da manhã todos os dias.

Se você ativar a proteção do servidor antes do intervalo de verificação, poderá exibir os resultados da verificação somente após a conclusão da verificação às 00:00 do dia seguinte.

Restrições

Atualmente, o HSS só pode proteger containers Docker e Containerd.

Pré-requisito

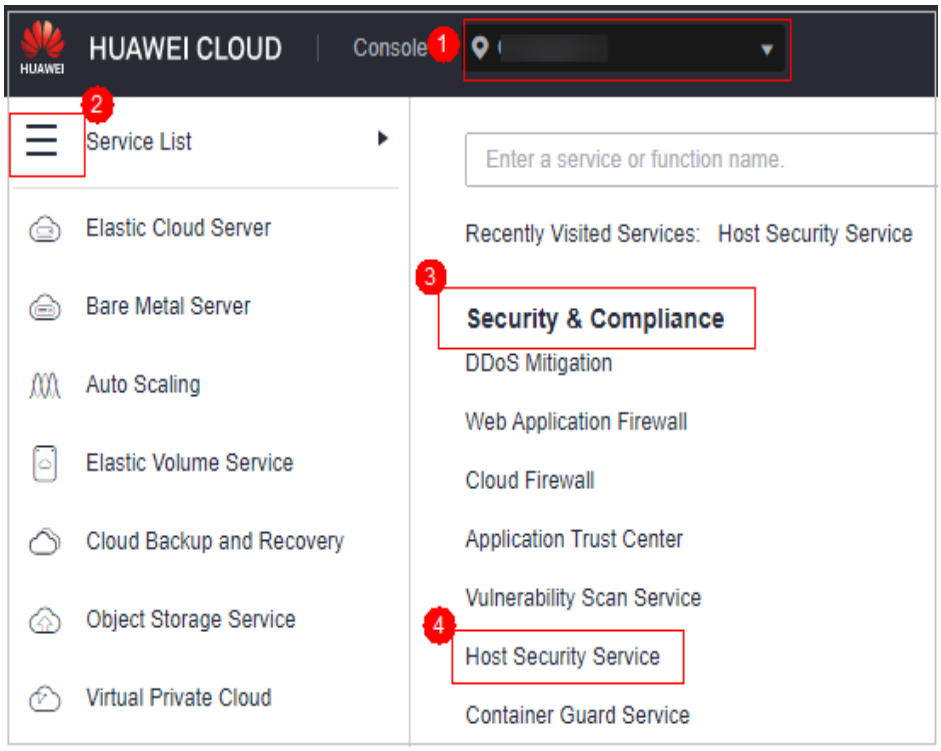
- O **Agent Status** de um servidor é **Online**. Para verificar o status, escolha **Host Security Service** > **Asset Management** > **Containers & Quota**.
- Você criou nós no CCE.
- O **Protection Status** do nó é **Unprotected**.

Procedimento

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

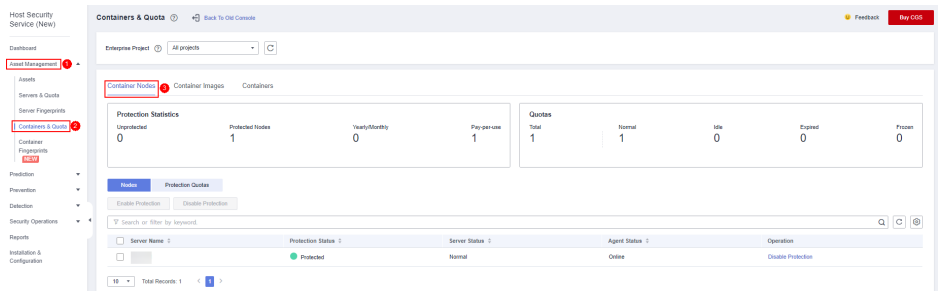
Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 1-18 Acessar o HSS



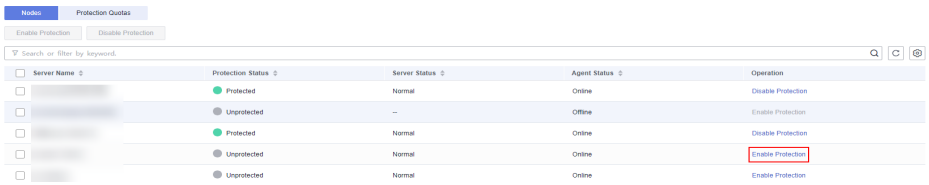
Passo 3 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Figura 1-19 Acessar a página de gerenciamento do nó do container



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

Figura 1-20 Ativar a proteção do container

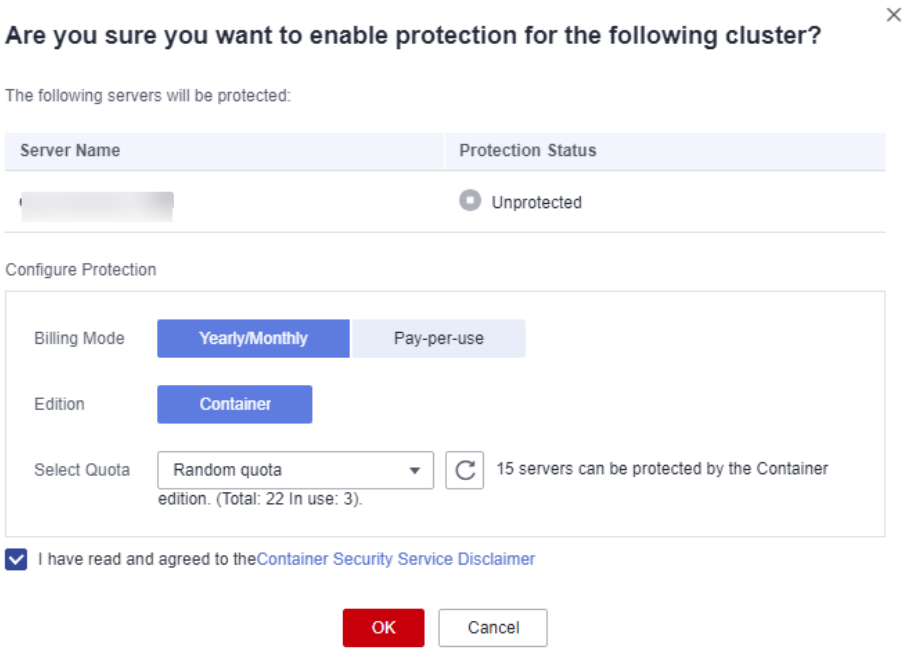


Passo 5 Você pode comprar cotas no modo de pagamento por uso ou anual/mensal.

- **Yearly/Monthly**

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

Figura 1-21 Ativar proteção anual/mensal



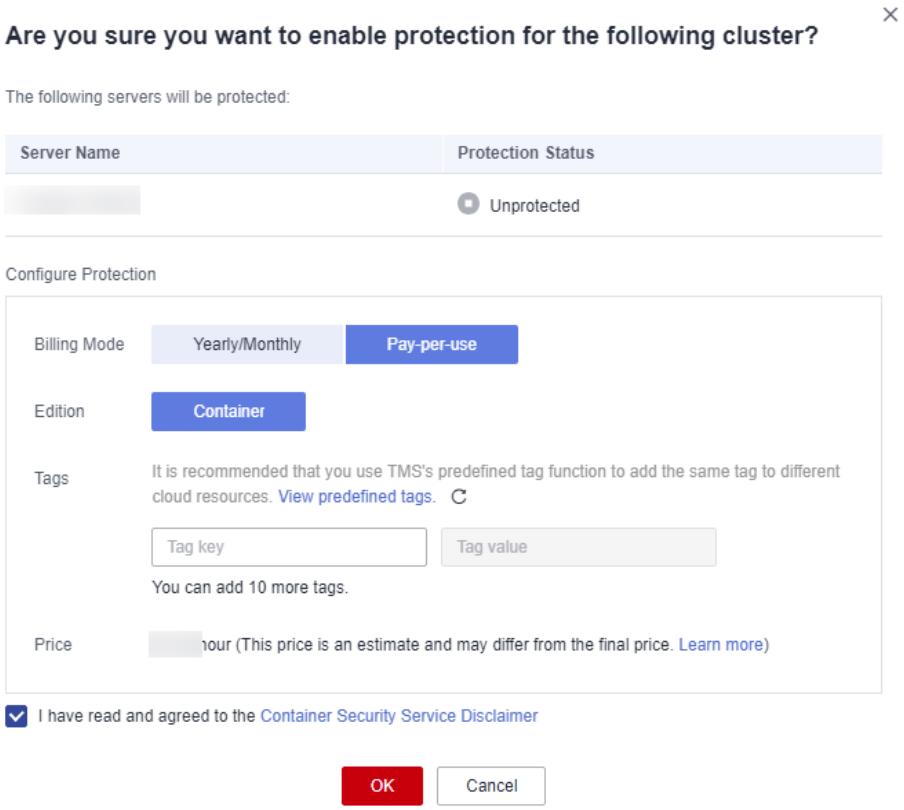
As cotas podem ser atribuídas das seguintes formas:

- Selecione **Random quota** para permitir que o sistema aloque a cota com a validade restante mais longa para o servidor.
- Selecione uma cota para alocar.

- **Pay-per-use**

  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 1-22 Ativar a proteção de pagamento por uso



Passo 6 Na caixa de diálogo exibida, leia o *Aviso de isenção de responsabilidade do Container Guard Service* e selecione **I have read and agreed to the Container Guard Service Disclaimer**.

Passo 7 Clique em **OK**. Se o **Protection Status** do servidor for alterado para **Protected**, a proteção foi ativada.

NOTA

Uma cota de segurança de container protege um nó de cluster.

- Uma cota de segurança de container protege um nó de cluster.
- A prevenção de ransomware é ativada automaticamente com a edição de container. Para aprimorar a prevenção de ransomware, você pode configurar diretórios protegidos e ativar a proteção dinâmica de honeypot conforme necessário. Você também é aconselhado a ativar o backup para que você possa restaurar os dados no caso de um ataque de ransomware para minimizar as perdas. Para obter detalhes, consulte **Modificação de uma política de proteção** e **Habilitação de backup de ransomware**.

----Fim

Procedimento de acompanhamento

Desativar a proteção para um nó

Escolha **Asset Management** > **Containers & Quota**, clique na guia **Container Nodes** e clique em **Nodes**. Na coluna **Operation**, clique em **Disable Protection**.

Se a proteção estiver desativada, o status da cota mudará de ocupado para ocioso. Você pode alocar a cota ociosa para outro nó ou cancelar a assinatura da cota desnecessária para evitar o desperdício da cota.

AVISO

- Antes de desativar a proteção, realize uma detecção abrangente no container, lide com os riscos detectados e registre as informações de operação para evitar erros de O&M e ataques ao container.
- Depois que a proteção for desativada, limpe dados importantes no container, interrompa aplicações importantes no container e desconecte o container da rede externa para evitar perdas desnecessárias causadas por ataques.

1.5 (Opcional) Alternação da edição do HSS

Você pode alternar a edição de cota de um servidor para a edição básica, profissional, empresarial ou premium, conforme necessário.

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

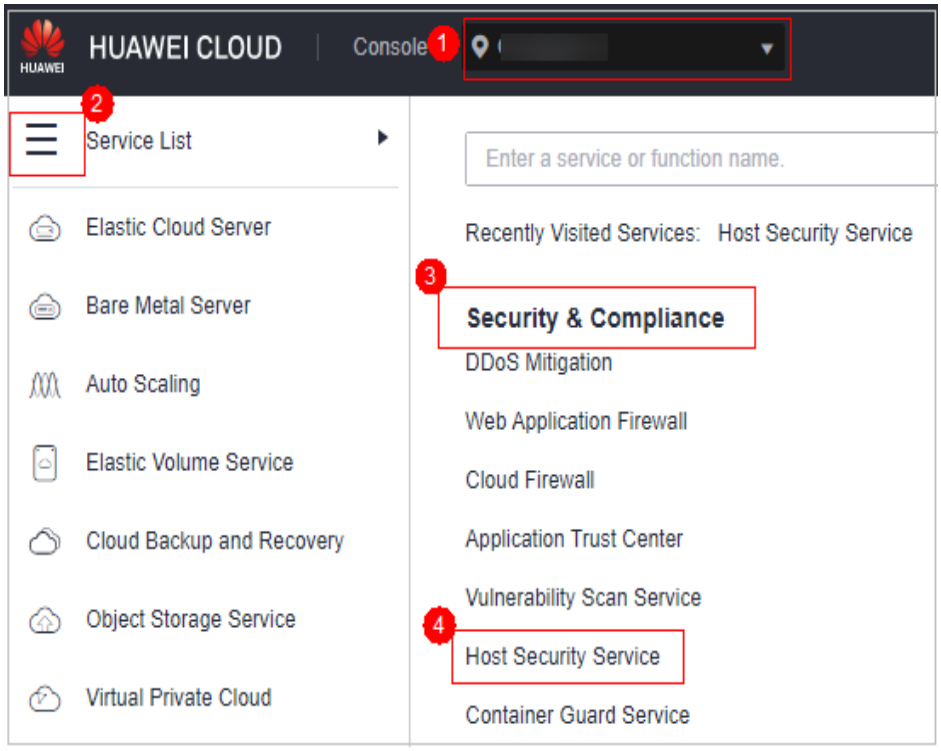
- O servidor cuja cota de proteção deve ser alterada está no estado **Protected**.
- Antes de mudar para uma quota no modo de cobrança anual/mensal, certifique-se de que a quota foi comprada e está disponível. Para obter detalhes, consulte **Compra de uma cota de HSS**.
- Antes de mudar para uma edição 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 1-23 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 1-7**. Para obter detalhes sobre as edições que podem ser alteradas, consulte **Tabela 1-8**.

Tabela 1-7 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 1-8 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 1-7**.
  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.

1.6 Ativação de 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.

- As configurações de notificação de alarme são efetivas somente para a região atual. Para receber notificações de outra região, mude para essa região e configure a notificação de alarme.
- As notificações de alarme podem ser bloqueadas por engano. Se você ativou as notificações, mas não recebeu nenhuma, verifique se elas foram bloqueadas como espasmos.
- O serviço Simple Message Notification (SMN) é um serviço pago. Para obter detalhes sobre o preço, consulte **Detalhes de preços do produto**.

Pré-requisitos

Antes de configurar a notificação de alarme,

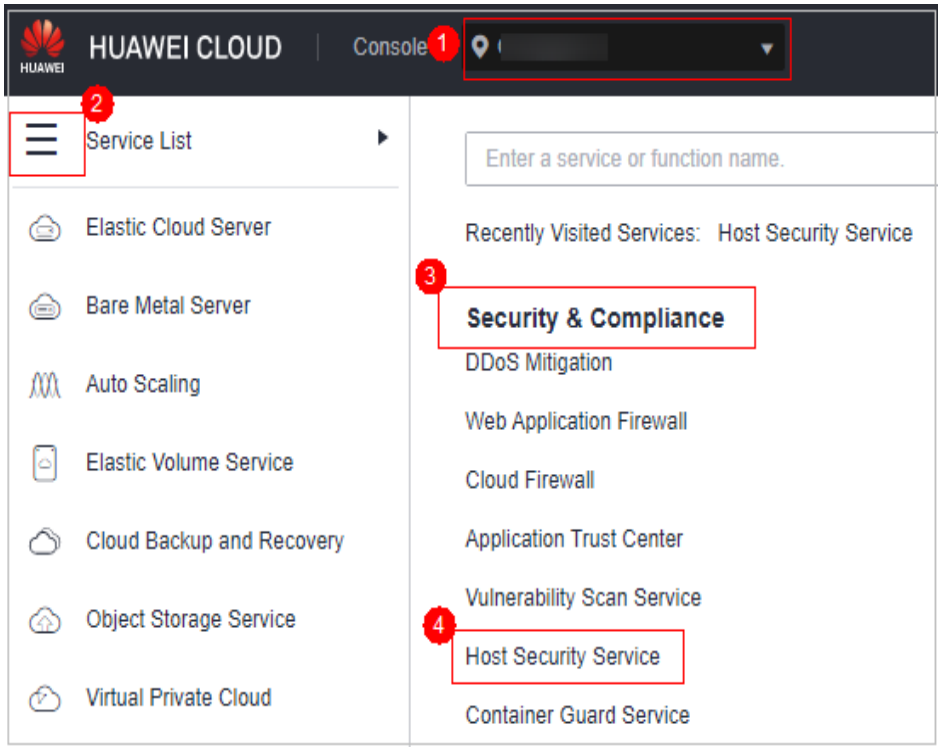
- Se definir **Alarm Receiving Settings** como **Use Message Center settings**, para definir destinatários, vá para a **Message Center** e escolha **Message Receiving Management** > **SMS & Email Settings**. Na área **Security**, clique em **Modify** na linha onde reside **Security event**.
- Se você definir **Alarm Receiving Settings** como **Use SMN topic settings**, é aconselhável criar um tópico de mensagem no serviço SMN como um administrador. Para obter detalhes, consulte **Publicação de uma mensagem**.

Ativação de notificações de alarme

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 1-24 Acessar o HSS



Passo 3 No painel de navegação, escolha **Installation & Configuration** e clique em **Alarm Notifications**. A **Tabela 1-9** descreve os parâmetros.

Figura 1-25 Configurações de alarme

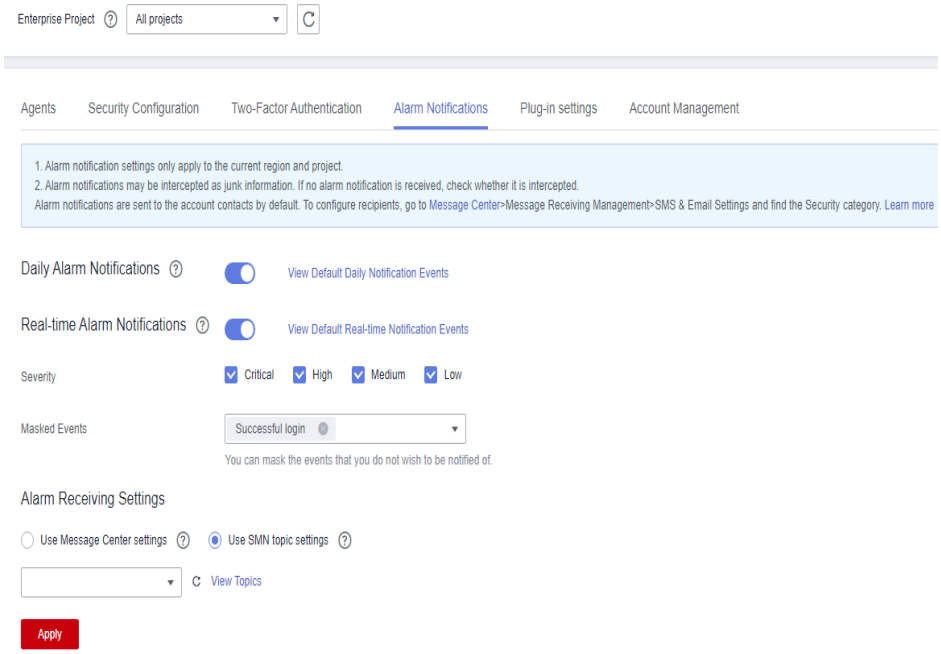


Tabela 1-9 Configurações de alarme

Item de notificação	Descrição	Sugestão
Daily alarm notification	O HSS verifica as contas, diretórios da Web, vulnerabilidades, programas maliciosos e configurações de chave no sistema do servidor às 00:00 todos os dias e envia os resultados resumidos da detecção para os destinatários que você definiu em Central de mensagens ou SMN, dependendo de qual você escolheu. Para visualizar itens de notificação, clique em **View Default Daily Notification Events**.	● Recomenda-se que você receba e verifique periodicamente todo o conteúdo na notificação diária de alarme para eliminar os riscos em tempo hábil. ● As notificações diárias de alarme contêm muitos itens de verificação. Se você quiser enviar as notificações para destinatários definidos em um tópico de SMN, é aconselhável definir o protocolo de tópico para **Email**.
Real-time alarm notification	Quando um invasor invade um servidor, os alarmes são enviados para os destinatários definidos em Central de mensagens ou SMN, dependendo de qual deles você escolheu. Para visualizar itens de notificação, clique em **View Default Real-time Notification Events**.	● É recomendável que você receba todo o conteúdo da notificação de alarme em tempo real e o visualize a tempo. O sistema do HSS monitora a segurança dos servidores em tempo real, detecta a intrusão do invasor e envia notificações de alarme em tempo real para que você possa lidar rapidamente com o problema. ● As notificações de alarme em tempo real são sobre problemas urgentes. Se você quiser enviar as notificações para destinatários definidos em um tópico de SMN, é aconselhável definir o protocolo de tópico para **SMS**.
Severity	Selecione as gravidades dos alarmes sobre os quais deseja ser notificado.	Todas
Masked Events	Selecione os eventos dos quais você não deseja ser notificado. Selecione os eventos a serem mascarados na caixa de listagem suspensa.	Determine os eventos a serem mascarados com base na descrição em **Notificações de alarme**.

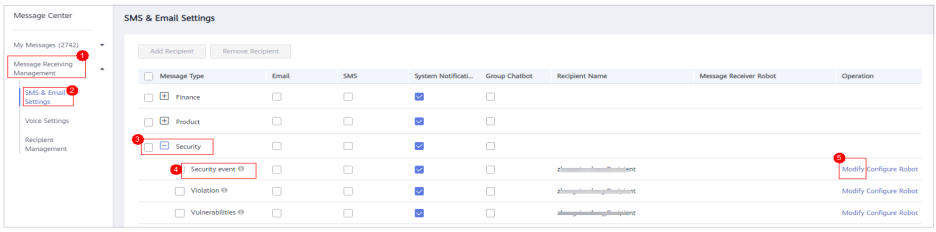
Passo 4 Selecione o modo de notificação de alarme.

- **Use Message Center settings**

Por padrão, as notificações de alarme são enviadas aos destinatários especificados na central de mensagens. Você pode fazer logon na sua conta para verificar as configurações do destinatário.

Para configurar os destinatários, escolha **Message Receive Management** > **SMS & Email Settings**. Na área **Security**, clique em **Modify** na linha onde reside **Security event**.

Figura 1-26 Editar destinatários de mensagens



- **Use SMN topic settings**

  Selecione um tópico disponível na lista suspensa ou clique em **View Topics** e crie um tópico.

  Para criar um tópico, ou seja, configurar um número de telefone celular ou endereço de e-mail para receber notificações de alarme, execute as seguintes etapas:

  a. Crie um tópico. Para obter detalhes, consulte **Criação de um tópico**.

  b. Configure o número de telefone celular ou o endereço de e-mail para receber notificações de alarme, ou seja, adicione uma ou mais assinaturas para o tópico criado. Para obter detalhes, consulte **Adição de uma assinatura**..

  c. Confirme a assinatura. Depois que a assinatura for adicionada, confirme a assinatura conforme solicitado pela mensagem SMS ou pelo e-mail recebido.

     A mensagem de confirmação sobre a assinatura do tópico pode ser considerada spam. Se você não receber a mensagem, verifique se ela é interceptada como spam.

  Você pode criar vários tópicos de notificação com base no plano de O&M e no tipo de notificação de alarme para receber diferentes tipos de notificações de alarme. Para obter detalhes sobre tópicos e assinaturas, consulte o *Guia de usuário da Simple Message Notification*.

Passo 5 Clique em **Apply**. Será exibida uma mensagem indicando que a notificação de alarme foi definida com sucesso.

----Fim

Notificações de alarme

Item de notificação	Item	Descrição
Daily Alarm Notifications O serviço verifica os riscos em seus servidores no início da manhã todos os dias, resume e coleta os resultados de detecção e envia os resultados para o seu telefone celular ou caixa de e-mail às 10:00 todos os dias.		
Ativos	Portas perigosas	Verificar se há portas abertas de alto risco e portas desnecessárias.

Item de notificação	Item	Descrição
	Agente não instalado	Verificar se há servidores sem nenhum agente do HSS instalado e lembrá-lo de instalar o agente nesses servidores em tempo hábil.
Vulnerabilidades	Vulnerabilidades críticas	Detectar vulnerabilidades críticas e corrigi-las em tempo hábil.
Configurações inseguras	Configurações inseguras	Detectar configurações inseguras de principais aplicações que provavelmente serão exploradas por hackers para invadir servidores.
	Senhas fracas comuns	Detectar senhas fracas em MySQL, FTP e contas do sistema.
Invasões	Programas maliciosos	Verificar e lidar com programas maliciosos detectados em um só lugar, incluindo web shells, cavalos de Troia, software de mineração, worms e vírus.
	Rootkits	Detectar ativos do servidor e relatar alarmes para módulos, arquivos e pastas do kernel suspeitos.
	Ransomware	Verificar se há ransomware em mídias como páginas da Web, software, e-mails e mídia de armazenamento. O ransomware pode criptografar e controlar seus ativos de dados, como documentos, e-mails, bancos de dados, código-fonte, imagens e arquivos compactados, para aproveitar a extorsão da vítima.
	Web shells	Verificar se os arquivos (frequentemente arquivos PHP e JSP) detectados pelo HSS em seus diretórios da Web são web shells. ● As informações de web shell incluem o caminho do arquivo do cavalo de Troia, o status, a hora da primeira descoberta e a hora da última descoberta. Você pode optar por ignorar o aviso em arquivos confiáveis. ● Você pode usar a função de detecção manual para detectar web shells em servidores.
	Shells reversos	Monitorar o comportamento do processo do usuário em tempo real para detectar shells reversos causados por conexões inválidas. Os shells reversos podem ser detectados para protocolos, incluindo TCP, UDP e ICMP.
	Explosões de vulnerabilidade do Redis	Detectar as modificações feitas pelo processo de Redis nos principais diretórios em tempo real e relatar alarmes.

Item de notificação	Item	Descrição
	Explosões de vulnerabilidade de Hadoop	Detectar as modificações feitas pelo processo de Hadoop nos principais diretórios em tempo real e relatar alarmes.
	Explorações de vulnerabilidade do MySQL	Detectar as modificações feitas pelo processo do MySQL nos principais diretórios em tempo real e informe os alarmes.
	Escalonamentos de privilégio de arquivo	Verificar os escalonamentos de privilégios de arquivos em seu sistema.
	Escalonamentos de privilégio do processo	As seguintes operações de escalonamento de privilégios de processo podem ser detectadas: ● Escalonamento de privilégio de raiz explorando vulnerabilidades do programa SUID ● Escalonamento de privilégios de raiz explorando vulnerabilidades do kernel
	Alterações em arquivo crítico	Receber alarmes quando arquivos críticos do sistema forem modificados.
	Alterações de arquivo/ diretório	Os arquivos e diretórios do sistema são monitorados. Quando um arquivo ou diretório é modificado, um alarme é gerado, indicando que o arquivo ou diretório pode ser adulterado.
	Comportamentos anormais do processo	Verificar os processos em servidores, incluindo seus IDs, linhas de comando, caminhos de processo e comportamento. Enviar alarmes sobre operações de processo não autorizadas e intrusões. O seguinte comportamento anormal do processo pode ser detectado: ● Uso anormal da CPU ● Processos de acesso a endereços IP maliciosos ● Aumento anormal nas conexões de processos simultâneos
	Execução de comandos de alto risco	Verificar os comandos executados em tempo real e gerar alarmes se os comandos de alto risco forem detectados.
	Shells anormais	Detectar ações em shells anormais, incluindo mover, copiar e excluir arquivos de shell e modificar as permissões de acesso e links físicos dos arquivos.

Item de notificação	Item	Descrição
	Tarefas suspeitas de crontab	Verificar e listar serviços iniciados automaticamente, tarefas agendadas, bibliotecas dinâmicas pré-carregadas, chaves de registro de execução e pastas de inicialização. Você pode ser notificado imediatamente quando itens anormais de inicialização automática forem detectados e localizar rapidamente os cavalos de Troia.
	Ataques de força bruta	Verificar se há tentativas de ataque de força bruta e ataques de força bruta bem-sucedidos. ● Suas contas estão protegidas contra ataques de força bruta. O HSS bloqueará os hosts atacantes ao detectar esses ataques. ● Acionar um alarme se um usuário efetuar logon no host por meio de um ataque de força bruta.
	Logons anormais	Verificar e lidar com logons remotos. Se a localização de logon de um usuário não for qualquer localização de logon comum que você definiu, um alarme será acionado.
	Contas inválidas	Verificar contas em servidores e listar contas suspeitas em tempo hábil.
	Escapes de vulnerabilidade	O serviço relata um alarme se detectar o comportamento do processo de container que corresponde ao comportamento de vulnerabilidades conhecidas (como Dirty COW, ataque de força bruta, runC e shocker).
	Escapes de arquivo	O serviço reporta um alarme se ele detecta que um processo de container acessa um diretório de arquivo de chave (por exemplo, **/etc/shadow** ou **/etc/crontab**). Os diretórios que atendem às regras de mapeamento de diretórios de containers também podem acionar esses alarmes.
	Processos de container anormal	Os serviços de container geralmente são simples. Se você tiver certeza de que apenas processos específicos são executados em um container, poderá adicionar os processos à lista branca de uma política e vincular a política ao container. O serviço relata um alarme se detectar que um processo que não está na lista branca está sendo executado no container.
	Inicializações anormais de containers	Verificar se há configurações de parâmetros inseguros usadas durante a inicialização do container. Determinados parâmetros de inicialização especificam permissões de container. Se suas configurações forem inadequadas, elas podem ser exploradas por invasores para invadir containers.

Item de notificação	Item	Descrição
	Chamadas de sistema de alto risco	Os usuários podem executar tarefas em kernels por chamadas do sistema de Linux. O serviço relata um alarme se detectar uma chamada de alto risco, como **open_by_handle_at**, **ptrace**, **setns** e **reboot**.
	Acesso a arquivos confidenciais	Detectar comportamentos de acesso suspeitos (como escalonamento e persistência de privilégios) em arquivos importantes.
	Prevenção de adulteração na páginas da Web para servidores de Windows	Proteger os arquivos de página da Web estáticos em seus servidores de site do Windows contra modificações maliciosas.
	Prevenção contra adulteração na páginas da Web para servidores de Linux	Proteger os arquivos de página da Web estáticos em seus servidores de sites do Linux contra modificações maliciosas.
	WTP dinâmica	Proteger os arquivos de página da Web estáticos em seus servidores de sites do Windows e Linux contra modificações maliciosas.
	Proteção da aplicação	Proteger as aplicações em execução. Você simplesmente precisa adicionar sondas às aplicações, sem ter que modificar os arquivos da aplicação. Atualmente, apenas servidores de Linux são suportados e apenas aplicações Java podem ser conectadas.
Real-Time Alarm Notifications Quando ocorre um evento, uma notificação de alarme é imediatamente enviada.		
Invasões	Programas maliciosos	Verificar e lidar com programas maliciosos detectados em um só lugar, incluindo web shells, cavalos de Troia, software de mineração, worms e vírus.
	Rootkits	Detectar ativos do servidor e relatar alarmes para módulos, arquivos e pastas do kernel suspeitos.
	Ransomware	Verificar se há ransomware em mídias como páginas da Web, software, e-mails e mídia de armazenamento. O ransomware pode criptografar e controlar seus ativos de dados, como documentos, e-mails, bancos de dados, código-fonte, imagens e arquivos compactados, para aproveitar a extorsão da vítima.

Item de notificação	Item	Descrição
	Web shells	Verificar se os arquivos (frequentemente arquivos PHP e JSP) detectados pelo HSS em seus diretórios da Web são web shells. ● As informações de web shell incluem o caminho do arquivo do cavalo de Troia, o status, a hora da primeira descoberta e a hora da última descoberta. Você pode optar por ignorar o aviso em arquivos confiáveis. ● Você pode usar a função de detecção manual para detectar web shells em servidores.
	Shells reversos	Monitorar o comportamento do processo do usuário em tempo real para detectar shells reversos causados por conexões inválidas. Os shells reversos podem ser detectados para protocolos, incluindo TCP, UDP e ICMP.
	Explosões de vulnerabilidade do Redis	Detectar as modificações feitas pelo processo de Redis nos principais diretórios em tempo real e relatar alarmes.
	Explosões de vulnerabilidade de Hadoop	Detectar as modificações feitas pelo processo de Hadoop nos principais diretórios em tempo real e relatar alarmes.
	Explorações de vulnerabilidade do MySQL	Detectar as modificações feitas pelo processo do MySQL nos principais diretórios em tempo real e informe os alarmes.
	Escalonamentos de privilégio de arquivo	Verificar os escalonamentos de privilégios de arquivos em seu sistema.
	Escalonamentos de privilégio do processo	As seguintes operações de escalonamento de privilégios de processo podem ser detectadas: ● Escalonamento de privilégio de raiz explorando vulnerabilidades do programa SUID ● Escalonamento de privilégios de raiz explorando vulnerabilidades do kernel
	Alterações em arquivo crítico	Receber alarmes quando arquivos críticos do sistema forem modificados.
	Alterações de arquivo/ diretório	Os arquivos e diretórios do sistema são monitorados. Quando um arquivo ou diretório é modificado, um alarme é gerado, indicando que o arquivo ou diretório pode ser adulterado.

Item de notificação	Item	Descrição
	Detecção de comportamento anormal do processo	Verificar os processos em servidores, incluindo seus IDs, linhas de comando, caminhos de processo e comportamento. Enviar alarmes sobre operações de processo não autorizadas e intrusões. O seguinte comportamento anormal do processo pode ser detectado: ● Uso anormal da CPU ● Processos de acesso a endereços IP maliciosos ● Aumento anormal nas conexões de processos simultâneos
	Detecção de execução de comando de alto risco	Verificar os comandos executados em tempo real e gerar alarmes se os comandos de alto risco forem detectados.
	Detecção de shell anormal	Detectar ações em shells anormais, incluindo mover, copiar e excluir arquivos de shell e modificar as permissões de acesso e links físicos dos arquivos.
	Tarefas suspeitas de crontab	Verificar e listar serviços iniciados automaticamente, tarefas agendadas, bibliotecas dinâmicas pré-carregadas, chaves de registro de execução e pastas de inicialização. Você pode ser notificado imediatamente quando itens anormais de inicialização automática forem detectados e localizar rapidamente os cavalos de Troia.
	Estatística de exceção	Verificar e lidar com logons remotos. Se a localização de logon de um usuário não for qualquer localização de logon comum que você definiu, um alarme será acionado.
	Conta inválida	Verificar contas em servidores e listar contas suspeitas em tempo hábil.
	Escapes de vulnerabilidade	O serviço relata um alarme se detectar o comportamento do processo de container que corresponde ao comportamento de vulnerabilidades conhecidas (como Dirty COW, ataque de força bruta, runC e shocker).
	Escapes de arquivo	O serviço reporta um alarme se ele detecta que um processo de container acessa um diretório de arquivo de chave (por exemplo, **/etc/shadow** ou **/etc/crontab**). Os diretórios que atendem às regras de mapeamento de diretórios de containers também podem acionar esses alarmes.

Item de notificação	Item	Descrição
	Processos de container anormal	Os serviços de container geralmente são simples. Se você tiver certeza de que apenas processos específicos são executados em um container, poderá adicionar os processos à lista branca de uma política e vincular a política ao container. O serviço relata um alarme se detectar que um processo que não está na lista branca está sendo executado no container.
	Inicializações anormais de containers	Verificar se há configurações de parâmetros inseguros usadas durante a inicialização do container. Determinados parâmetros de inicialização especificam permissões de container. Se suas configurações forem inadequadas, elas podem ser exploradas por invasores para invadir containers.
	Chamadas de sistema de alto risco	Os usuários podem executar tarefas em kernels por chamadas do sistema de Linux. O serviço relata um alarme se detectar uma chamada de alto risco, como **open_by_handle_at**, **ptrace**, **setns** e **reboot**.
	Acesso a arquivos confidenciais	Detectar comportamentos de acesso suspeitos (como escalonamento e persistência de privilégios) em arquivos importantes.
	Prevenção de adulteração na páginas da Web para servidores de Windows	Proteger os arquivos de página da Web estáticos em seus servidores de site do Windows contra modificações maliciosas.
	Prevenção contra adulteração na páginas da Web para servidores de Linux	Proteger os arquivos de página da Web estáticos em seus servidores de sites do Linux contra modificações maliciosas.
	WTP dinâmica	Proteger os arquivos de página da Web estáticos em seus servidores de sites do Windows e Linux contra modificações maliciosas.
	Proteção da aplicação	Proteger as aplicações em execução. Você simplesmente precisa adicionar sondas às aplicações, sem ter que modificar os arquivos da aplicação. Atualmente, apenas servidores de Linux são suportados e apenas aplicações Java podem ser conectadas.

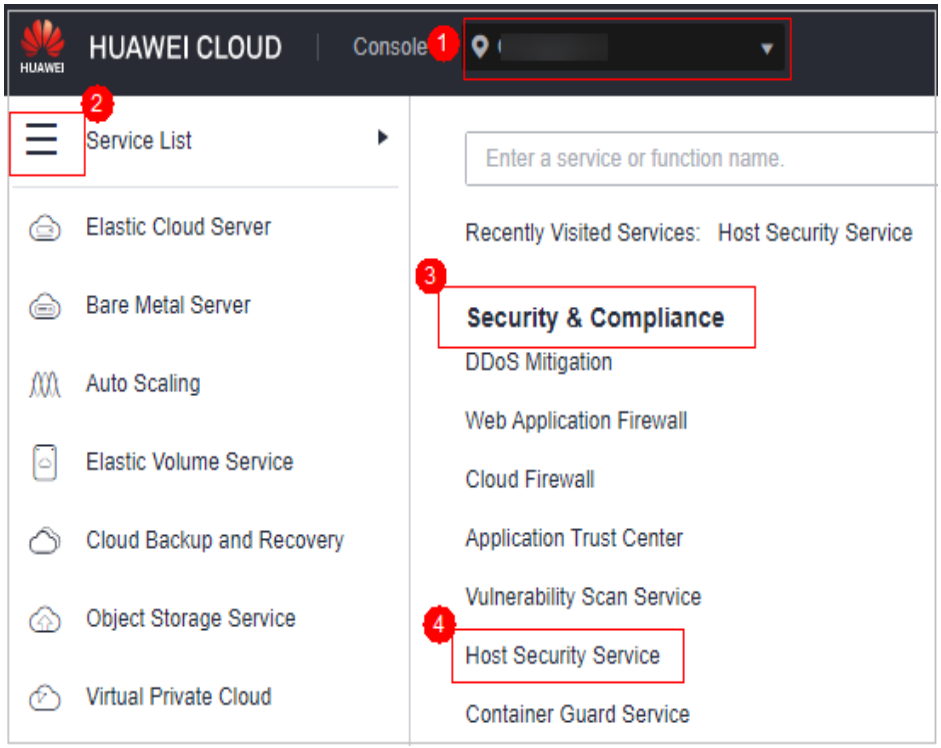
1.7 Instalação e configuração

Depois que a proteção estiver ativada, você poderá configurar as localizações de logon comuns, os endereços IP de logon comuns e a lista branca de endereços IP de logon SSH. Você também pode ativar o isolamento automático e a eliminação de programas maliciosos.

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 1-27 Acessar o HSS



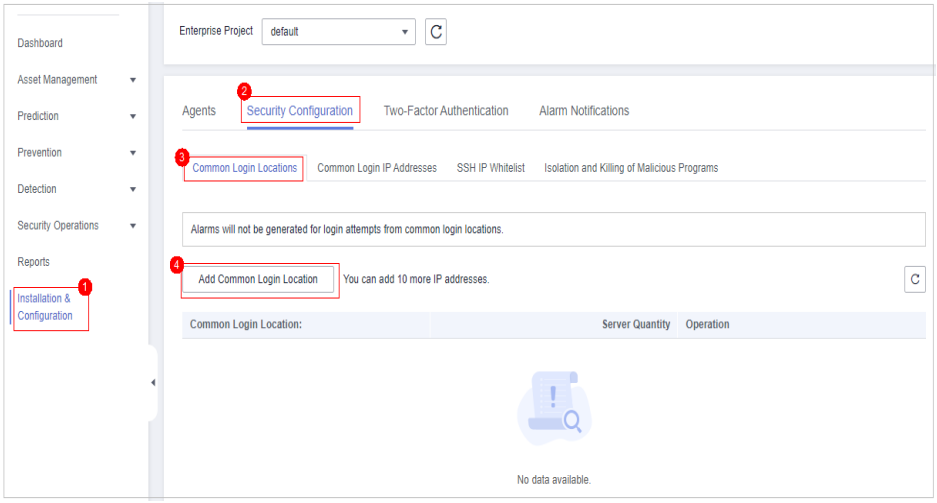
----Fim

Configuração de localizações comuns de logon

Depois de configurar localizações de logon comuns, o HSS gerará alarmes nos logons de outras localizações de logon. Um servidor pode ser adicionado a várias localizações de logon.

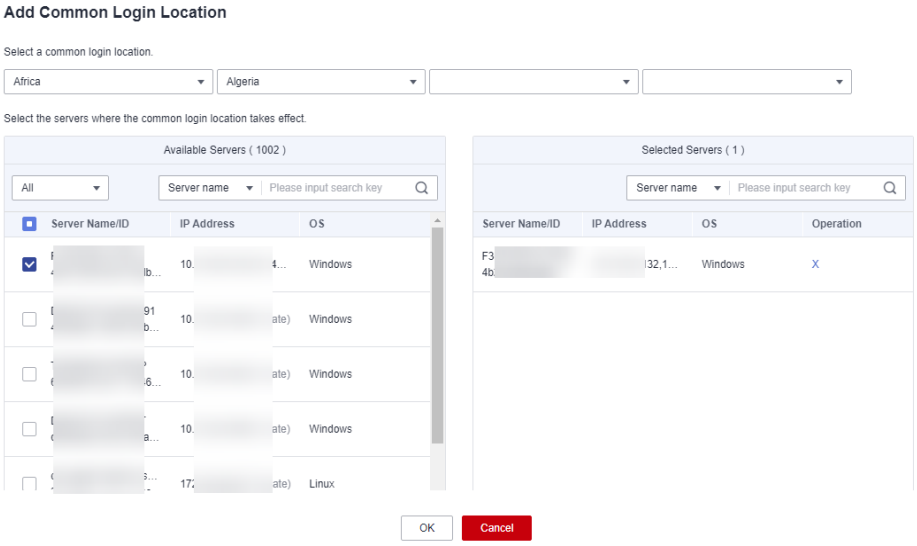
Passo 1 Escolha **Installation & Configuration** e clique na guia **Security Configuration**. Clique em **Common Login Locations** e clique em **Add Common Login Location**.

Figura 1-28 Adicionar uma localização de logon comum



Passo 2 Na caixa de diálogo que é exibida, selecione uma localização geográfica e selecione servidores. Confirme as informações e clique em **OK**.

Figura 1-29 Configuração de localizações comuns de logon



Passo 3 Retorne à guia **Security Configuration** da página **Installation & Configuration**. Verifique se as localizações adicionadas são exibidas na subguia **Common Login Locations**.

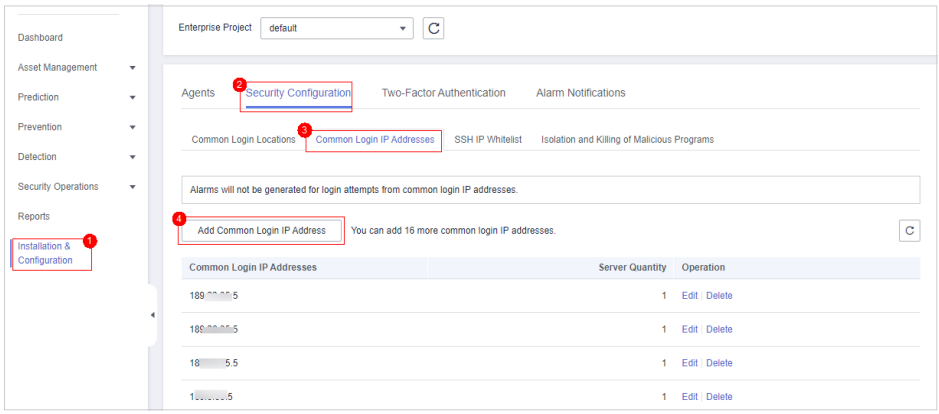
----Fim

Configuração de endereços IP comuns de logon

Depois de configurar endereços IP comuns, o HSS gerará alarmes nos logons de outros endereços IP.

Passo 1 Escolha **Installation & Configuration** e clique na guia **Security Configuration**. Clique em **Common Login IP Addresses** e clique em **Add Common Login IP Address**.

Figura 1-30 Adicionar um endereço IP de logon comum

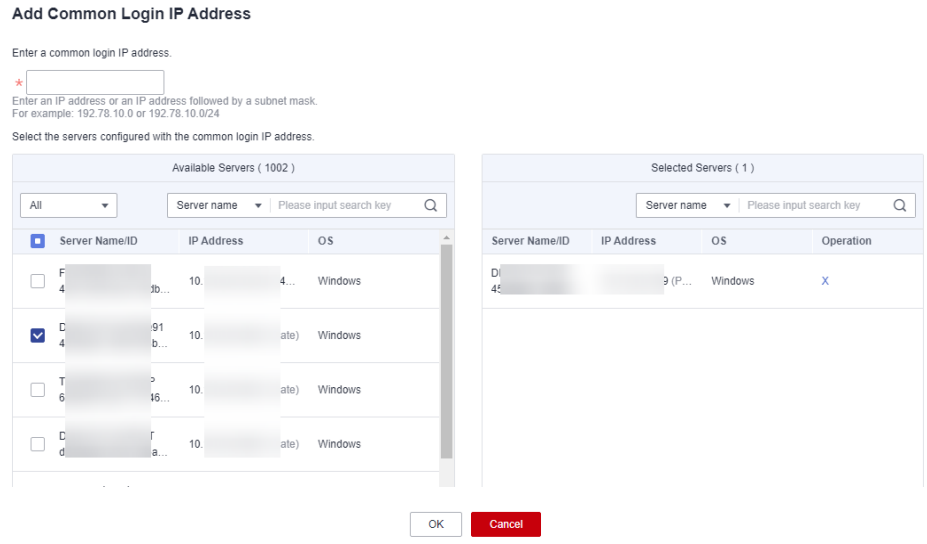


Passo 2 Na caixa de diálogo exibida, insira um endereço IP e selecione servidores. Confirme as informações e clique em **OK**.

NOTA

- Um endereço IP de logon comum deve ser um endereço IP público ou segmento de endereço IP. Caso contrário, você não pode efetuar logon remotamente no servidor no modo SSH.
- Apenas um endereço IP pode ser adicionado por vez. Para adicionar vários endereços IP, repita as operações até que todos os endereços IP sejam adicionados. Até 20 endereços IP podem ser adicionados.

Figura 1-31 Inserir um endereço IP de logon comum



Passo 3 Retorne à guia **Security Configuration** da página **Installation & Configuration**. Verifique se as localizações adicionadas são exibidas na subguia **Common Login IP Addresses**.

----Fim

Configuração de uma lista branca de endereços IP de logon SSH

A lista branca de logon SSH controla o acesso SSH aos servidores para evitar quebra de conta.

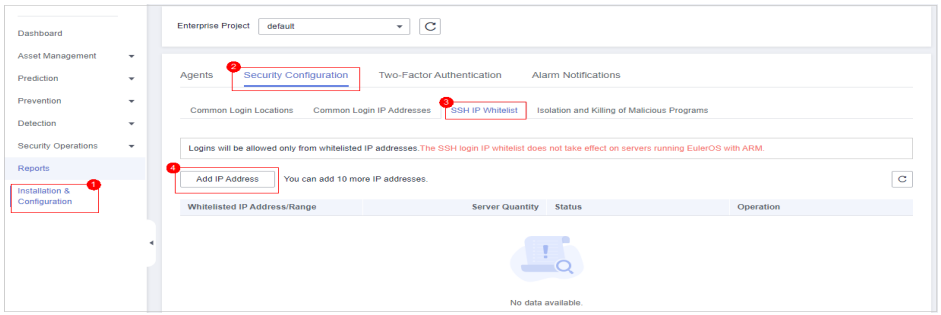
NOTA

- Uma conta pode ter até 10 endereços IP de logon SSH na lista branca.
- Depois de configurar uma lista branca de endereços IP de logon SSH, os logons SSH serão permitidos apenas a partir de endereços IP na lista branca.
  - Antes de ativar esta função, certifique-se de que todos os endereços IP que precisam iniciar logons SSH sejam adicionados à lista branca. Caso contrário, você não pode fazer logon remotamente em seu servidor usando SSH.

    Se o seu serviço precisa acessar um servidor, mas não necessariamente via SSH, você não precisa adicionar seu endereço IP à lista branca.
  - Tenha cuidado ao adicionar um endereço IP à lista branca. Isso fará com que o HSS não restrinja mais o acesso deste endereço IP aos seus servidores.

Passo 1 Escolha **Installation & Configuration** e clique na guia **Security Configuration**. Clique em **SSH IP Whitelist** e clique em **Add IP Address**.

Figura 1-32 Configuração de uma lista branca de endereços IP

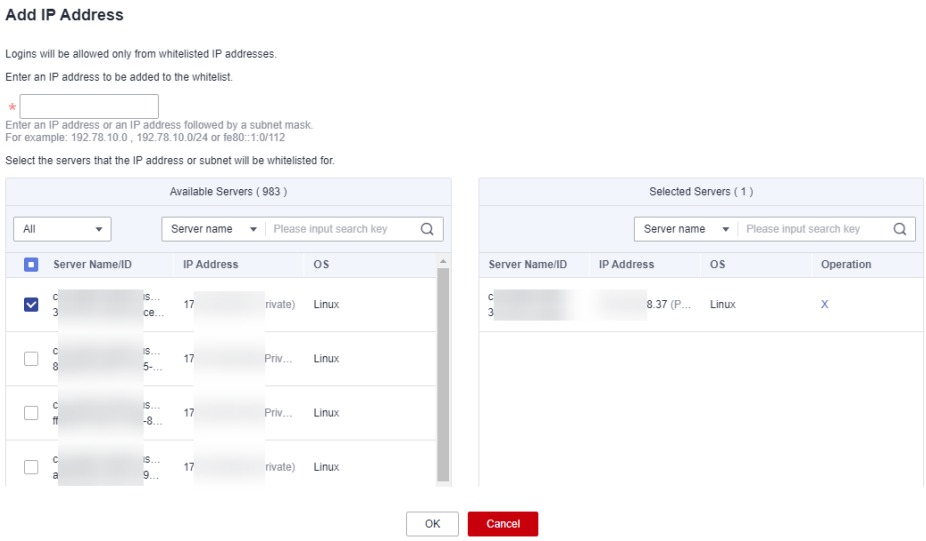


Passo 2 Na caixa de diálogo exibida, insira um endereço IP e selecione servidores. Confirme as informações e clique em **OK**.

NOTA

- Um endereço IP de logon comum deve ser um endereço IP público ou segmento de endereço IP. Caso contrário, você não pode efetuar logon remotamente no servidor no modo SSH.
- Apenas um endereço IP pode ser adicionado por vez. Para adicionar vários endereços IP, repita as operações até que todos os endereços IP sejam adicionados.

Figura 1-33 Inserir um endereço IP



Passo 3 Retorne à guia **Security Configuration** da página **Installation & Configuration**. Verifique se as localizações adicionadas são exibidas na subguia **Common Login IP Addresses**.

----Fim

Isolar e eliminar programas maliciosos

O HSS isola e elimina automaticamente os programas maliciosos identificados, como web shells, cavalos de Troia e worms, eliminando riscos de segurança.

Os programas são isolados e eliminados com base em seus índices de confiança. Um índice alto indica uma alta probabilidade de que o programa detectado seja um programa malicioso. Para evitar parar por engano programas confiáveis e afetar serviços, apenas os programas suspeitos com um índice de confiança de 95 ou superior são automaticamente isolados e eliminados. Você pode isolar e eliminar manualmente programas com índices mais baixos. Para obter detalhes, consulte **Manipulação de alarmes de servidor**.

NOTA

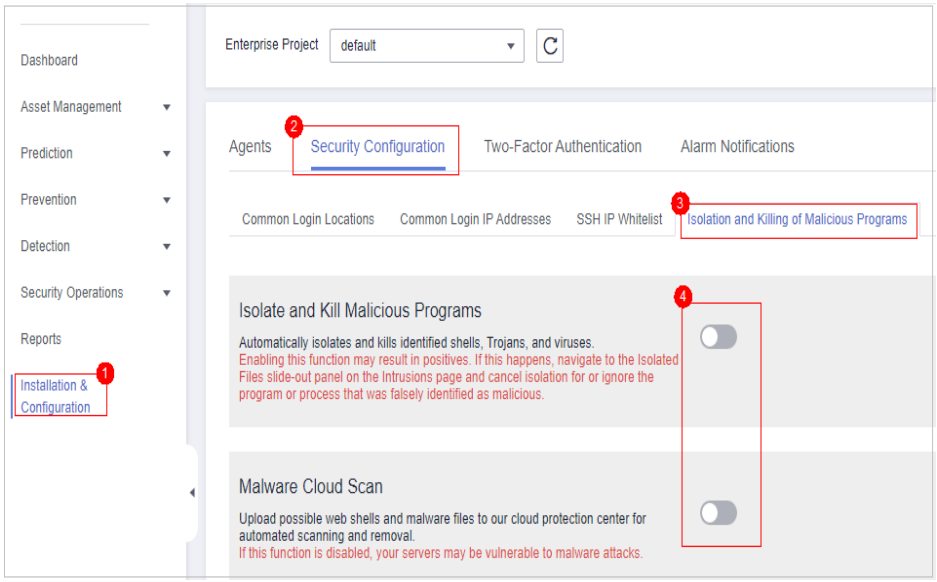
Para verificar o índice de confiança de um programa suspeito, escolha **Detection** > **Alarms** no console do HSS e clique em **Server Alarms**. Clique no nome de um alarme de programa malicioso para ver os detalhes.

Passo 1 Escolha **Installation & Configuration** e clique na guia **Security Configuration**. Clique na guia **Isolation and Killing of Malicious Programs** e ative **Isolate and Kill Malicious Programs** e **Malware Cloud Scan**.

NOTA

Depois que a função de verificação em nuvem estiver ativada, todos os servidores do HSS serão verificados. Algumas edições de cota do HSS podem oferecer suporte apenas a recursos limitados de verificação. Portanto, você é aconselhado a ativar a edição empresarial ou superior para desfrutar de todos os recursos da função de isolamento e eliminação.

Figura 1-34 Ativar isolamento e eliminação



Passo 2 Na caixa de diálogo de confirmação, clique em **OK** para ativar o isolamento e a eliminação de programas maliciosos e a verificação de malware na nuvem.

Isolamento e eliminação automáticos podem causar falsos positivos. Você pode escolher **Intrusions** > **Events** para exibir programas maliciosos isolados. Você pode cancelar o isolamento ou ignorar os programas maliciosos relatados incorretamente. Para obter detalhes, consulte **Visualização de alarmes de intrusão**.

AVISO

- Quando um programa é isolado e eliminado, o processo do programa é encerrado imediatamente. Para evitar impacto nos serviços, verifique o resultado da detecção e cancele o isolamento ou deixe de ignorar programas maliciosos informados incorretamente (se houver).
- Se **Isolate and Kill Malicious Programs** estiver definido como **Disable** na guia **Isolation and Killing of Malicious Programs**, o HSS gerará um alarme quando detectar um programa malicioso.

  Para isolar e eliminar os programas maliciosos que acionaram os alarmes, escolha **Intrusions** > **Events** e clique em **Malicious program**.

----Fim

Ativar a 2FA

- A autenticação de dois fatores (2FA) requer que os usuários forneçam códigos de verificação antes de efetuar logon. Os códigos serão enviados para seus telefones celulares ou caixas de e-mail.
- Você tem que escolher um tópico SMN para servidores onde a 2FA está ativada. O tópico especifica os destinatários dos códigos de verificação de logon e o HSS autenticará os usuários de logon de acordo.

Pré-requisitos

- Você criou um tópico de mensagem cujo protocolo é SMS ou e-mail.
- A proteção do servidor foi ativada.
- Para ativar a 2FA, você precisa desativar o firewall do SELinux.
- Em um servidor do Windows, a 2FA pode entrar em conflito com o G01 e o 360 Guard (edição do servidor). Você é aconselhado a detê-los.

Restrições e limitações

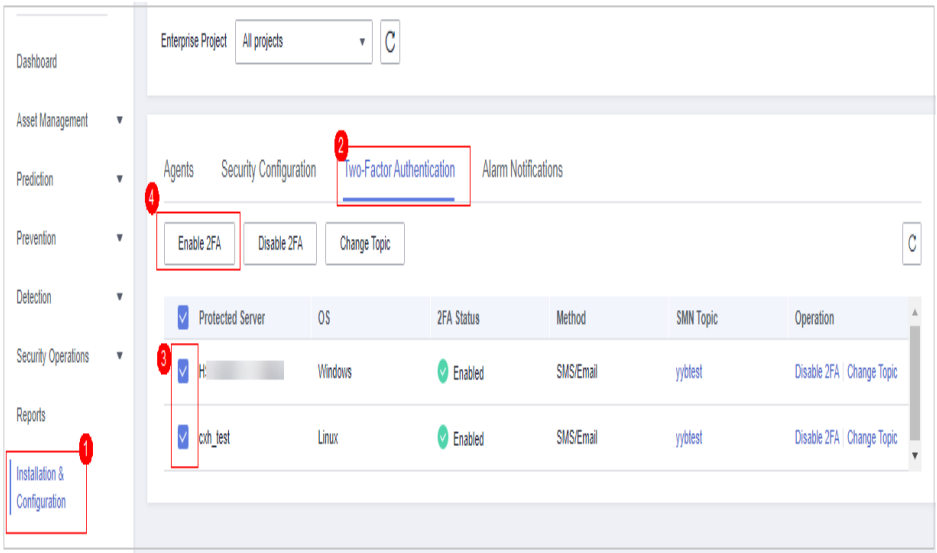
Se a 2FA estiver ativada, ela poderá ser usada apenas nos seguintes cenários:

- Linux: a senha SSH é usada para efetuar logon em um ECS e a versão do OpenSSH é anterior à 8.
- Windows: o arquivo RDP é usado para efetuar logon em um ECS do Windows.

Procedimento

Passo 1 Na guia **Two-Factor Authentication**, selecione servidores e clique em **Enable 2FA**. Como alternativa, clique em **Enable** na coluna **Operation**.

Figura 1-35 Ativar a 2FA



Passo 2 Na caixa de diálogo **Enable 2FA** exibida, selecione um modo de autenticação.

- **SMS/Email**

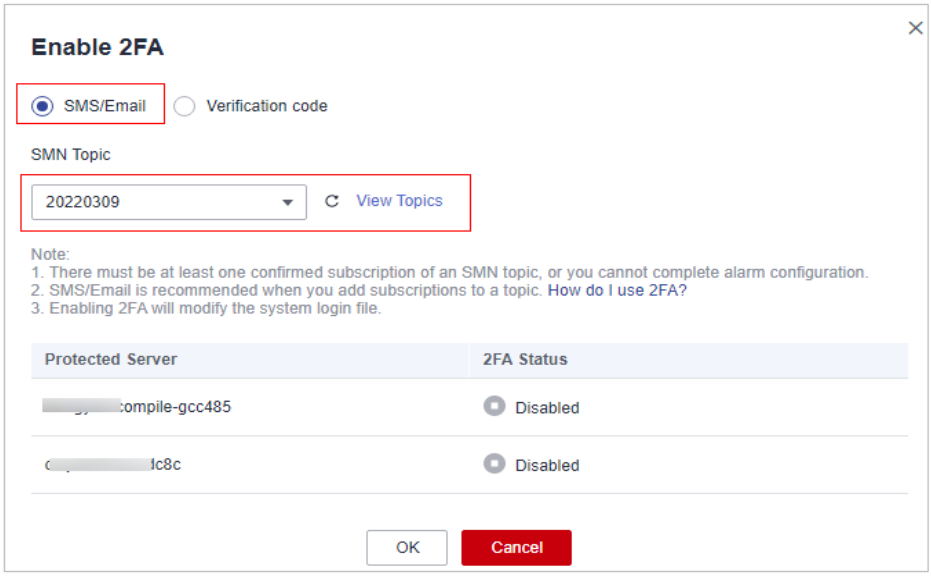
  Você precisa selecionar um tópico SMN para verificação de SMS e e-mail.

  – A lista suspensa exibe apenas os tópicos de notificação que foram confirmados.

  – Se não houver nenhum tópico, clique em **View** para criar um. Para obter detalhes, consulte **Criação de um tópico**.

  – Durante a autenticação, todos os números de celular e endereços de e-mail especificados no tópico receberão um SMS ou e-mail de verificação. Você pode excluir números de celular e endereços de e-mail que não precisam receber mensagens de verificação.

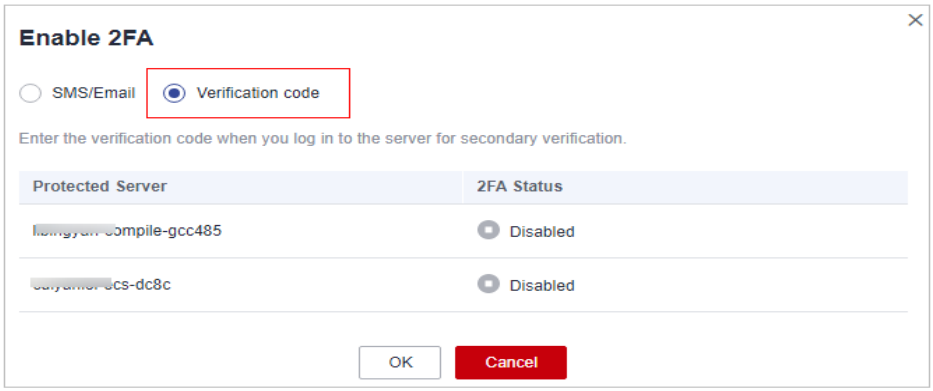
Figura 1-36 SMS/Email



- **Verification code**

  Use o código de verificação que você recebe em tempo real para verificação.

Figura 1-37 Configuração do método para Verification code



Passo 3 Clique em **OK**. Depois que a 2FA é ativada, leva cerca de 5 minutos para que a configuração entre em vigor.

AVISO

Quando você faz logon em um servidor do Windows remoto a partir de outro servidor do Windows em que a 2FA está ativada, é necessário adicionar manualmente as credenciais no segundo. Caso contrário, o logon falhará.

Para adicionar credenciais, escolha **Start** > **Control Panel** e clique em **User Accounts**. Clique em **Manage your credentials** e, em seguida, clique em **Add a Windows credential**. Adicione o nome de usuário e a senha do servidor remoto que você deseja acessar.

----Fim

2 Painel

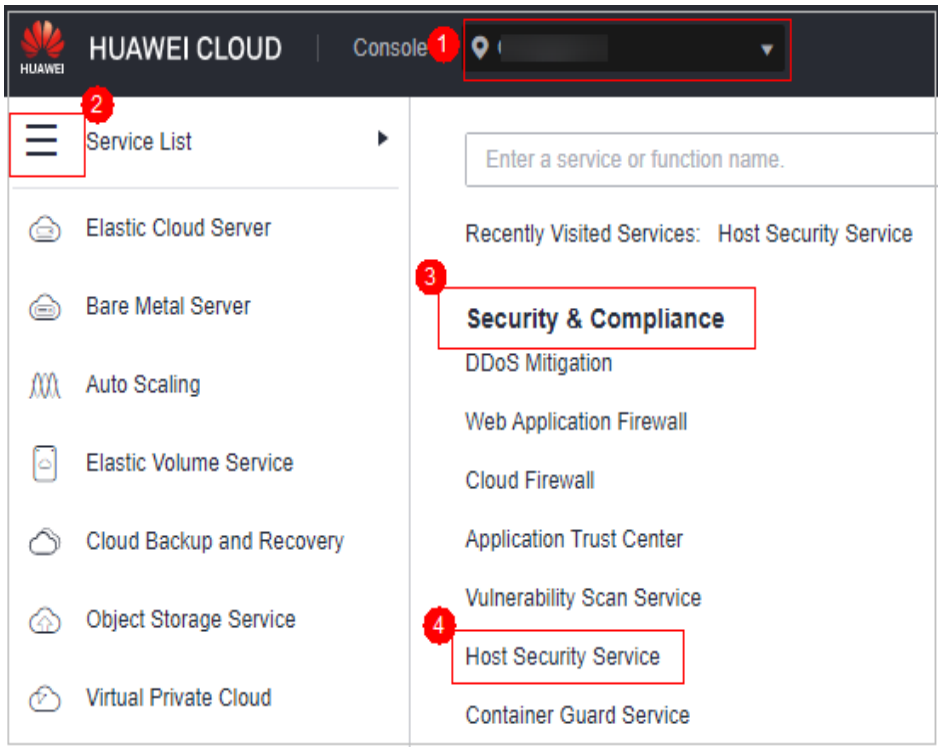
No painel de HSS, você pode verificar a pontuação de segurança, os riscos e a visão geral de proteção de todos os seus ativos em tempo real, incluindo servidores e containers.

Visualização da página do painel

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 **Dashboard** e verifique a visão geral de segurança. Para obter mais informações, consulte **Tabela 2-1**.

NOTA

Se seus servidores forem gerenciados por projetos empresariais, você poderá selecionar o projeto empresarial de destino para visualizar ou operar as informações de ativo e detecção.

Figura 2-2 Painel

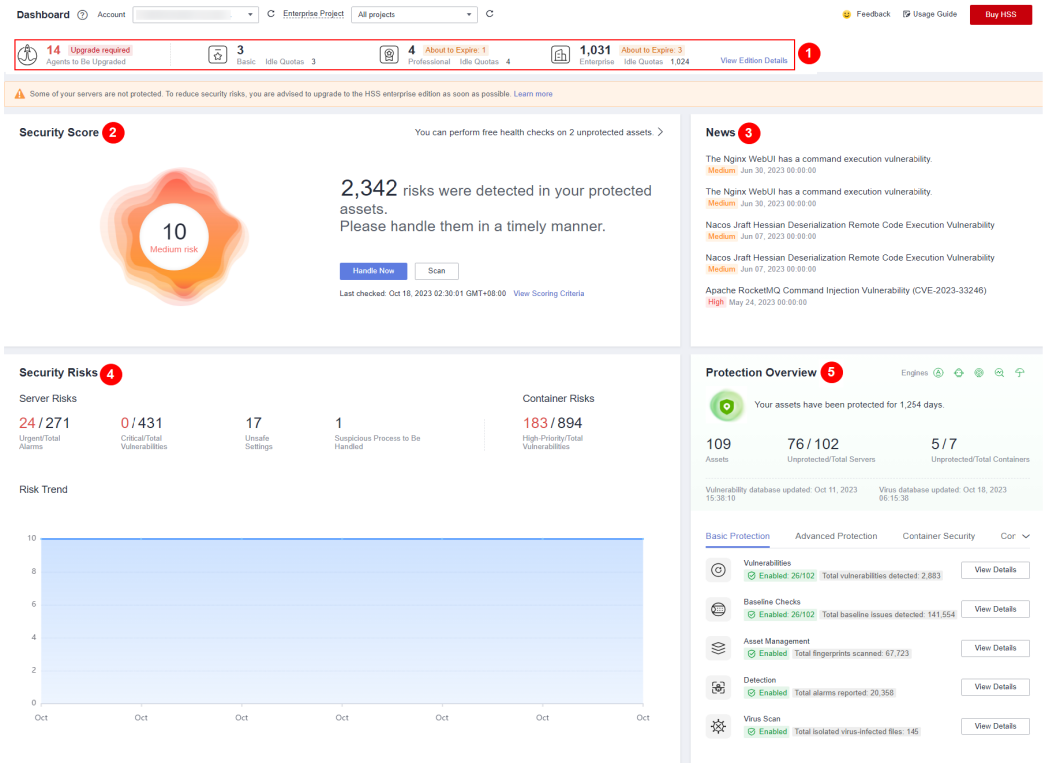


Tabela 2-1 Componentes do painel

Componente	Descrição
Cotas e agentes a serem atualizados (componente 1 em **Figura 2-2**).	Cotas de edição do HSS e seu uso e o número de agentes a serem atualizados. ● Clique no número de cotas para ir para a lista de cotas. ● Clique no número de agentes a serem atualizados para ir para a lista de agentes e atualizar os agentes. **NOTA** O HSS será atualizado continuamente para fornecer novos recursos e corrigir bugs. Para aproveitar os melhores recursos do HSS, atualize o agente para a versão mais recente em tempo hábil. Para obter detalhes, consulte **Atualização do agente**.

Componente	Descrição
Security Score (componente 2 em **Figura 2-2**)	A pontuação de segurança está no intervalo de 0 a 100. A pontuação padrão para ativos sem risco é de 100. Os pontos são deduzidos com base nos riscos de linha de base, riscos de vulnerabilidade, riscos de intrusão e riscos de ativos. Uma pontuação baixa indica altos riscos de segurança em ativos. Para obter detalhes sobre os critérios de pontuação e como melhorar sua pontuação, consulte **Dedução da pontuação de segurança**.
News (componente 3 em **Figura 2-2**)	Últimas informações sobre vulnerabilidades.

Componente	Descrição
Security Risks (componente 4 em **Figura 2-2**)	Riscos de segurança detectados pelo HSS em seus ativos. ● **Server Risks** – **Urgent/Total Alarms**: número de alarmes que precisam ser manuseados imediatamente e o número total de alarmes. Você pode clicar no número de alarmes urgentes para ir para a página **Alarms** e lidar com os alarmes. Para mais detalhes, consulte **Manipulação de alarmes do servidor**. – **Critical/Total Vulnerabilities**: número de vulnerabilidades críticas e o número total de vulnerabilidades. Você pode clicar no número de vulnerabilidades críticas para ir para a página **Vulnerabilities** e lidar com as vulnerabilidades. Para mais detalhes, consulte **Manipulação de vulnerabilidades**. – **Unsafe Settings**: número de riscos de linha de base a serem tratados. Você pode clicar no número para ir para a página **Baseline Checks** e corrigir os riscos da linha de base. Para mais detalhes, consulte **Correção de configurações inseguras**. – **Suspicious Processes to Be Handled**: número total de processos suspeitos a serem tratados. Você pode clicar no número de processos suspeitos a serem manipulados para ir para a página **Application Process Control** e lidar com processos suspeitos. Para mais detalhes, consulte **Verificação e tratamento de processos suspeitos**. ● **Container Risks** **High-Priority/Total Vulnerabilities**: número de vulnerabilidades de alto risco e o número total de vulnerabilidades. Você pode clicar no número de vulnerabilidades de alta prioridade para acessar a guia **Image Vulnerabilities** e verificar as sugestões de correção de vulnerabilidades. Para mais detalhes, consulte **Vulnerabilidades de imagem**. ● **Risk Trend** Tendência do risco dos ativos nos últimos sete dias.

Componente	Descrição
Protection Overview (componente 5 em **Figura 2-2**)	Visão geral da proteção de ativos. ● **Assets**: número total de ativos na região atual. Você pode clicar no número total de ativos para ir para a página **Assets** para visualizar a distribuição de ativos e o status de proteção. ● **Unprotected/Total Servers**: número de servidores desprotegidos e o número total de servidores. Você pode clicar no número de servidores desprotegidos para acessar a página **Servers & Quota** para visualizar os servidores e ativar a proteção. Para mais detalhes, consulte **Habilitação de HSS**. ● **Unprotected/Total Containers**: número de containers desprotegidos e o número total de containers. Você pode clicar no número de containers desprotegidos para ir para a página **Containers & Quota** para visualizar containers e ativar a proteção. Para mais detalhes, consulte **Ativação da proteção de nó de container**. ● Status do recurso de segurança: o número de servidores protegidos por cada recurso e o número de itens detectados por cada recurso. Você pode clicar em **View Details** para ir para a página de recursos correspondente.
Melhores práticas	Melhores práticas do HSS. Clique em um título para visualizar os detalhes.
Pergunta frequente	Melhores perguntas frequentes sobre HSS. Clique em um título para visualizar os detalhes.
Serviços relacionados	Serviços de segurança relacionados ao HSS. Clique em um nome de serviço para acessar seu console.

----Fim

Dedução da pontuação de segurança

O HSS calcula sua pontuação de segurança com base em itens de segurança detectados (vulnerabilidades, linhas de base, intrusões, ativos e imagens) e ativos desprotegidos. A pontuação completa é 100. A pontuação completa de cada categoria é a seguinte:

- Nenhuma vulnerabilidade detectada: 20
- Nenhum risco de linha de base detectado: 20
- Nenhum risco de intrusão detectado: 30
- Nenhum risco de ativo detectado: 10
- Nenhum risco de imagem detectado: 10
- Nenhum ativo desprotegido: 10

Os pontos são deduzidos toda vez que um risco é detectado em uma categoria até que todos os pontos nessa categoria sejam deduzidos. Para obter mais informações, consulte **Tabela 2-2**.

Tabela 2-2 Dedução da pontuação de segurança

Categoria		Item de dedução de pontuação	Edição do HSS afetada	Pontos deduzidos	Multiplicar a pontuação deduzida pela quantidade de risco	Como melhorar a pontuação
Vulnerabilidades	Vulnerabilidades não tratadas	Vulnerabilidades críticas não tratadas	Todas	10	√	Corrija vulnerabilidades com base nas sugestões fornecidas, procure vulnerabilidades novamente e atualize a pontuação. ● Para obter detalhes sobre como corrigir vulnerabilidades, consulte **Manipulação de vulnerabilidades**. ● Para obter detalhes sobre como fazer a verificação de vulnerabilidades, consulte **Verificação de vulnerabilidade**.
		Vulnerabilidades de alto risco não tratadas	Todas	3	√	
		Vulnerabilidades de risco médio não tratadas	Todas	1	√	
		Vulnerabilidades de baixo risco não tratadas	Todas	0,1	√	

Categoria		Item de dedução de pontuação	Edição do HSS afetada	Pontos deduzidos	Multiplicar a pontuação deduzida pela quantidade de risco	Como melhorar a pontuação
	Nenhuma verificação de vulnerabilidades	Nenhuma verificação de vulnerabilidade foi realizada no último mês.	Todas	15	×	• A edição básica do HSS não fornece verificação de vulnerabilidades. Para usar esse recurso, atualize o HSS para a edição empresarial ou premium. Para mais detalhes, consulte **Atualização de sua edição**. • Nas edições profissional, empresarial, premium e WTP do HSS, é recomendável realizar verificações de vulnerabilidade. Para mais detalhes, consulte **Verificação de vulnerabilidade**.

Categoria		Item de dedução de pontuação	Edição do HSS afetada	Pontos deduzidos	Multiplicar a pontuação deduzida pela quantidade de risco	Como melhorar a pontuação
Problemas de linha de base	Itens de não conformidade não tratados	Itens de não conformidade de alto risco não tratados	Todas	10	√	Corrija itens de não conformidade, execute uma verificação de linha de base novamente e atualize a pontuação. ● Para obter detalhes sobre como corrigir riscos de linha de base, consulte **Correção de configurações inseguras**. ● Para obter detalhes sobre como executar uma verificação de linha de base, consulte **Visualização de detalhes da verificação da linha de base**.
		Itens de não conformidade de risco médio não tratados	Todas	3	√	
		Itens de não conformidade de baixo risco não tratados	Todas	1	√	
	Senhas fracas	Senhas fracas	Todas	10	√	Use senhas fortes. Para obter detalhes, consulte **Como definir uma senha segura?**
	Verificação de senha fraca não ativada	Política de verificação de senha fraca não ativada	Todas	10	×	Ative a política **Weak Password Detection** para verificar se há senhas fracas nos servidores. Para mais detalhes, consulte **Visualização de um grupo de políticas**.

Categoria		Item de dedução de pontuação	Edição do HSS afetada	Pontos deduzidos	Multiplicar a pontuação deduzida pela quantidade de risco	Como melhorar a pontuação
	Verificação de linha de base não realizada	Nenhuma verificação de linha de base foi realizada no último mês.	Todas	10	×	• As edições básicas e profissionais do HSS não fornecem verificação de linha de base. Para usar esse recurso, é recomendável atualizar o HSS para a edição empresarial ou premium. Para mais detalhes, consulte **Atualização de sua edição**. • Nas edições profissional, empresarial, premium e WTP do HSS, é aconselhável realizar verificações de linha de base. Para mais detalhes, consulte **Visualização de um grupo de políticas**.
Invasões	Alarmes não tratados	Alarmes críticos não tratados	Todas	10	√	Manipule os alarmes com base nas sugestões fornecidas. Depois que os alarmes são manipulados, o HSS atualizará automaticamente a pontuação. Para mais detalhes, veja **Manipulação de alarmes do servidor** e **Manipulação de alarmes de container**.
		Alarmes de alto risco não tratados	Todas	3	√	
		Alarmes de risco médio não tratados	Todas	1	√	
		Alarmes de baixo risco não tratados	Todas	0,1	√	

Categoria		Item de dedução de pontuação	Edição do HSS afetada	Pontos deduzidos	Multiplicar a pontuação deduzida pela quantidade de risco	Como melhorar a pontuação
	Proteção não ativada	Nenhuma política de segurança ativada	Todas	30	×	Nas edições profissional, empresarial, premium, WTP e de container do HSS, você precisa ativar as políticas de proteção. Para mais detalhes, consulte **Visualização de um grupo de políticas**. As políticas de detecção de intrusão que precisam ser ativadas para cada edição são as seguintes: ● Edição profissional/ empresarial: – Linux: detecção de web shell, proteção de arquivos, detecção HIPS, verificação de segurança de logon, detecção de arquivos maliciosos, comportamentos anormais de processos, escalonamento de privilégios de raiz, processo em tempo real e detecção de rootkit – Windows: detecção AV, detecção de web shell, detecção HIPS, verificação de segurança de logon e

Categoria		Item de dedução de pontuação	Edição do HSS afetada	Pontos deduzidos	Multiplicar a pontuação deduzida pela quantidade de risco	Como melhorar a pontuação
						processo em tempo real ● Edição premium/WTP – Linux: detecção de intrusão de cluster, detecção de web shell, proteção de arquivos, detecção HIPS, verificação de segurança de logon, detecção de arquivos maliciosos, detecção de verificação de portas, comportamentos anormais de processos, escalonamento de privilégios de raiz, processo em tempo real e detecção de rootkit – Windows: detecção AV, detecção de web shell, detecção HIPS, verificação de segurança de logon e processo em tempo real ● Edição de container Detecção de intrusão de cluster, detecção de escape de container, detecção de web shell, monitoramento

Categoria		Item de dedução de pontuação	Edição do HSS afetada	Pontos deduzidos	Multiplicar a pontuação deduzida pela quantidade de risco	Como melhorar a pontuação
						de arquivos de container, lista branca de processos de container e comportamentos de imagem suspeitos
		Política de segurança de logon não ativada	Todas	10	×	Nas edições profissional, empresarial, premium, WTP e de container do HSS, é necessário ativar a política **Login Security Check** para servidores. Para mais detalhes, consulte **Visualização de um grupo de políticas**.
		Política de prevenção de ransomware não ativada	Edição premium	15	×	As edições premium, WTP e de container do HSS oferecem suporte à prevenção de ransomware. Nessas edições, você precisa ativar a política de prevenção de ransomware e a política de backup. (Serão deduzidos 10 pontos se o backup não estiver ativado). Para mais detalhes, consulte **Ativação da prevenção de ransomware**.
		A política WTP não está ativada	Edição WTP	20	×	Na edição WTP do HSS, você precisa ativar a política WTP para servidores. Para mais detalhes, consulte **Habilitação da edição WTP**.

Categoria		Item de dedução de pontuação	Edição do HSS afetada	Pontos deduzidos	Multiplicar a pontuação deduzida pela quantidade de risco	Como melhorar a pontuação
		Política de detecção de tempo de execução de container não ativada	Edição de container	20	×	Na edição de container do HSS, você precisa ativar a política **Container Escape** para servidores. Para mais detalhes, consulte **Visualização de um grupo de políticas**.
Riscos de ativos	Portas abertas	Portas de alto risco TCP/UDP abertas	Todas	1	√	É aconselhável desativar portas desnecessárias. Para ativar uma porta, escolha **Asset Management** > **Server Fingerprints**, clique em **Open Ports** e ignore a porta.
	Descoberta de ativos não ativada	Política de descoberta de ativos não ativada	Todas	5	×	● As edições básica, profissional e empresarial do HSS não fornecem detecção de ativos. Para usar esse recurso, atualize o HSS para a edição premium. Para mais detalhes, consulte **Atualização de sua edição**. ● Nas edições premium e WTP do HSS, é aconselhável ativar a política **Asset Discovery**. Para mais detalhes, consulte **Visualização de um grupo de políticas**.

Categoria		Item de dedução de pontuação	Edição do HSS afetada	Pontos deduzidos	Multiplicar a pontuação deduzida pela quantidade de risco	Como melhorar a pontuação
Riscos da imagem	Imagens inseguras	Imagens de alto risco	Edição de container	3	√	Recrie uma imagem, verifique a imagem e atualize a pontuação.
		Imagens de médio risco	Edição de container	1	√	
		Imagens de médio risco	Edição de container	0,1	√	
	Verificação de segurança de imagem não executada	Nenhuma verificação de segurança de imagem foi realizada no último mês.	Edição de container	5	×	Na edição de container do HSS, é aconselhável executar verificações de segurança de imagem. Para mais detalhes, consulte **Imagens do container**.

Categoria		Item de dedução de pontuação	Edição do HSS afetada	Pontos deduzidos	Multiplicar a pontuação deduzida pela quantidade de risco	Como melhorar a pontuação
Proteção do servidor não ativada	Proteção do servidor não ativada	Servidores desprotegidos	Todas	0.1–1	√	Os pontos deduzidos para um servidor desprotegido variam dependendo de sua importância do ativo: ● Ativo importante: 1 ● Ativo geral: 0,5 ● Ativo de teste: 0,1 É aconselhável ativar a proteção para o seu servidor o mais rápido possível. Para mais detalhes, consulte **Habilitação de HSS**.

3 Gerenciamento de ativos

3.1 Gerenciamento de ativos

Você pode contar todos os seus ativos e verificar suas estatísticas, incluindo o status do agente, o status da proteção, a cota, a conta, a porta, o processo, o software e os itens iniciados automaticamente.

Restrições

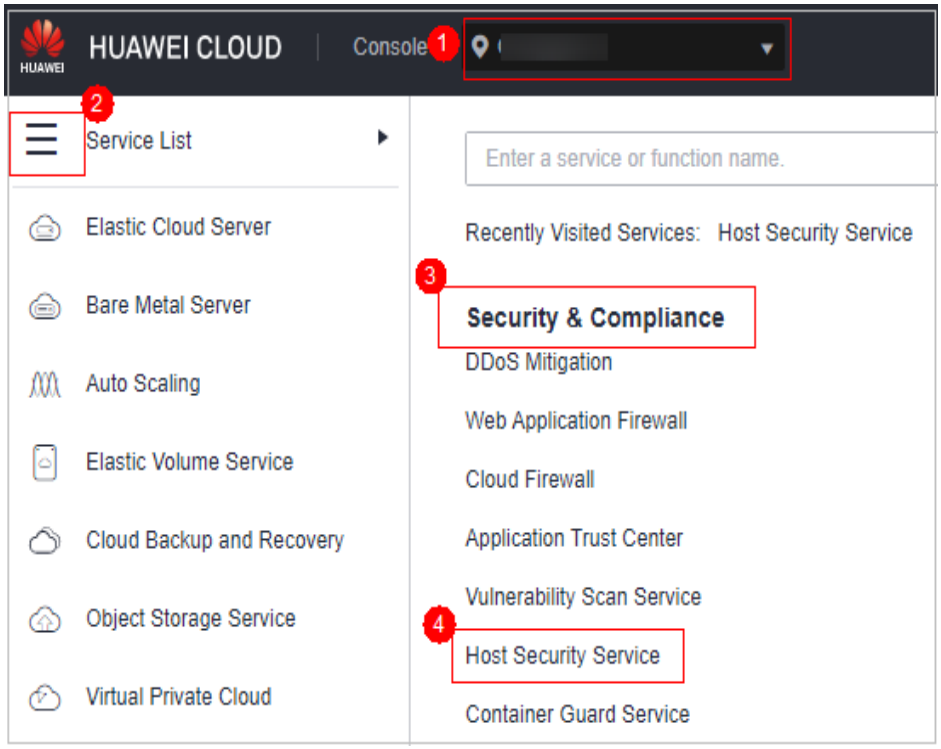
Os servidores que não são protegidos pelo HSS não suportam a função de visão geral de ativos.

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 3-1 Acessar o HSS



Passo 3 Escolha **Asset Management** > **Assets**. Verifique seus ativos e suas estatísticas.

NOTA

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

----Fim

3.2 Impressões digitais do servidor

3.2.1 Visualização de impressões digitais de ativos do servidor

O HSS pode coletar impressões digitais de ativos do servidor, incluindo informações sobre portas, processos, aplicações Web, serviços da Web, estruturas da Web e itens iniciados automaticamente. Você pode verificar centralmente as informações de ativos do servidor e detectar ativos arriscados em tempo hábil com base nas impressões digitais do servidor. O HSS não toca nos seus ativos. Você precisa eliminar manualmente os riscos.

Restrições

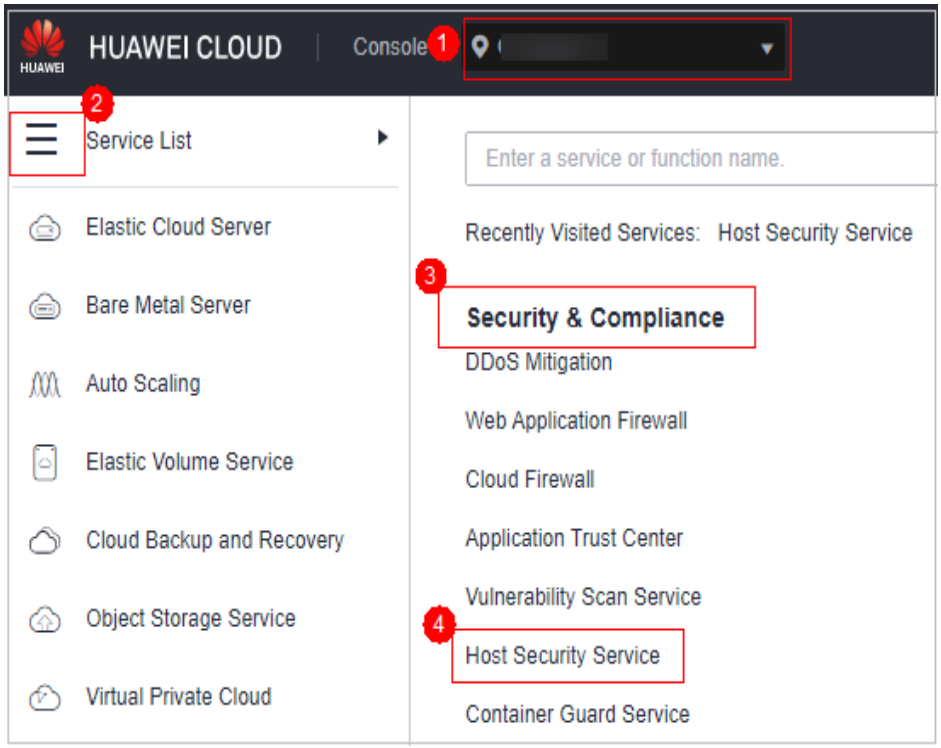
Seus servidores são protegidos pela edição empresarial, premium, WTP ou de container do HSS.

Visualização de informações de ativos de todos os servidores

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

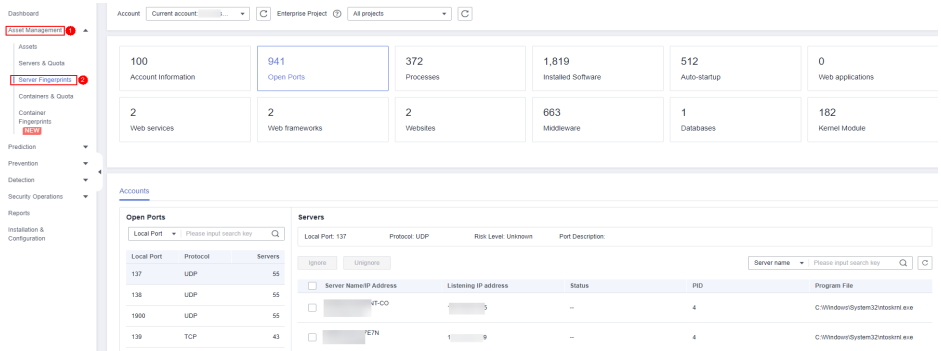


Passo 3 Escolha **Asset Management** > **Server Fingerprints** para visualizar todos os ativos do servidor.

NOTA

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

Figura 3-3 Visualização de informações de ativos do servidor



----Fim

Tabela 3-1 Impressões digitais de ativos

Item	Descrição	SO suportado	Frequência de verificação
Accounts	Verificar e gerenciar todas as contas em seus servidores para mantê-las seguras. Você pode verificar em tempo real e informações históricas da conta para encontrar contas suspeitas. ● As informações da conta em tempo real incluem o nome da conta, o número de servidores, o nome do servidor/endereço IP, a permissão de logon, a permissão de raiz, o grupo de usuários, o diretório de usuários, o shell iniciado pelo usuário e a hora da última verificação. ● Os registros históricos de alteração da conta incluem o nome do servidor/endereço IP, status de alteração, permissão de logon, permissão de raiz, grupo de usuários, diretório de usuários, shell iniciado pelo usuário e a hora da última verificação.	Linux e Windows	Verificação em tempo real
Open ports	Verificar as portas abertas em seus servidores, incluindo portas arriscadas e desconhecidas. Você pode encontrar facilmente portas de alto risco verificando portas locais, tipos de protocolos, nomes de servidores, endereços IP, status, PIDs e arquivos de programa. ● Desativação manual de portas de alto risco Se o HSS detectar portas abertas de alto risco ou portas não utilizadas, verifique se elas são realmente usadas por seus serviços. Para portas de alto risco, verifique os arquivos de programa. Se houver riscos, exclua ou isole os arquivos de origem. É recomendável que você lide com as portas no nível de risco **Dangerous** imediatamente e lide com as portas no nível **Unknown** com base nas condições reais de serviço. ● Ignorar os riscos: se uma porta de alto risco detectada for realmente uma porta normal usada para serviços, você poderá ignorá-la. A porta não será mais considerada arriscada nem gerará alarmes.	Linux e Windows	Verificação em tempo real

Item	Descrição	SO suportado	Frequência de verificação
Processes	Verificar os processos em seus servidores e encontrar processos anormais. Você pode facilmente identificar processos anormais com base em caminhos de processos, nomes de servidores, endereços IP, parâmetros de inicialização, tempo de inicialização, usuários que executam os processos, permissões de arquivo, PIDs e hashes de arquivo. Se um processo suspeito não for detectado nos últimos 30 dias, suas informações serão automaticamente excluídas da lista de processos.	Linux e Windows	Verificação em tempo real
Installed software	Verificar e gerenciar todos os softwares instalados em seus servidores e identificar versões inseguras. Você pode verificar informações históricas e em tempo real sobre o software para determinar se ele é arriscado. ● As informações de software em tempo real incluem o nome do software, o número de servidores, os nomes dos servidores, os endereços IP, as versões do software, a hora da atualização do software e a hora da última verificação. ● Os registros históricos de alterações de software incluem os nomes dos servidores, endereços IP, status de alteração, versões de software, hora de atualização de software e hora da última verificação.	Linux e Windows	Verificação automática todos os dias
Auto-startup	Verificar se há itens de inicialização automática e localizar rapidamente cavalos de Troia. ● Informações em tempo real sobre itens iniciados automaticamente incluem seus nomes, tipos (serviço iniciado automaticamente, pasta de inicialização, biblioteca dinâmica pré-carregada, chave do registro Run ou tarefa agendada), número de servidores, nomes de servidores, endereços IP, caminhos, hashes de arquivos, usuários e a hora da última verificação. ● Os registros históricos de alteração de itens iniciados automaticamente incluem nomes de servidores, endereços IP, status de alteração, caminhos, hashes de arquivos, usuários e a hora da última verificação.	Linux e Windows	Verificação em tempo real

Item	Descrição	SO suportado	Frequência de verificação
Websites	Você pode verificar estatísticas sobre diretórios da Web e sites que podem ser acessados pela Internet. Você pode visualizar os diretórios e permissões, caminhos de acesso, portas externas, informações de certificados (a serem fornecidas posteriormente) e processos-chave de sites.	Linux	Uma vez por semana (06:00 a.m. todas as segundas-feiras)
Web frameworks	Você pode verificar estatísticas sobre estruturas usadas para apresentação de conteúdo da Web, incluindo suas versões, caminhos e processos vinculados.	Linux	Uma vez por semana (06:00 a.m. todas as segundas-feiras)
Middleware	Você pode verificar informações sobre servidores, versões, caminhos e processos vinculados ao middleware.	Linux e Windows	Uma vez por semana (06:00 a.m. todas as segundas-feiras)
Kernel module	Verificar informações sobre todos os arquivos de módulo do programa em execução nos kernels, incluindo servidores vinculados, números de versões, descrições de módulos, caminhos de arquivos de driver, permissões de arquivos e hashes de arquivos.	Linux	Uma vez por semana (06:00 a.m. todas as segundas-feiras)
Web services	Você pode verificar detalhes sobre o software usado para acesso ao conteúdo da Web, incluindo versões, caminhos, arquivos de configuração e processos vinculados de todos os softwares.	Linux	Uma vez por semana (06:00 a.m. todas as segundas-feiras)

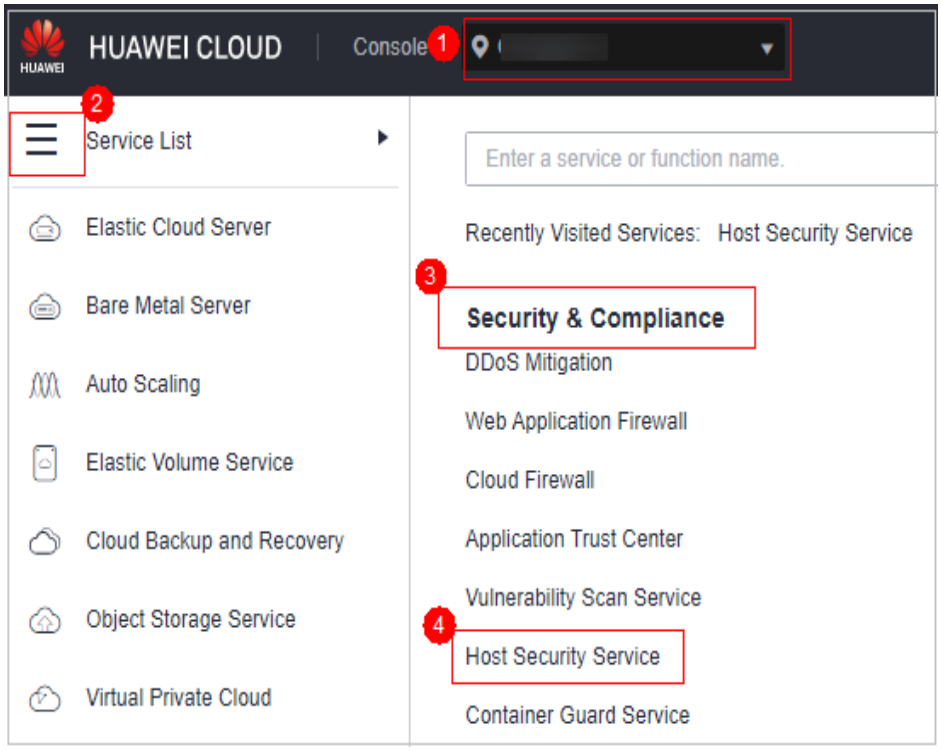
Item	Descrição	SO suportado	Frequência de verificação
Web applications	Você pode verificar detalhes sobre o software usado para push e lançamento de conteúdo da Web, incluindo versões, caminhos, arquivos de configuração e processos vinculados de todos os softwares.	Linux e Windows (somente o Tomcat é suportado)	Uma vez por semana (06:00 a.m. todas as segundas-feiras)
Databases	Você pode verificar detalhes sobre o software que fornece armazenamento de dados, incluindo versões, caminhos, arquivos de configuração e processos vinculados de todos os softwares.	Linux e Windows (apenas MySQL é suportado)	Uma vez por semana (06:00 a.m. todas as segundas-feiras)

Visualização de informações sobre ativos de um único 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 3-4 Acessar o HSS



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

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 Clique no nome do servidor de destino. Na página de detalhes do servidor exibida, clique na guia **Asset Fingerprints** > **Servers**

Passo 5 Clique em uma impressão digital na lista de impressões digitais para visualizar suas informações de ativos. Para obter mais informações, consulte **Tabela 3-1**.

----Fim

3.2.2 Visualização do histórico de operações dos ativos do servidor

O HSS registra proativamente as alterações nas informações da conta, informações de software e itens iniciados automaticamente. Você pode verificar os detalhes da alteração de acordo com diferentes dimensões e intervalos de tempo.

Restrições

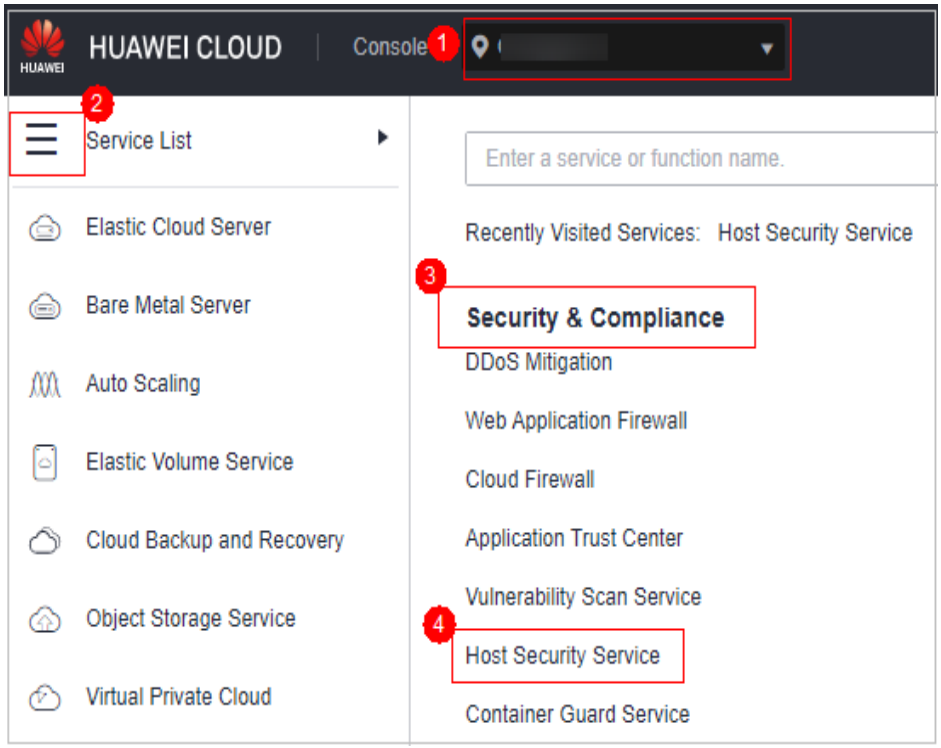
Seus servidores são protegidos pela edição empresarial, premium, WTP ou de container do HSS.

Verificar registros de alteração

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 Escolha **Asset Management** > **Server Fingerprints** e clique em **Operation History**. Na página **Operation History** exibida, selecione uma dimensão e um período de tempo para exibir o histórico de alterações de contas, softwares e itens iniciados automaticamente.

NOTA

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

----Fim

Gerenciar informações da conta

As alterações de conta são registradas.

- **Action**: a coluna **Action** registra as operações. Seu valor pode ser **Create** (recém-encontrado na última verificação), **Delete** (encontrado em verificações anteriores, mas faltando na última) e **Modify** (são detectadas alterações nas informações da conta, como nomes de contas, direitos de administrador e grupos de usuários).
- **Last Scan Time**: a hora da última verificação indica a hora da última verificação executada para servidores em um período.

Você pode verificar as informações e alterações em todas as contas aqui. Se você encontrar contas desnecessárias ou superprivilegiadas (como **root**) que não sejam obrigatórias para os serviços, exclua-as ou modifique suas permissões para evitar explorações.

Gerenciar softwares

As operações feitas nas contas são registradas.

- **Action**: **Create** e **Delete**.
- **Last Scan Time**: a hora da última verificação registra a hora em que as alterações foram detectadas, não a hora em que foram feitas.

Você pode verificar as informações e alterações em todos os softwares, atualizar softwares e excluir softwares desnecessários, suspeitos ou em versão anterior.

Itens iniciados automaticamente

Os cavalos de Troia geralmente invadem os servidores criando serviços iniciados automaticamente, tarefas agendadas, bibliotecas dinâmicas pré-carregadas, chaves de registro Run ou pastas de inicialização. A função de verificação de inicialização automática coleta informações sobre todos os itens iniciados automaticamente, incluindo seus nomes, tipos e número de servidores afetados, facilitando a localização de itens suspeitos iniciados automaticamente.

Você pode verificar os servidores, os endereços IP, as alterações, os caminhos, os hashes de arquivos, os usuários e o tempo da última verificação dos itens de inicialização automática.

3.2.3 Atualização manual das informações de ativos do servidor em tempo real

Esta seção descreve como obter as informações mais recentes sobre aplicações Web, serviços Web, estruturas Web, sites, middleware, módulos do kernel e bancos de dados de seus servidores.

Restrições

- Seus servidores são protegidos pela edição empresarial, premium, WTP ou de container do HSS.
- Somente servidores do Linux são suportados.
- O status do agente do servidor deve ser **Online** e a versão do agente deve ser 3.2.5 ou posterior. Para obter detalhes sobre como verificar as versões de agentes, consulte **Visualização do gerenciamento de agente**.

Frequência de verificação

As contas e as portas abertas são verificadas em tempo real. O resultado da detecção de porta aberta é atualizado a cada seis horas.

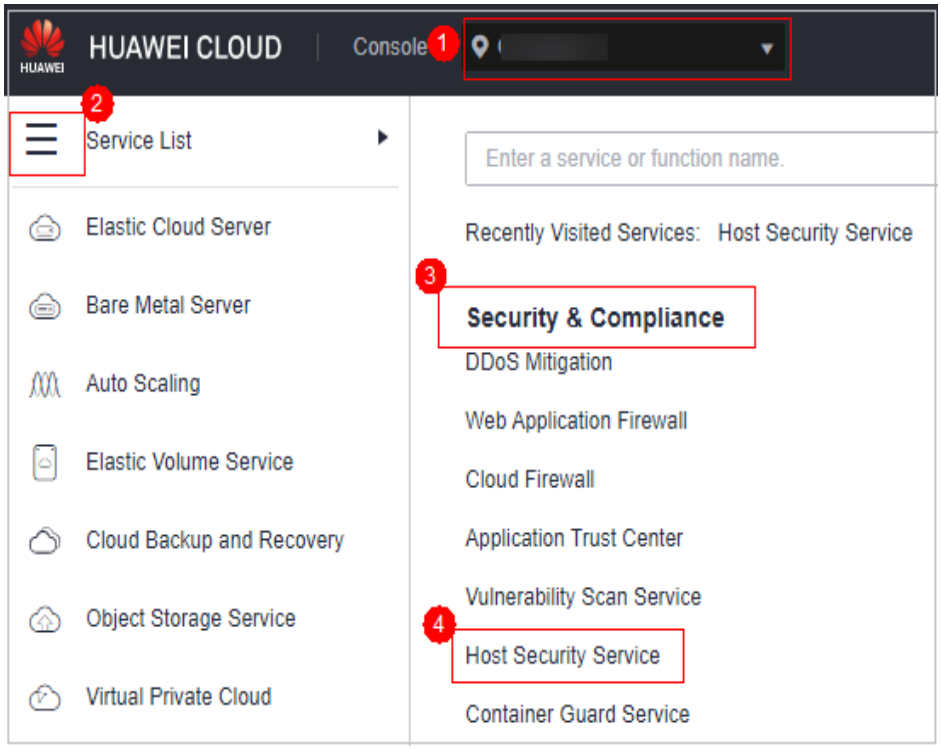
Processos, diretórios Web, software e itens de inicialização automática são verificados automaticamente **todos os dias no início da manhã**.

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 3-6 Acessar o HSS



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

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 Clique no nome do servidor de destino. Na página de detalhes do servidor exibida, clique na guia **Asset Fingerprints** > **Servers**

Passo 5 Clique em um tipo de impressão digital na lista de impressões digitais e clique em **Discover Assets** na área superior da lista à direita.

NOTA

Atualmente, apenas as informações sobre aplicações Web, serviços Web, estruturas Web, sites, middleware, módulos de kernel e bancos de dados podem ser coletadas manualmente e atualizadas em tempo real. Informações sobre outros tipos são coletadas automaticamente e atualizadas todos os dias.

Passo 6 Após a conclusão da execução automática, o horário da última verificação é atualizado e as informações mais recentes sobre o ativo do servidor são exibidas.

----Fim

3.3 Impressões digitais de containers

3.3.1 Visualização de impressões digitais de ativos de containers

O HSS pode coletar impressões digitais de ativos de containers, incluindo clusters de containers, serviços, cargas de trabalho, contas, portas e processos. Você pode verificar centralmente as informações de ativos do container e detectar ativos arriscados em tempo hábil com base nas impressões digitais do container. Esta seção descreve como visualizar as informações de ativos de container coletadas.

Restrições

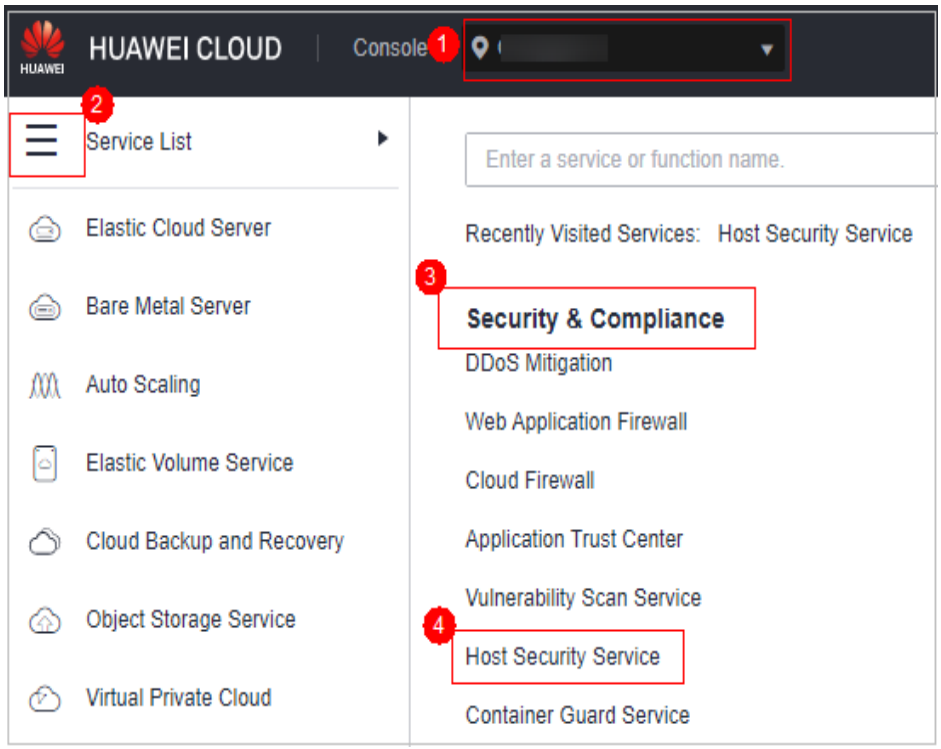
- Somente a edição de container do HSS suporta a função de impressão digital do container.
- Somente Linux é suportado.

Visualização de dados de impressões digitais de ativos de todos os containers

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 **Asset Management** > **Container Fingerprints** > **Asset Fingerprints**. Na página **Asset Fingerprints** que é exibida, visualize os dados de impressão digital de todos os containers.

NOTA

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

Figura 3-8 Visualização de ativos de container

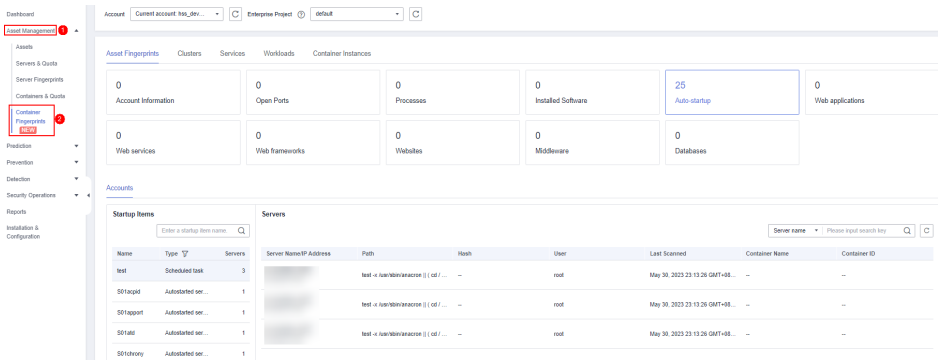


Tabela 3-2 Impressões digitais de ativos do container

Recurso	Descrição	Frequência de verificação
Contas	Verificar e gerenciar todas as contas em seus containers para mantê-las seguras. As informações da conta em tempo real incluem o nome da conta, o número de servidores, o nome do servidor, o endereço IP, a permissão de logon, a permissão raiz, o grupo de usuários, o diretório de usuários, o shell iniciado pelo usuário, o nome do container, o ID do container e a hora da última verificação.	Verificação em tempo real

Recurso	Descrição	Frequência de verificação
Portas abertas	Verificar as portas abertas em seus containers, incluindo portas arriscadas e desconhecidas. Você pode encontrar facilmente portas de alto risco em containers verificando portas locais, tipos de protocolos, nomes de servidores, endereços IP, status, PIDs e arquivos de programa. ● Desativação manual de portas de alto risco Se o HSS detectar portas abertas de alto risco ou portas não usadas, verifique se elas são realmente usadas por seus serviços. Para portas de alto risco, verifique os arquivos de programa. Se houver riscos, exclua ou isole os arquivos de origem. É recomendável que você lide com as portas no nível de risco **Dangerous** imediatamente e lide com as portas no nível **Unknown** com base nas condições reais de serviço. ● Ignorar os riscos: se uma porta de alto risco detectada for realmente uma porta normal usada para serviços, você poderá ignorá-la. A porta não será mais considerada arriscada nem gerará alarmes.	Verificação em tempo real
Processos	Verificar os processos em seus containers e encontrar processos anormais. Você pode identificar facilmente processos anormais em seus caminhos de processo baseados em containers, nomes de servidores, endereços IP, parâmetros de inicialização, tempo de inicialização, usuários que executam os processos, permissões de arquivo, PIDs e hashes de arquivo. Se um processo suspeito não for detectado nos últimos 30 dias, suas informações serão automaticamente excluídas da lista de processos.	Verificação em tempo real
Software instalado	Verificar e gerenciar todos os softwares instalados em seus containers e identificar versões inseguras. Você pode verificar informações históricas e em tempo real sobre o software para determinar se ele é arriscado. ● As informações de software em tempo real incluem o nome do software, o número de servidores, os nomes dos servidores, os endereços IP, as versões do software, a hora da atualização do software e a hora da última verificação. ● Os registros históricos de alterações de software incluem os nomes dos servidores, endereços IP, status de alteração, versões de software, hora de atualização de software e a hora da última verificação.	Verificação automática todos os dias

Recurso	Descrição	Frequência de verificação
Itens iniciados automaticamente	Verificar se há itens iniciados automaticamente e localizar rapidamente cavalos de Troia. Informações em tempo real sobre itens iniciados automaticamente incluem seus nomes, tipos (serviço iniciado automaticamente, pasta de inicialização, biblioteca dinâmica pré-carregada, chave do registro Run ou tarefa agendada), número de servidores, nomes de servidores, endereços IP, caminhos, hashes de arquivos, usuários, nome do container, ID do container e a hora da última verificação.	Verificação em tempo real
Verificação do site	Você pode verificar estatísticas sobre diretórios da Web e sites que podem ser acessados a partir da Internet. Você pode visualizar os diretórios e permissões, caminhos de acesso, portas externas, informações de certificados (a serem fornecidas posteriormente) e processos-chave de sites.	Uma vez por semana (06:00 a.m. todas as segundas-feiras)
Estrutura de Web	Você pode verificar estatísticas sobre estruturas usadas para apresentação de conteúdo da Web, incluindo suas versões, caminhos e processos vinculados.	Uma vez por semana (06:00 a.m. todas as segundas-feiras)
Middleware	Você também pode verificar informações sobre servidores, versões, caminhos e processos vinculados ao middleware.	Uma vez por semana (06:00 a.m. todas as segundas-feiras)
Serviços de Web	Você pode verificar detalhes sobre o software usado para acesso ao conteúdo da Web, incluindo versões, caminhos, arquivos de configuração e processos vinculados de todos os softwares.	Uma vez por semana (06:00 a.m. todas as segundas-feiras)
Aplicações Web	Você pode verificar detalhes sobre o software usado para push e lançamento de conteúdo da Web, incluindo versões, caminhos, arquivos de configuração e processos vinculados de todos os softwares.	Uma vez por semana (06:00 a.m. todas as segundas-feiras)
Banco de dados	Você pode verificar detalhes sobre o software que fornece armazenamento de dados, incluindo versões, caminhos, arquivos de configuração e processos vinculados de todos os softwares.	Uma vez por semana (06:00 a.m. todas as segundas-feiras)

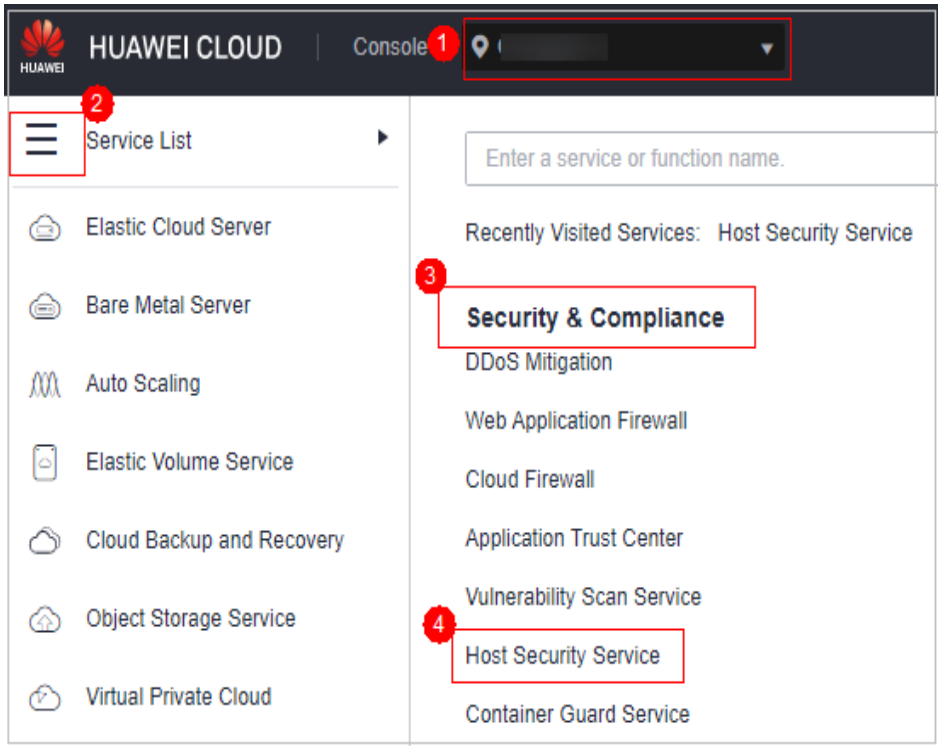
----Fim

Visualização de dados de impressão digital de ativos de um único container

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 No painel de navegação, escolha **Asset Management** > **Servers & Quota**. Clique na guia **Servers**.

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 Clique no nome do servidor de destino. Na página de detalhes do servidor exibida, clique na guia **Asset Fingerprints** > **Containers**.

Passo 5 Clique em uma impressão digital na lista de impressões digitais para visualizar suas informações de ativos. Para obter mais informações, consulte **Tabela 3-2**.

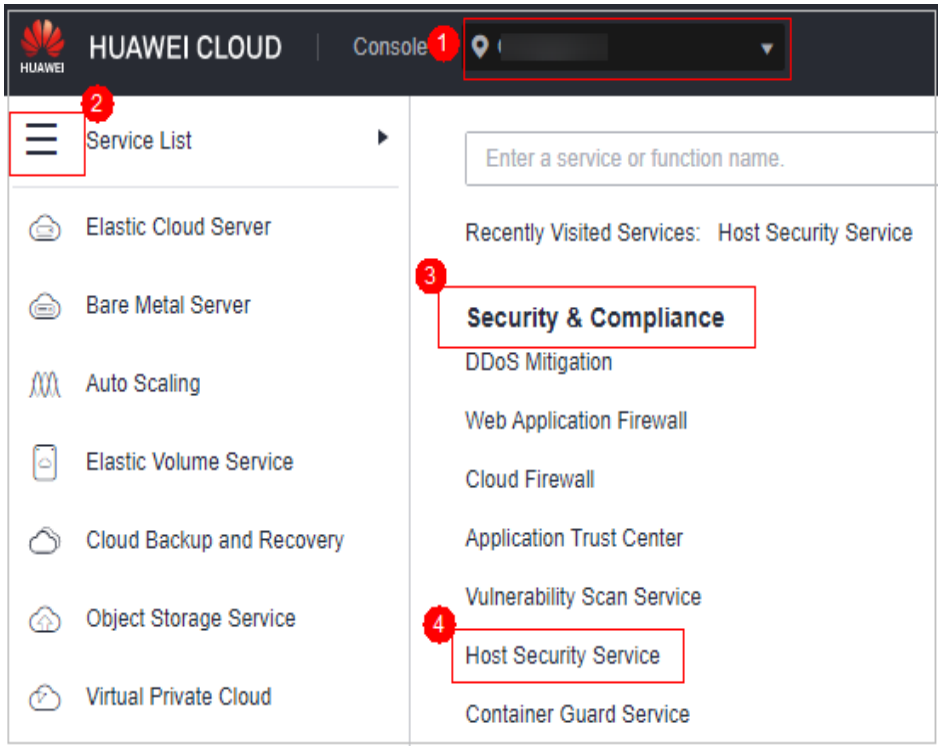
----Fim

Visualização de informações do cluster

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 3-10 Acessar o HSS



Passo 3 No painel de navegação, escolha **Asset Management** > **Container Fingerprints**.

Passo 4 Escolha **Clusters** e clique em **Synchronize** no canto superior esquerdo.

Passo 5 **Last Synchronized** indica que os dados de cluster, serviço, carga de trabalho e container do CCE foram sincronizados com sucesso.

Passo 6 Na página **Clusters**, visualize as informações do cluster.

A página **Clusters** exibe o nome, o tipo, o nó, a versão, a hora de criação e o status do cluster.

- Pesquisar o cluster de destino

  Você pode inserir informações como o nome e o status do cluster na caixa de pesquisa e clicar em para procurar o cluster de destino.
- Visualizar detalhes sobre o cluster de destino
  a. Clique no nome do cluster de destino para ir para o console do CCE.
  b. No console do CCE, clique no nome do cluster de destino. Na página de detalhes do cluster exibida, visualize as informações básicas, a configuração de rede e as informações de conexão.

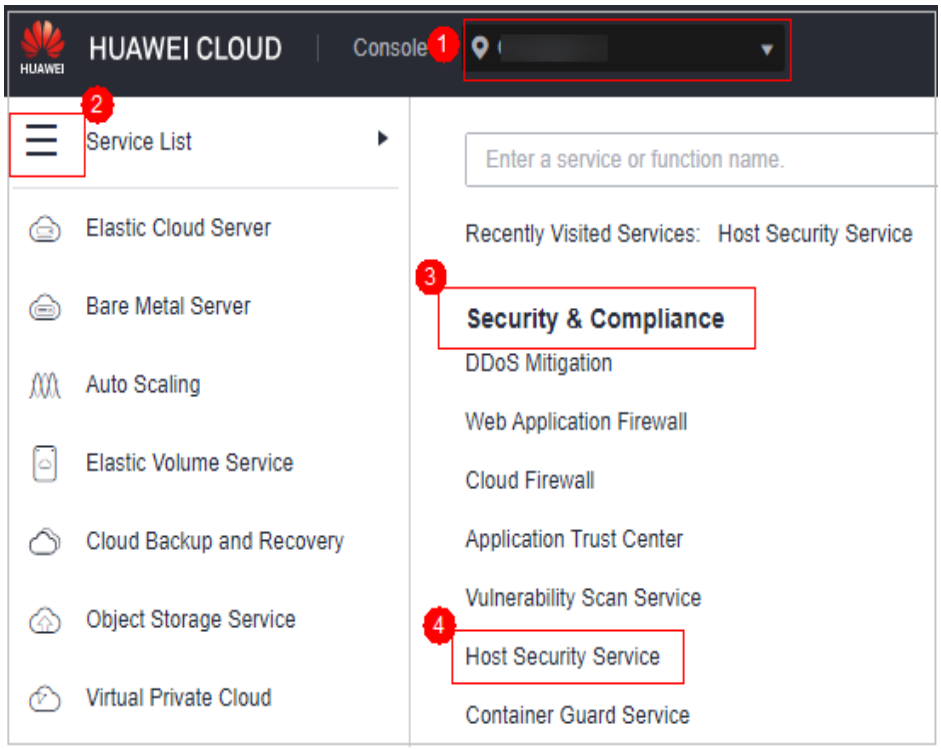
----Fim

Visualização de serviços

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 3-11 Acessar o HSS



Passo 3 No painel de navegação, escolha **Asset Management** > **Container Fingerprints**.

Passo 4 Escolha **Clusters** e clique em **Synchronize** no canto superior esquerdo.

Passo 5 **Last Synchronized** indica que os dados de cluster, serviço, carga de trabalho e container do CCE foram sincronizados com sucesso.

Passo 6 Na página de guia **Services**, visualize as informações.

A página exibe o nome do serviço, o nome do ponto de extremidade, o modo de acesso, o endereço IP do serviço, o namespace, o cluster e a hora de criação.

- Pesquisar um serviço

  Você pode inserir informações como o nome do serviço e o modo de acesso na caixa de pesquisa e clicar em para pesquisar o serviço.
- Visualizar detalhes sobre um serviço

  Clique no nome de um serviço. Na página de detalhes do serviço que é exibida, você pode visualizar o seletor, a tag e a porta do serviço.

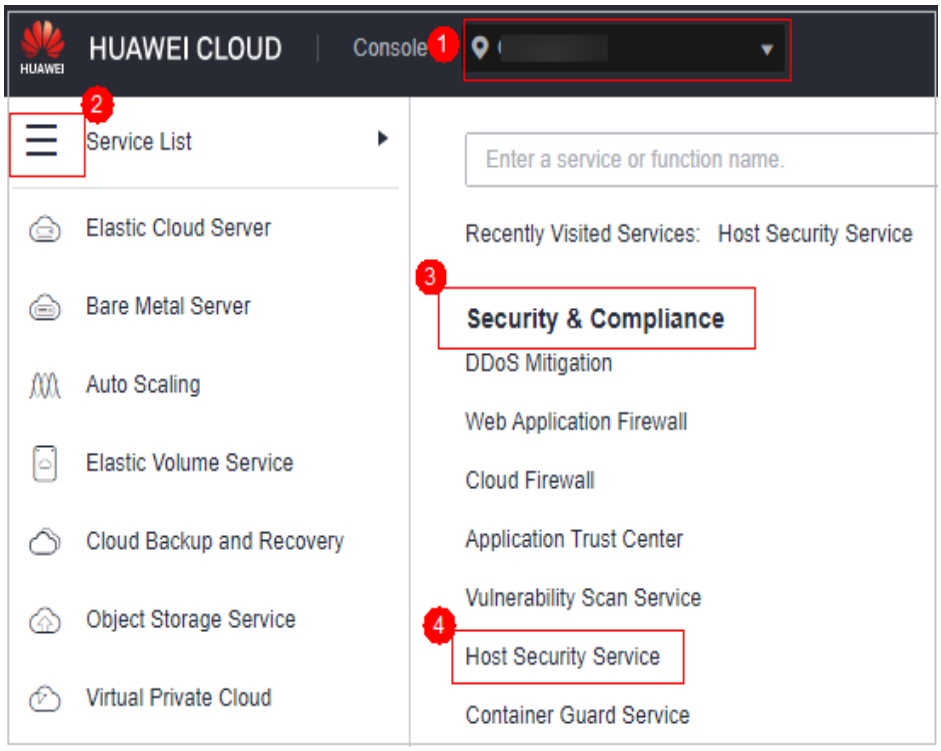
----Fim

Visualização de pontos de extremidade

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 3-12 Acessar o HSS



Passo 3 No painel de navegação, escolha **Asset Management** > **Container Fingerprints**.

Passo 4 Escolha **Clusters** e clique em **Synchronize** no canto superior esquerdo.

Passo 5 **Last Synchronized** indica que os dados de cluster, serviço, carga de trabalho e container do CCE foram sincronizados com sucesso.

Passo 6 Escolha **Services** > **Endpoints**. Visualize informações de pontos de extremidade.

A página exibe o nome, o namespace, o cluster e a hora da criação do ponto de extremidade, bem como se o ponto de extremidade está vinculado a um serviço e o nome do serviço vinculado.

- Pesquisar um ponto de extremidade

  Você pode inserir informações como o nome do ponto de extremidade e o namespace na caixa de pesquisa e clicar em para pesquisar o ponto de extremidade.
- Visualizar detalhes sobre um ponto de extremidade

  Clique no nome de um ponto de extremidade. Na página de detalhes do ponto de extremidade que é exibida, você pode visualizar o mapeamento do pod e as informações da porta.

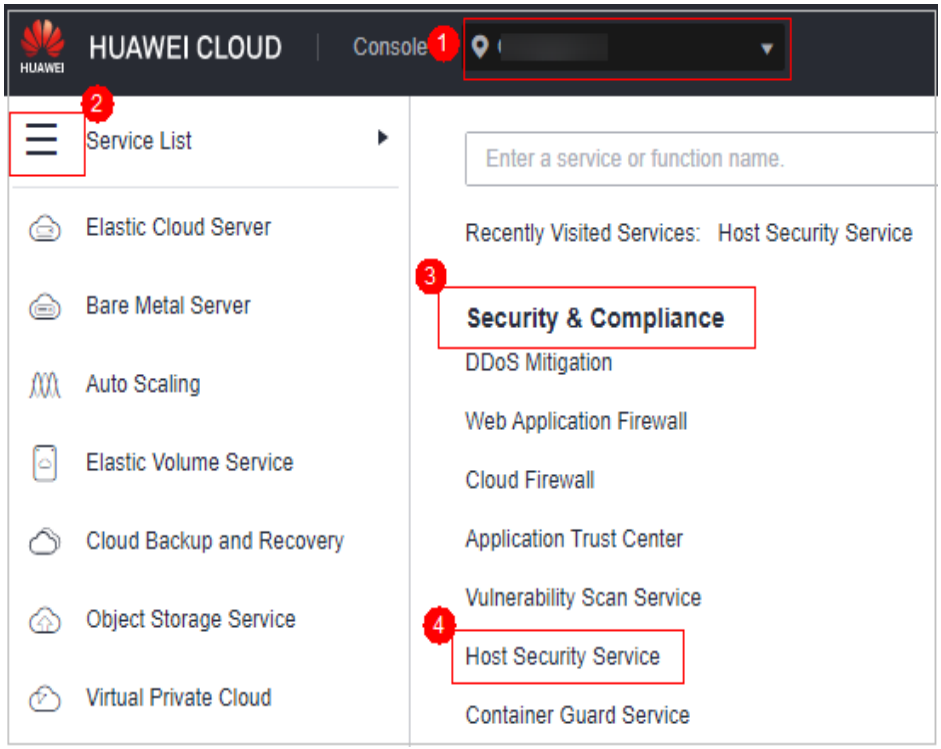
----Fim

Visualização de uma carga de trabalho

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 3-13 Acessar o HSS



Passo 3 No painel de navegação, escolha **Asset Management** > **Container Fingerprints**.

Passo 4 Escolha **Clusters** e clique em **Synchronize** no canto superior esquerdo.

Passo 5 **Last Synchronized** indica que os dados de cluster, serviço, carga de trabalho e container do CCE foram sincronizados com sucesso.

Passo 6 Clique na guia **Workloads**.

Passo 7 Selecione diferentes cargas de trabalho e visualize informações.

Você pode visualizar informações sobre **Deployment**, **StatefulSets**, **DaemonSets**, **Jobs**, **Cron Jobs** e **Pods**. Para obter detalhes sobre os itens de informações, consulte **Itens de informações sobre a carga de trabalho**.

Você pode inserir informações como o nome da carga de trabalho e o cluster na caixa de pesquisa e clicar em para pesquisar a carga de trabalho de destino.

Tabela 3-3 Informações sobre a carga de trabalho

Tipo de carga de trabalho	Item
Deployment	● Workload name ● Status ● Instances ● Namespaces ● Created ● Image name ● Cluster
StatefulSets	● Workload name ● Status ● Instances ● Namespace ● Created ● Image name ● Cluster
DaemonSets	● Workload name ● Status ● Instances ● Namespace ● Created ● Image name ● Cluster
Jobs	● Workload name ● Status ● Instances ● Namespace ● Created ● Image name ● Cluster

Tipo de carga de trabalho	Item
Cron Jobs	● Workload name ● Status ● Trigger ● Running jobs ● Namespace ● Latest scheduled ● Created ● Image name ● Cluster
Pods	● Name ● Namespace ● Cluster ● Node ● Pod IP address ● POD IP ● Status ● Created

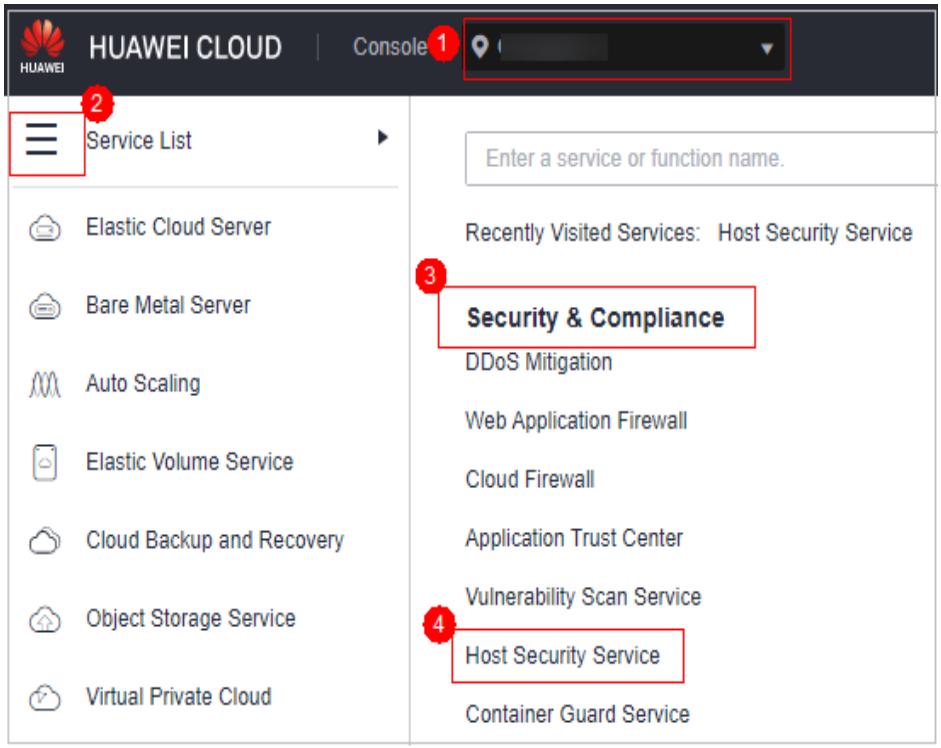
----Fim

Visualização de instâncias de container

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 3-14 Acessar o HSS



Passo 3 No painel de navegação, escolha **Asset Management** > **Container Fingerprints**.

Passo 4 Escolha **Clusters** e clique em **Synchronize** no canto superior esquerdo.

Passo 5 **Last Synchronized** indica que os dados de cluster, serviço, carga de trabalho e container do CCE foram sincronizados com sucesso.

Passo 6 Clique na guia **Container Instances**.

O nome do container, status, pod, cluster, hora de criação e nome da imagem são exibidos.

- Pesquisar um container

  Você pode inserir informações como o nome e o status do container na caixa de pesquisa e clicar em para pesquisar o container.
- Visualizar detalhes sobre um container

  Clique no nome de um container. Na página de detalhes do container exibida, você pode visualizar o processo, a porta e o caminho de montagem.

----Fim

3.3.2 Atualização manual de informações de ativos de containers em tempo real

Esta seção descreve como obter as impressões digitais de ativos, clusters, serviços, cargas de trabalho e containers mais recentes.

Restrições

- Somente a edição de container do HSS suporta a função de impressão digital do container.

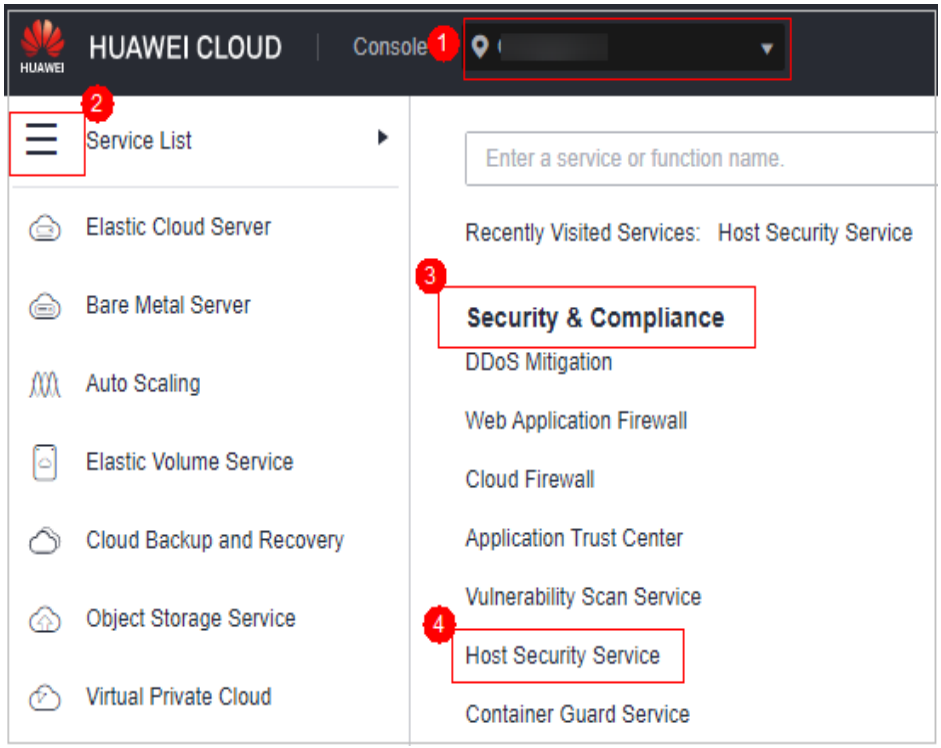
- Somente Linux é suportado.
- O status do agente do servidor deve ser **Online** e a versão do agente deve ser 3.2.5 ou posterior. Para obter detalhes sobre como verificar as versões do agente, consulte **Visualização do gerenciamento de agente**.

Atualizar dados de impressão digital do container em tempo real

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 3-15 Acessar o HSS



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

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 Clique no nome do servidor de destino. Na página de detalhes do servidor exibida, clique na guia **Asset Fingerprints** > **Containers**.

Passo 5 Clique em um tipo de impressão digital na lista de impressões digitais e clique em **Discover Assets** na área superior da lista à direita.

NOTA

Atualmente, apenas **Web applications**, **Web services**, **Web frameworks**, **Websites**, **Middleware** e **Databases** suportam coleta e atualização manual em tempo real. Informações sobre outros tipos são coletadas automaticamente e atualizadas todos os dias.

Passo 6 Após a conclusão da execução automática, o horário da última verificação é atualizado e as informações mais recentes sobre o ativo do container são exibidas.

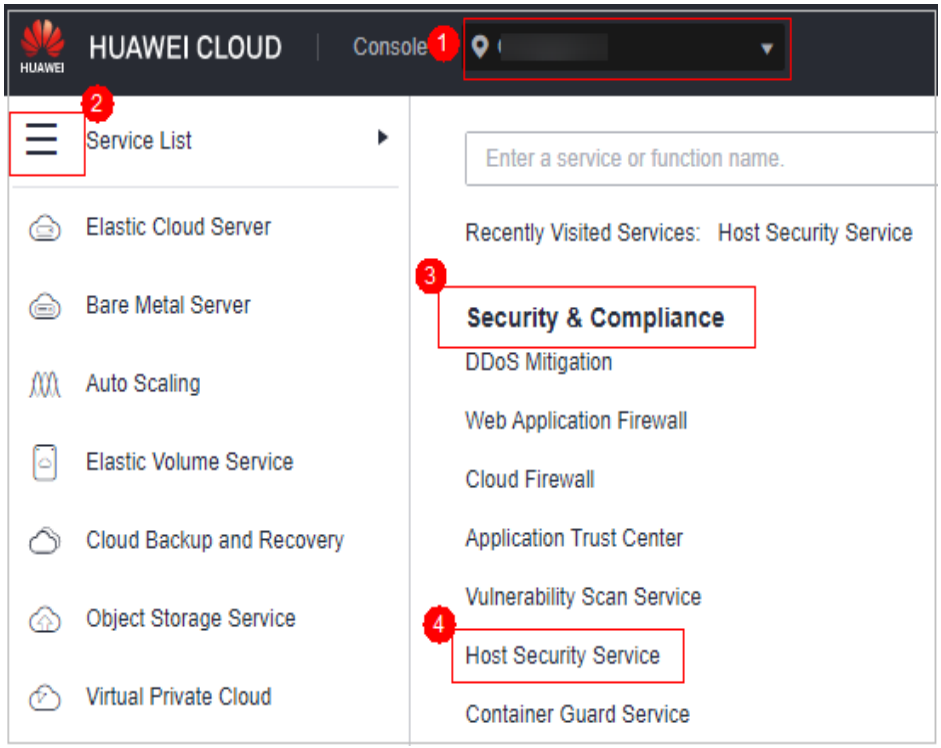
----Fim

Atualizar informações sobre clusters, serviços, cargas de trabalho e containers em tempo real

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 3-16 Acessar o HSS



Passo 3 No painel de navegação, escolha **Asset Management** > **Container Fingerprints**.

Passo 4 Escolha **Clusters** e clique em **Synchronize** no canto superior esquerdo.

Passo 5 **Last Synchronized** indica que os dados de cluster, serviço, carga de trabalho e container do CCE foram sincronizados com sucesso.

----Fim

3.4 Gerenciamento de servidores

3.4.1 Visualização do status da proteção do servidor

A lista de servidores na página **Servers & Quota** exibe o status de proteção apenas dos seguintes servidores:

- Servidores da Huawei Cloud comprados na região selecionada
- Servidores não da Huawei Cloud que foram adicionados à região selecionada

NOTA

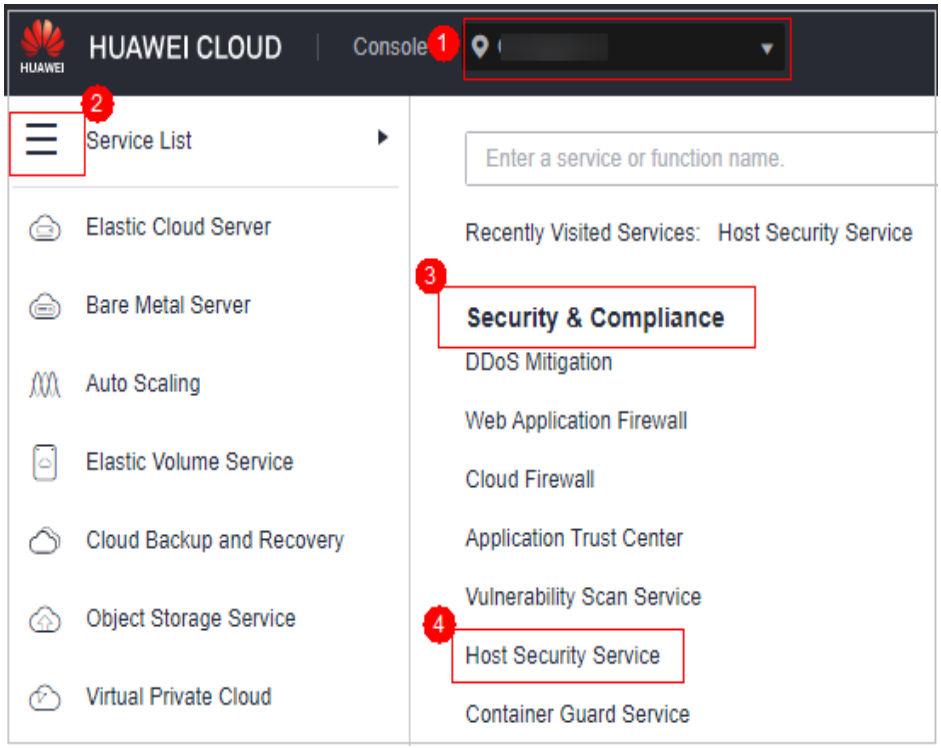
- Alterne para a região correta antes de procurar seus servidores.
- Se você ativou a função de projeto empresarial, pode selecionar seu projeto empresarial na lista suspensa do projeto **Enterprise** para verificar a visão geral do risco do servidor do projeto.

Visualização da lista de servidores

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 3-17 Acessar o HSS



Passo 3 No painel de navegação, escolha **Asset Management** > **Servers & Quota**. Na guia **Servers**, visualize o status de proteção do servidor. Para obter mais informações, consulte **Tabela 3-4**.

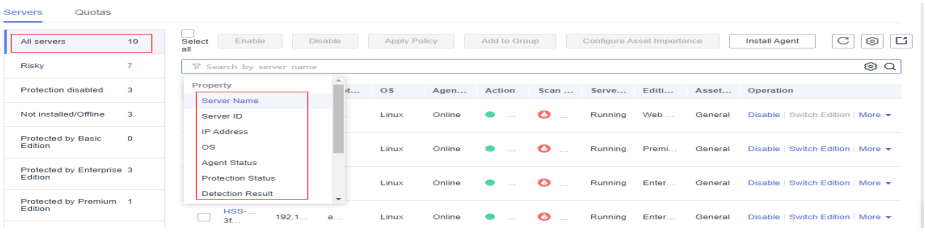
NOTA

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

Você pode verificar o nome do servidor, ID, endereço IP, SO, status de execução e projeto empresarial. Para definir os itens a serem exibidos na lista de proteção do servidor, clique em ⚙ no canto superior direito.

- Para verificar o status de proteção de um servidor, digite um nome de servidor, ID de servidor ou endereço IP na caixa de pesquisa acima da lista de proteção do servidor e clique em .

  Figura 3-18 Pesquisar um servidor protegido



- À esquerda da lista de proteção de servidor, selecione uma edição de proteção de servidor ou uma categoria de importância de ativo para visualizar o status de proteção de cada tipo de servidor.

Tabela 3-4 Status

Parâmetro	Descrição
Agent Status	● **Not installed**: o agente não foi instalado ou iniciado com sucesso. Clique em **Install Agent** e instale o agente conforme solicitado. Para obter detalhes, consulte **Instalação de um agente**. ● **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.
Action	● **Enabled**: o servidor está totalmente protegido por HSS. ● **Unprotected**: o HSS está desativado para o servidor. Clique em **Enable** na coluna **Operation** para ativar o HSS para o servidor. ● **Protection interrupted**: o servidor foi encerrado, a comunicação do agente está anormal ou o agente foi desinstalado.
Scan Results	● **Risky**: o host tem riscos. ● **Safe**: nenhum risco é encontrado. ● **Pending risk detection**: o HSS não está ativado para o servidor.

----Fim

Visualização do status da WTP

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 Escolha **Prevention** > **Web Tamper Protection** e clique em **Servers** para visualizar o status de proteção dos servidores.

NOTA

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

Para verificar o status de proteção de um servidor de destino, digite um nome de servidor, ID de servidor ou endereço IP na caixa de pesquisa acima da lista de proteção e clique em .

Figura 3-19 Servidores protegidos por WTP

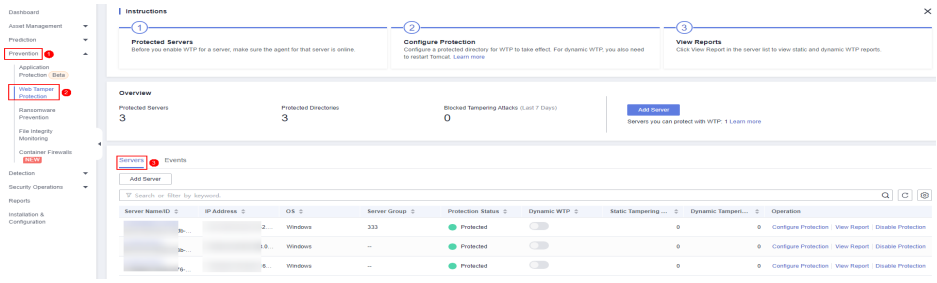


Tabela 3-5 Status

Parâmetro	Descrição
Protection Status	**Protected**: o HSS fornece proteção contra adulteração da Web (WTP) estática para o servidor.
Dynamic WTP	Status da WTP dinâmica, que pode ser: ● : ativar a WTP dinâmica ● : desativar a WTP dinâmica (Depois de ativar a WTP dinâmica, reinicie o Tomcat para que essa configuração tenha efeito.)
Static Tampering Attacks	Número de vezes que os arquivos estáticos de páginas da Web são atacados e adulterados.
Dynamic Tampering Attacks	Número de explorações de vulnerabilidade de aplicações Web e ataques de injeção.

----Fim

Exportação da lista de servidores

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 Escolha **Asset Management** > **Servers & Quota**. A página de guia **Servers** é exibida.

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 3 Clique em no canto superior direito da página de guia **Server** para exportar os detalhes da lista de servidores.

NOTA

Os detalhes de até 1000 servidores podem ser exportados por vez.

----Fim

3.4.2 Habilitação da proteção

3.4.2.1 Edição básica/profissional/empresarial/premium

As edições básica, profissional, empresarial e premium oferecem diferentes níveis de proteção para seus servidores. Você pode comprar e habilitá-las conforme necessário.

Precauções

A edição empresarial pode ser paga após o uso. Para habilitar outras edições, compre suas cotas primeiro. Para obter mais informações, consulte **Compra de uma cota do HSS**.

Verificar a frequência

O HSS realiza uma verificação completa no início da manhã todos os dias.

Depois de ativar a proteção do servidor, você pode exibir os resultados da verificação após a verificação automática na manhã seguinte ou executar uma verificação manual imediatamente.

Pré-requisito

O agente foi instalado nos servidores a serem protegidos, o status do agente é **Online** e o status da proteção é **Unprotected**.

Restrições

- Linux

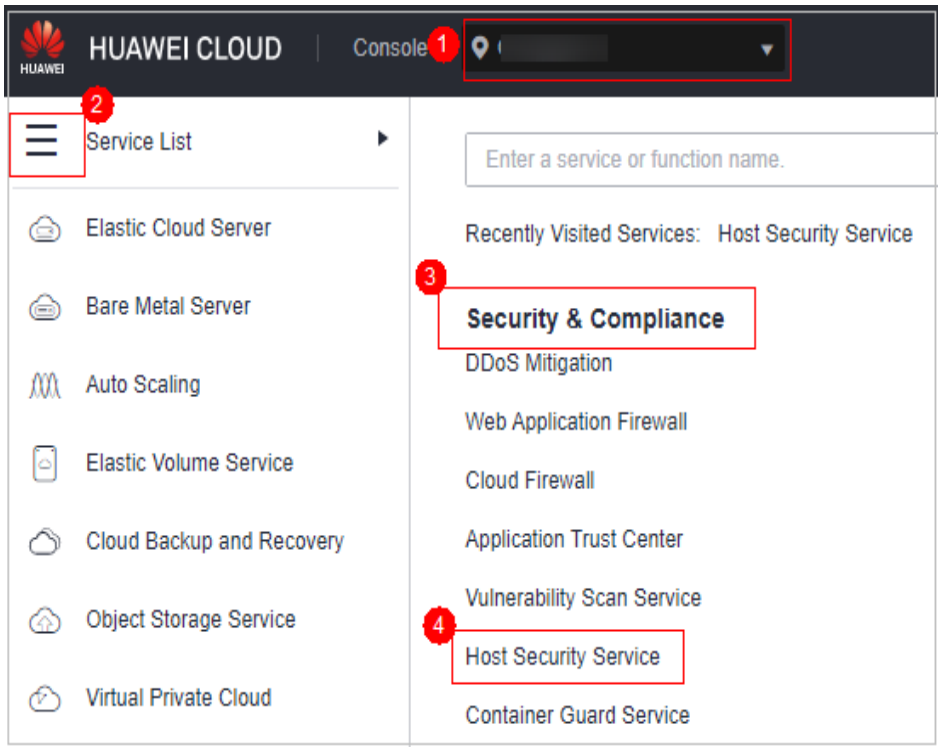
  Em servidores que executam o EulerOS com ARM, o HSS não bloqueia os endereços IP suspeitos de ataques de força bruta de SSH, mas apenas gera alarmes.
- Windows
  - Autorize o firewall do Windows quando ativar a proteção para um servidor do Windows. Não desative o firewall do Windows durante o período 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 3-20 Acessar o HSS



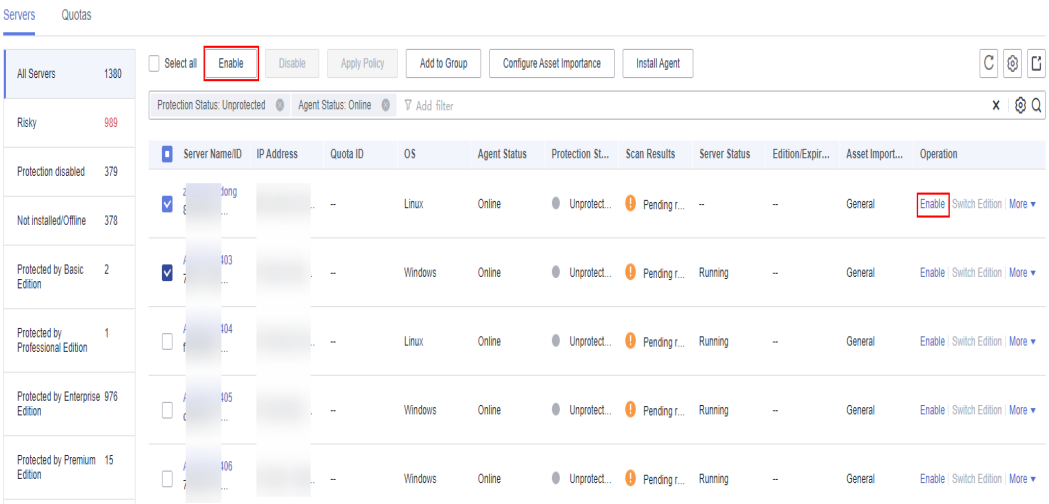
Passo 3 No painel de navegação, escolha **Asset Management** > **Servers & Quota**. Clique na guia **Servers**.

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 Habilite a proteção para um ou vários servidores.

Figura 3-21 Habilitar a proteção



- **Habilitar a proteção para um servidor**

Clique em **Enable** na coluna **Operation** de um servidor. Na caixa de diálogo exibida, confirme as informações do servidor e selecione o modo de cobrança, a edição e a cota.

Tabela 3-6 Parâmetros de proteção

Parâmetro	Descrição	Exemplo de valor
Billing Mode	– Anual/Mensal ■ Selecione a edição empresarial, básica, profissional ou premium. ■ Nenhuma avaliação gratuita está disponível aqui. Você será cobrado pela duração necessária selecionada. ■ Um pacote anual/mensal oferece um desconto maior do que o modo de pagamento por uso e é recomendado para usuários de longo prazo. – Pagamento por uso ■ As edições profissional ou empresarial são suportadas. ■ Você paga pelo tempo de uso dos recursos. Os preços são calculados por hora, e nenhuma taxa mínima é necessária.	Yearly/ Monthly
Edition	Selecione a edição básica, profissional, empresarial ou premium. – 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 está entre a edição básica e a edição empresarial. Ela suporta alterações de diretório de arquivos, detecção de shell anormal e gerenciamento de políticas. Para obter detalhes, consulte **Edições e recursos**. – Edição empresarial: fornece suporte para **DJCP MLPS certification**. 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. Para obter detalhes, consulte **Edições e recursos**. – Edição premium: ela ajuda você com **DJCP MLPS certification** 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 detalhes, consulte **Edições e recursos**.	Enterprise

Parâmetro	Descrição	Exemplo de valor
Select Quota	Selecione uma cota para o servidor. – Se você não quiser especificar uma cota, selecione **Select a quota randomly**. – Você também pode selecionar uma cota. Se você estiver ativando a proteção para vários servidores, apenas um deles será vinculado à cota selecionada e o restante dos servidores será vinculado a cotas alocadas aleatoriamente. **NOTA** Se o sistema exibir uma mensagem indicando que não há cotas disponíveis, você precisará comprar cotas primeiro.	Select a quota randomly

- **Habilitar a proteção em lotes**

  Selecione vários servidores e clique em **Enable** acima da lista de servidores. Na caixa de diálogo exibida, confirme as informações do servidor e selecione o modo de cobrança, a edição e a cota.

  NOTA

  Somente a edição empresarial é suportada.

Tabela 3-7 Parâmetros de proteção

Parâmetro	Descrição	Exemplo de valor
Billing Mode	– Anual/Mensal ■ Selecione a edição empresarial, básica, profissional ou premium. ■ Nenhuma avaliação gratuita está disponível aqui. Você será cobrado pela duração necessária selecionada. ■ Um pacote anual/mensal oferece um desconto maior do que o modo de pagamento por uso e é recomendado para usuários de longo prazo. – Pagamento por uso ■ As edições profissional ou empresarial são suportadas. ■ Você paga pelo tempo de uso dos recursos. Os preços são calculados por hora, e nenhuma taxa mínima é necessária.	Yearly/ Monthly

Parâmetro	Descrição	Exemplo de valor
Edition	Selecione a edição básica, profissional, empresarial ou premium. – 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 está entre a edição básica e a edição empresarial. Ela suporta alterações de diretório de arquivos, detecção de shell anormal e gerenciamento de políticas. Para obter detalhes, consulte **Edições e recursos**. – Edição empresarial: fornece suporte para **DJCP MLPS certification**. 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. Para obter detalhes, consulte **Edições e recursos**. – Edição premium: ela ajuda você com **DJCP MLPS certification** 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 detalhes, consulte **Edições e recursos**.	Enterprise
Select Quota	Selecione uma cota para o servidor. – Se você não quiser especificar uma cota, selecione **Select a quota randomly**. – Você também pode selecionar uma cota. Se você estiver ativando a proteção para vários servidores, apenas um deles será vinculado à cota selecionada e o restante dos servidores será vinculado a cotas alocadas aleatoriamente. **NOTA** Se o sistema exibir uma mensagem indicando que não há cotas disponíveis, você precisará comprar cotas primeiro.	Select a quota randomly

Passo 5 Confirme as informações e clique em **OK**. Se o status de proteção dos servidores de destino for **Protected**, a proteção foi ativada.

NOTA

A prevenção de ransomware é ativada automaticamente com a edição premium. Para aprimorar a prevenção de ransomware, você pode configurar diretórios protegidos e ativar a proteção dinâmica de honeypot conforme necessário. Você também é aconselhado a ativar o backup para que você possa restaurar os dados no caso de um ataque de ransomware para minimizar as perdas. Para obter detalhes, consulte **Modificação de uma política de proteção** and **Habilitação de backup de ransomware**.

----Fim

Procedimento de acompanhamento

A edição premium suporta proteção contra ransomware. Após a compra da edição premium, você pode ativar a proteção contra ransomware para o seu servidor consultando **Habilitação da proteção contra ransomware**.

3.4.2.2 Edição WTP

A edição WTP fornece recursos de proteção contra adulteração na Web para seus servidores.

Como a WTP evita a adulteração de páginas na Web

Tabela 3-8 Como funciona a WTP

Tipo	Mecanismo
Proteção estática de páginas da Web	1. Bloqueio de diretório local A WTP bloqueia arquivos em um diretório de arquivos da Web em uma unidade para impedir que invasores os modifiquem. Os administradores do site podem atualizar o conteúdo do site usando processos privilegiados. 2. Backup e restauração proativos Se a WTP detectar que um arquivo em um diretório protegido foi adulterado, ela usará imediatamente o arquivo de backup no servidor local para restaurar o arquivo. 3. Backup e restauração remotos Se um diretório de arquivo ou diretório de backup no servidor local for inválido, você pode usar o serviço de backup remoto para restaurar a página da Web adulterada.
Proteção dinâmica de páginas da Web	Proteção dinâmica de página da Web para o Tomcat. 1. Filtragem de comportamento malicioso baseada em RASP A autoproteção de aplicações em tempo de execução (RASP), exclusiva da Huawei, detecta comportamentos de programas de aplicações, impedindo que os invasores adulterem páginas da Web por meio de programas de aplicações. 2. Controle de acesso a arquivos de disco de rede A WTP implementa um gerenciamento refinado para controlar as permissões para adicionar, modificar e consultar o conteúdo do arquivo em discos de rede, evitando adulterações sem afetar a liberação do conteúdo do site.

Pré-requisito

- O agente foi instalado nos servidores a serem protegidos, o status do agente é **Online** e o status da proteção é **Unprotected**.

Configuração de diretórios protegidos

Você pode adicionar até 50 diretórios a serem protegidos. Para obter detalhes, consulte **Adição de um diretório protegido**.

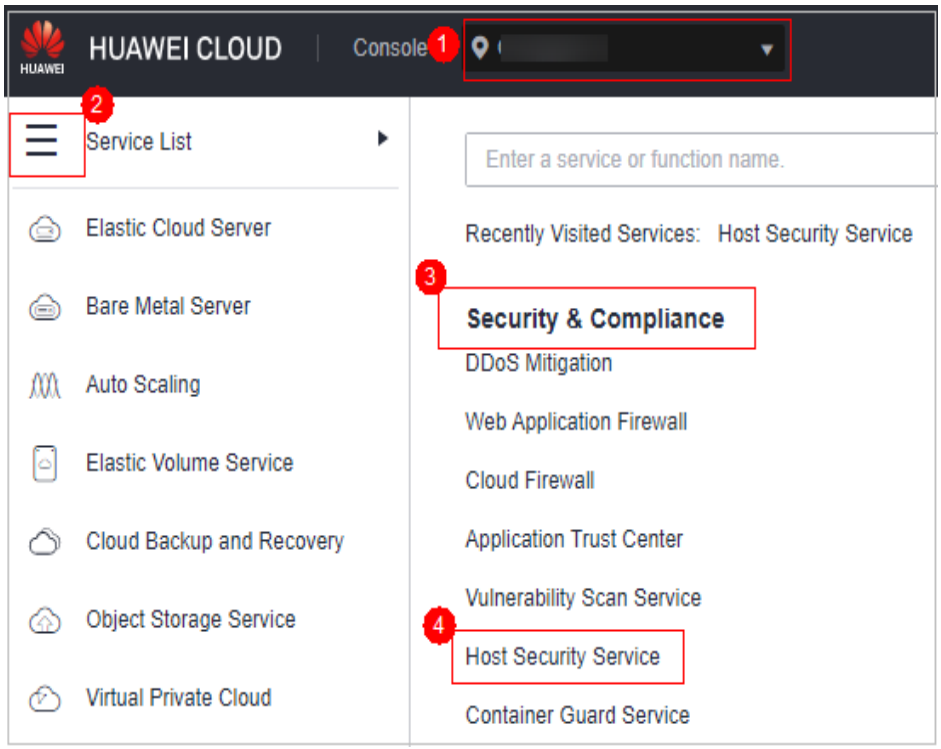
Para registrar o status de execução do servidor em tempo real, exclua os arquivos de log no diretório protegido. Você pode conceder altas permissões de leitura e gravação para arquivos de log para impedir que invasores visualizem ou adulterem os arquivos de log.

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 3-22 Acessar o HSS

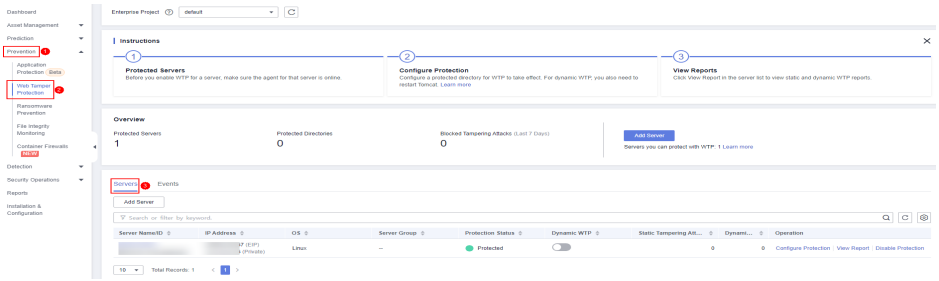


Passo 3 No painel de navegação, escolha **Protection** > **Web Tamper Protection**. Na página **Web Tamper Protection**, clique na guia **Servers**.

NOTA

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

Figura 3-23 Entrar na página para configurações de diretório protegido

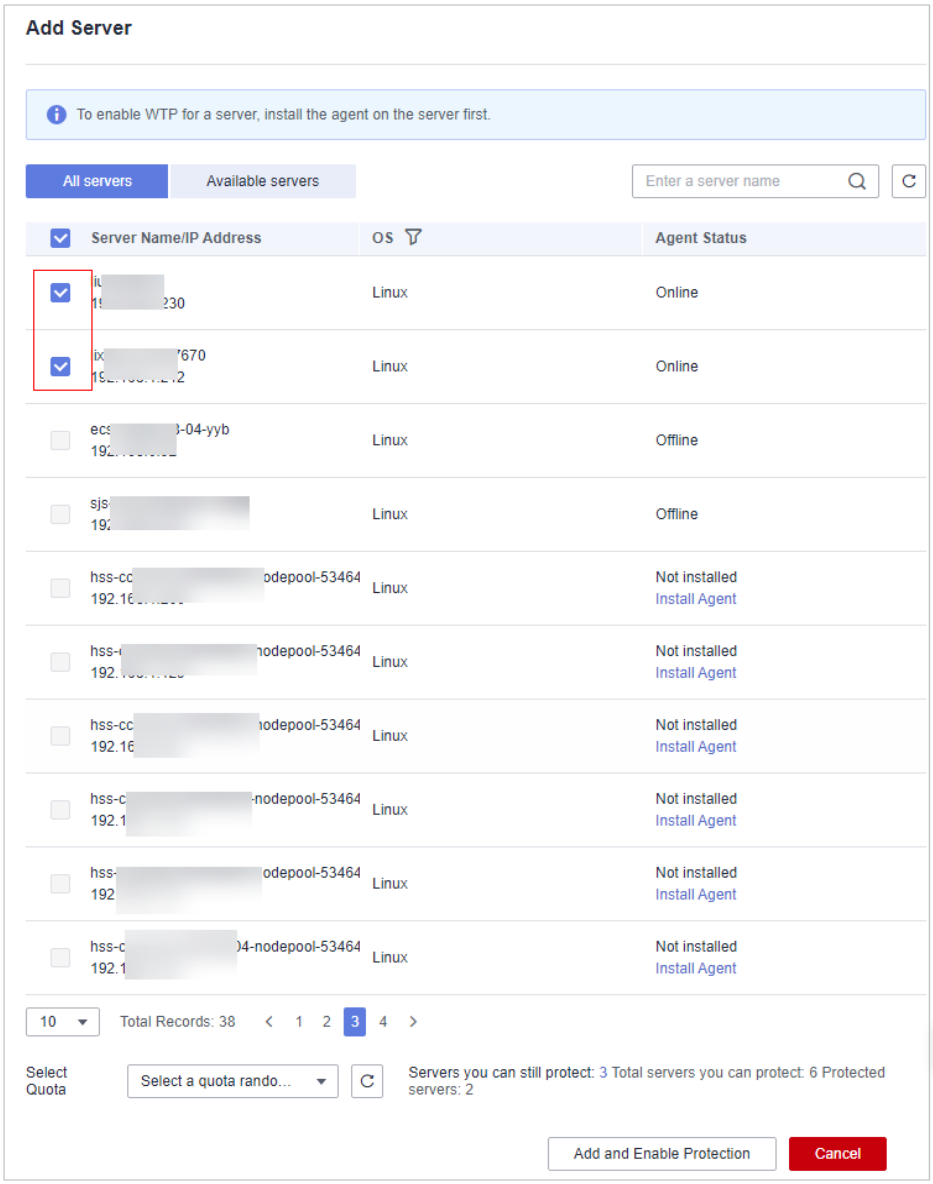


Passo 4 Clique em **Add Server**. Na caixa de diálogo exibida, selecione servidores. Na lista suspensa **Select Quota**, selecione **Select a quota randomly**.

NOTA

Os servidores selecionados devem ser iguais ou menores que as cotas disponíveis. Para obter mais informações, consulte **Compra de cotas da WTP**.

Figura 3-24 Adicionar servidores protegidos



Passo 5 Clique em **Add and Enable Protection** e verifique o status da proteção. Escolha **Protection** > **Web Tamper Protection**. Na página **Web Tamper Protection**, clique na guia **Servers**. Se o **Protection Status** do servidor for **Protected**, a WTP foi ativada.

AVISO

- Depois que a WTP estiver ativada, configure os diretórios protegidos para que a WTP entre em vigor. Para mais detalhes, consulte **Adição de um diretório protegido**.
- A WTP dinâmica só pode ser ativada para servidores do Linux e só pode ser usada após a reinicialização do Tomcat.
- Você pode verificar o status da proteção do servidor na página **Web Tamper Protection**.

  A edição premium será ativada quando você ativar a WTP. Você pode executar as seguintes operações para verificar o status da proteção:

  – Escolha **Prevention** > **Web Tamper Protection**. Se o **Protection Status** do servidor for **Protected**, a WTP foi ativada.

  – Escolha **Asset Management** > **Servers & Quota** e clique na guia **Servers**. Se o status de proteção do servidor de destino estiver **Enabled** e a **Edition/Expiration Date** dele for **Premium (included with WTP)**, a edição premium fornecida pela edição WTP será ativada gratuitamente.
- A prevenção de ransomware é ativada automaticamente com a edição WTP. Para aprimorar a prevenção de ransomware, você pode configurar diretórios protegidos e ativar a proteção dinâmica de honeypot conforme necessário. Você também é aconselhado a ativar o backup para que você possa restaurar os dados no caso de um ataque de ransomware para minimizar as perdas. Para obter detalhes, consulte **Modificação de uma política de proteção** e **Ativação de backup de ransomware**.

----Fim

Procedimento de acompanhamento

A edição WTP suporta proteção contra ransomware. Depois que a edição WTP for comprada, você poderá ativar a proteção contra ransomware para o seu servidor consultando **Ativação da prevenção contra ransomware**.

3.4.3 Desativação da proteção

3.4.3.1 Edição básica/profissional/empresarial/premium

Você pode desabilitar a proteção de um servidor. Uma cota que foi desvinculada de um servidor pode ser vinculada a outro.

Precauções

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

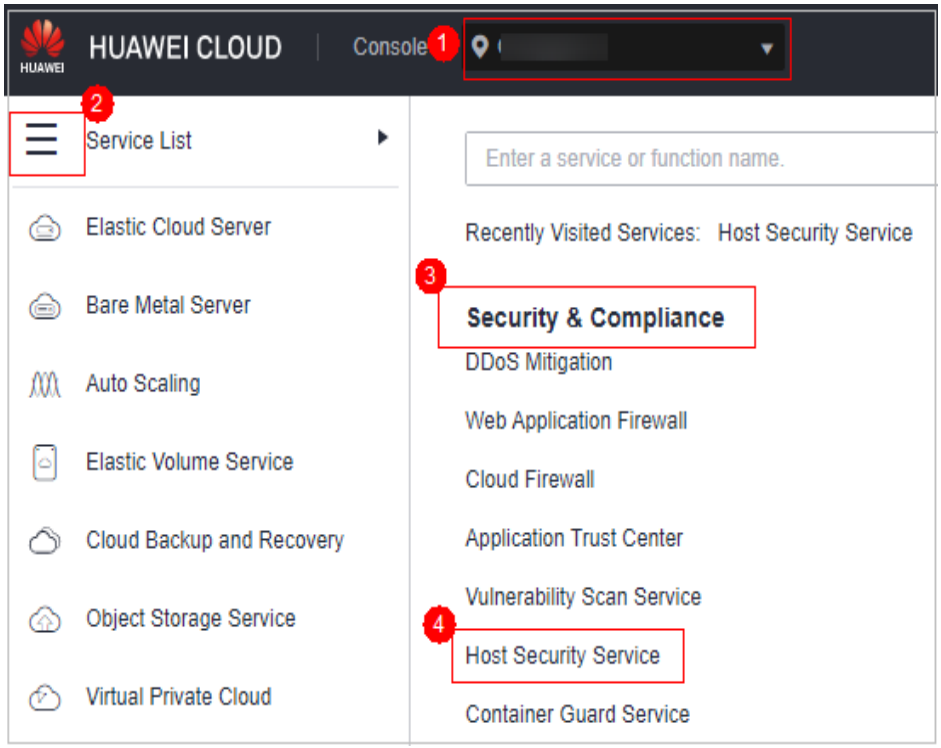
Para cancelar a assinatura da cota de pagamento por uso da edição empresarial, você só precisa desabilitar a proteção.

Desabilitação da 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 3-25 Acessar o HSS



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

NOTA

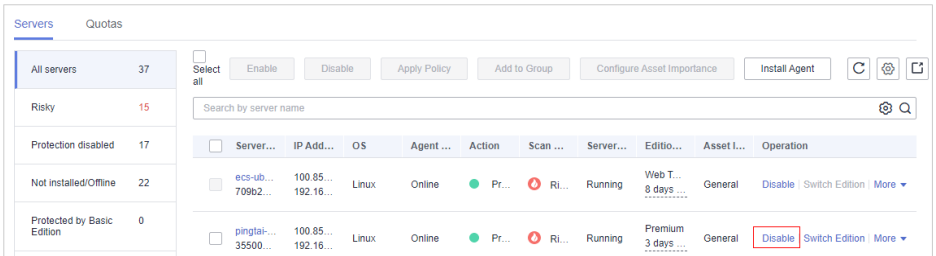
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Passo 4 Desabilite a proteção para um ou vários servidores.

- **Desabilitar a proteção para um servidor**

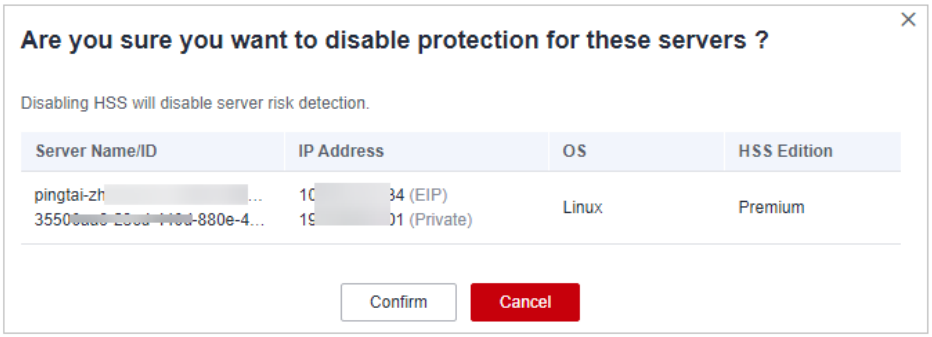
  a. Clique em **Disable** na coluna **Operation** de um servidor.

  Figura 3-26 Desabilitar a proteção para um servidor



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

Figura 3-27 Confirmar as informações sobre um servidor



c. Verifique o status da proteção na lista de servidores. Se estiver **Unprotected**, a proteção foi desabilitada.

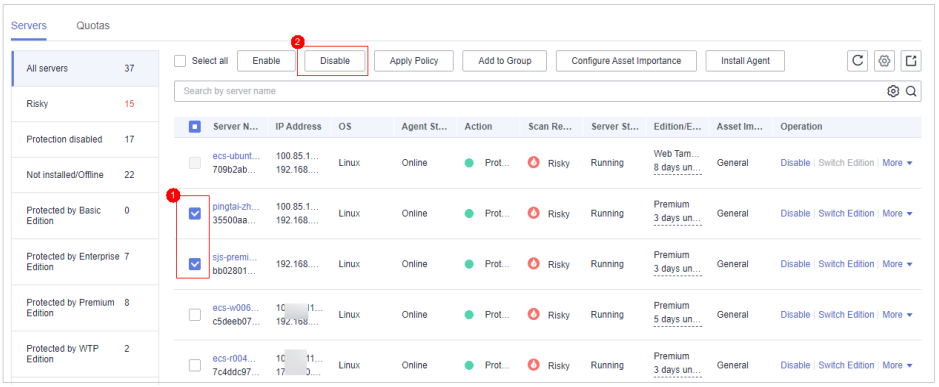
⚠ CUIDADO

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

- **Desabilitar a proteção em lotes**

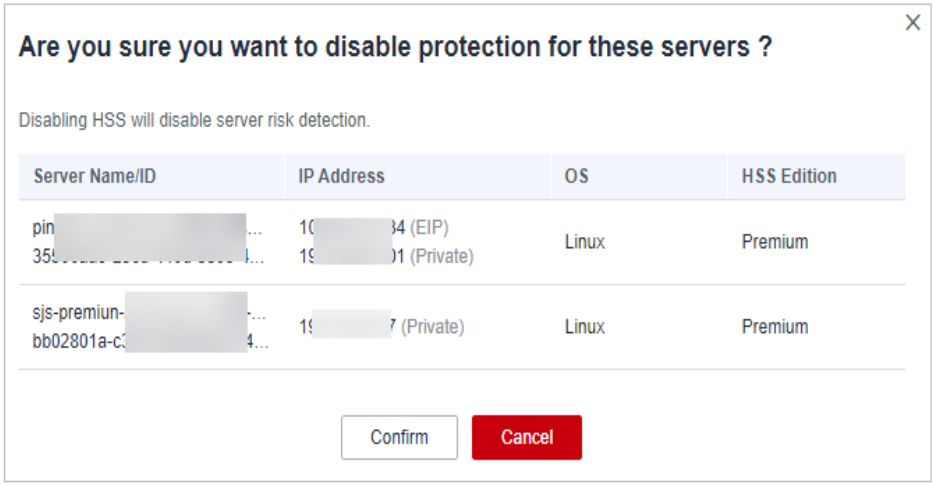
a. Selecione vários servidores e clique em **Disable** acima da lista de servidores.

Figura 3-28 Desabilitar a proteção em lotes



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

Figura 3-29 Confirmar informações sobre vários servidores



c. Verifique o status da proteção na lista de servidores. Se estiver **Unprotected**, a proteção foi desabilitada.

CUIDADO

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

----Fim

3.4.3.2 Edição WTP

Você pode desativar a edição WTP para um servidor. Uma cota que foi desvinculada de um servidor pode ser vinculada a outro.

Precauções

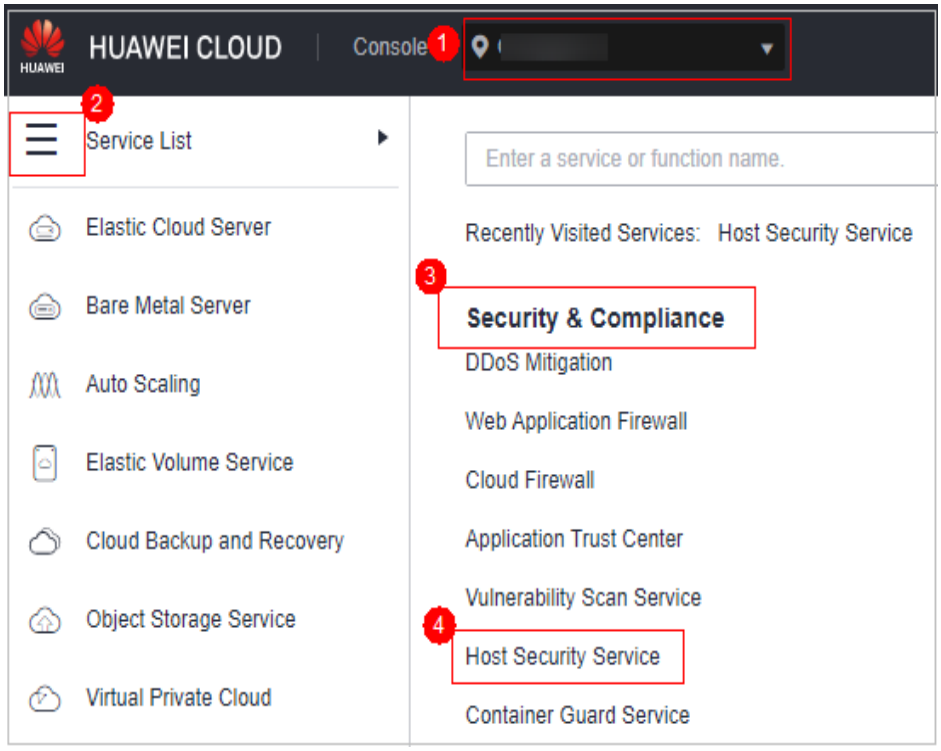
Desativar a proteção não afeta os serviços, mas aumentará os riscos de segurança. É aconselhável manter seus servidores protegidos.

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 3-30 Acessar o HSS

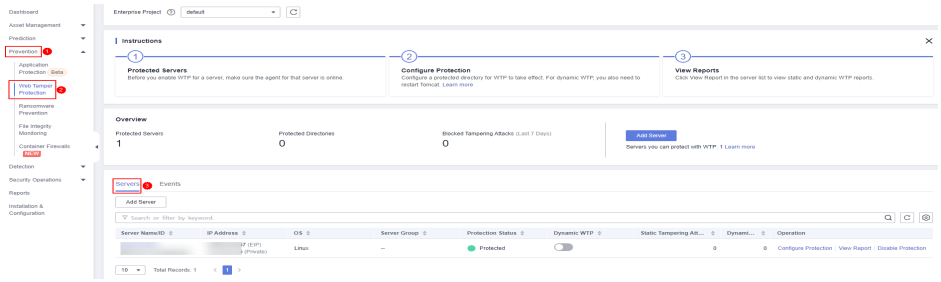


Passo 3 No painel de navegação, escolha **Protection** > **Web Tamper Protection**. Na página **Web Tamper Protection**, clique na guia **Servers**.

NOTA

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

Figura 3-31 Entrar na página para configurações de diretório protegido

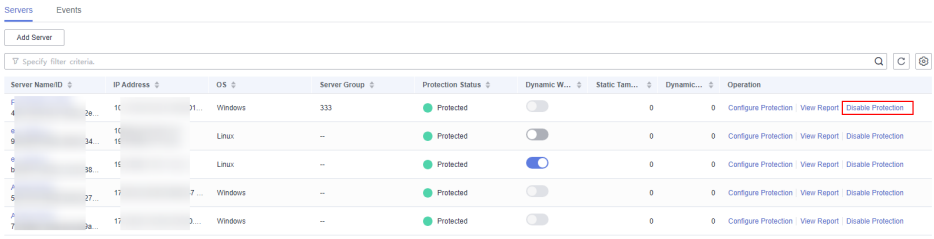


Passo 4 Clique em **Disable** na coluna **Operation**.

NOTA

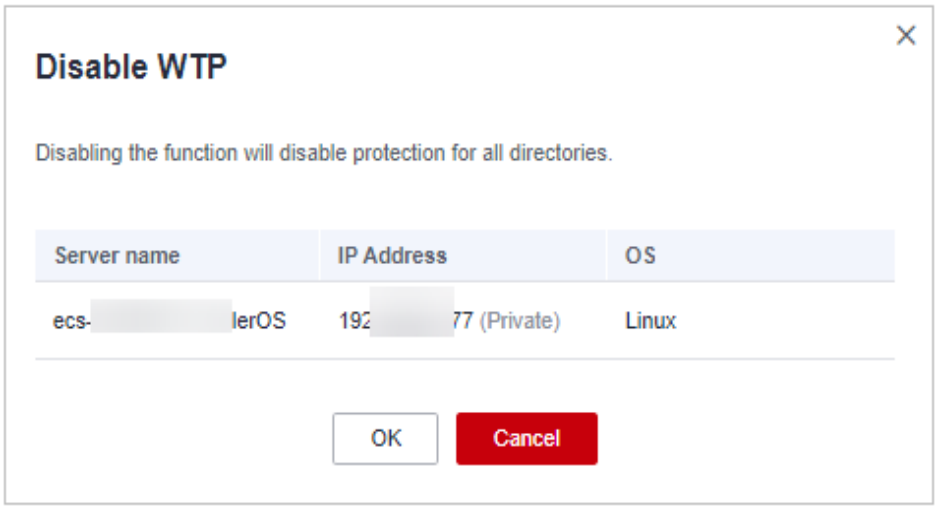
A edição WTP não pode ser desativada para servidores em lotes.

Figura 3-32 Desativar a WTP



Passo 5 Na caixa de diálogo exibida, confirme as informações e clique em **OK**.

Figura 3-33 Confirmar informações sobre a desativação da WTP



Passo 6 Escolha **Asset Management** > **Servers & Quota** e clique na guia **Servers**. 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

3.4.4 Aplicação de uma política

Você pode rapidamente configurar e iniciar verificações de servidor usando grupos de políticas. Basta criar um grupo, adicionar políticas a ele e aplicar esse grupo aos servidores. Os agentes implementados em seus servidores farão a verificação de tudo especificado nas políticas.

Precauções

- Quando você habilita a edição empresarial, o grupo de políticas desta edição (incluindo senha fraca e políticas de detecção de shell de site) entra em vigor para todos os seus servidores por padrão.

- Quando você habilita a edição premium sozinha ou a edição premium incluída na edição WTP, o grupo de políticas desta edição entra em vigor por padrão.

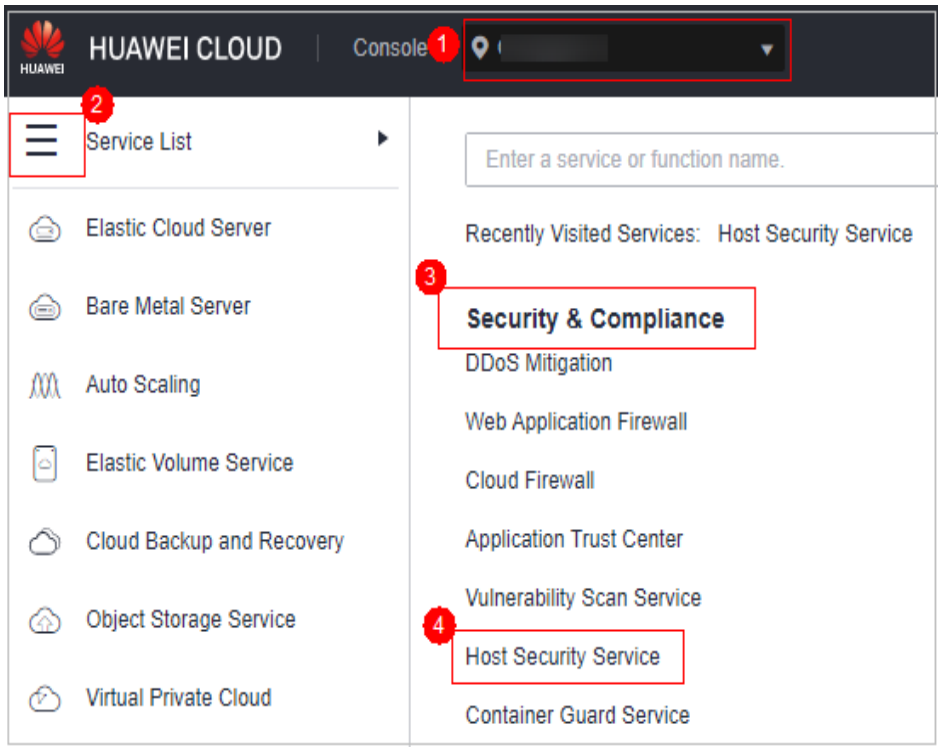
  Para criar seu próprio grupo de políticas, você pode copiar o grupo de políticas da edição premium e adicionar ou remover políticas na cópia.

Criação de um grupo de políticas

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 3-34 Acessar o HSS



Passo 3 Na árvore de navegação à esquerda, escolha **Security Operations** > **Policies**

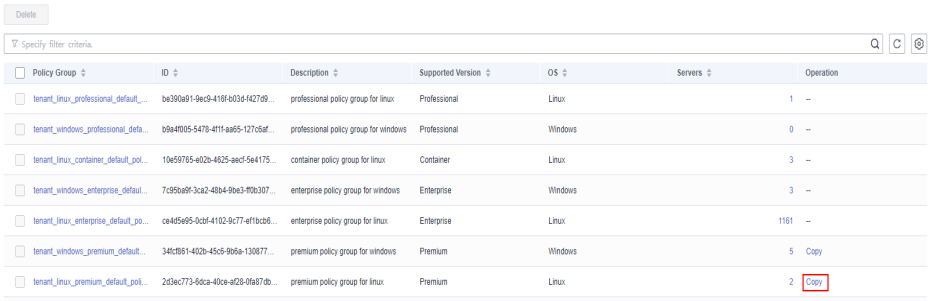
NOTA

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 Copie um grupo de políticas.

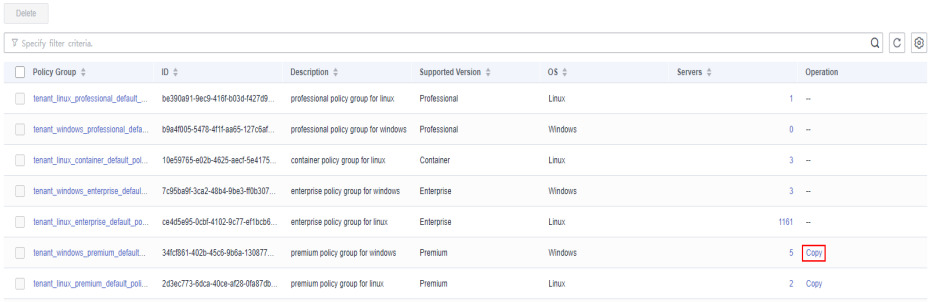
- Selecione o grupo de políticas **tenant_linux_premium_default_policy_group**. Localize a linha em que esse grupo de políticas reside e clique em **Copy** na coluna **Operation**.

Figura 3-35 Copiar um grupo de políticas do Linux



- Selecione o grupo de políticas **tenant_windows_premium_default_policy_group**. Clique em **Copy** na coluna **Operation**.

Figura 3-36 Copiar um grupo de políticas do Windows

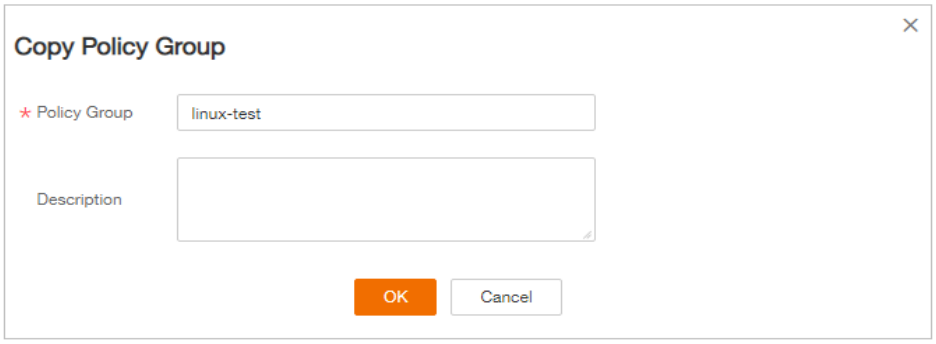


Passo 5 Na caixa de diálogo exibida, insira um nome e uma descrição do grupo de políticas e clique em **OK**.

NOTA

- O nome de um grupo de políticas deve ser exclusivo, ou o grupo não será criado.
- O nome do grupo de políticas e sua descrição podem conter apenas letras, dígitos, sublinhados (_), hifens (-) e espaços e não podem começar ou terminar com um espaço.

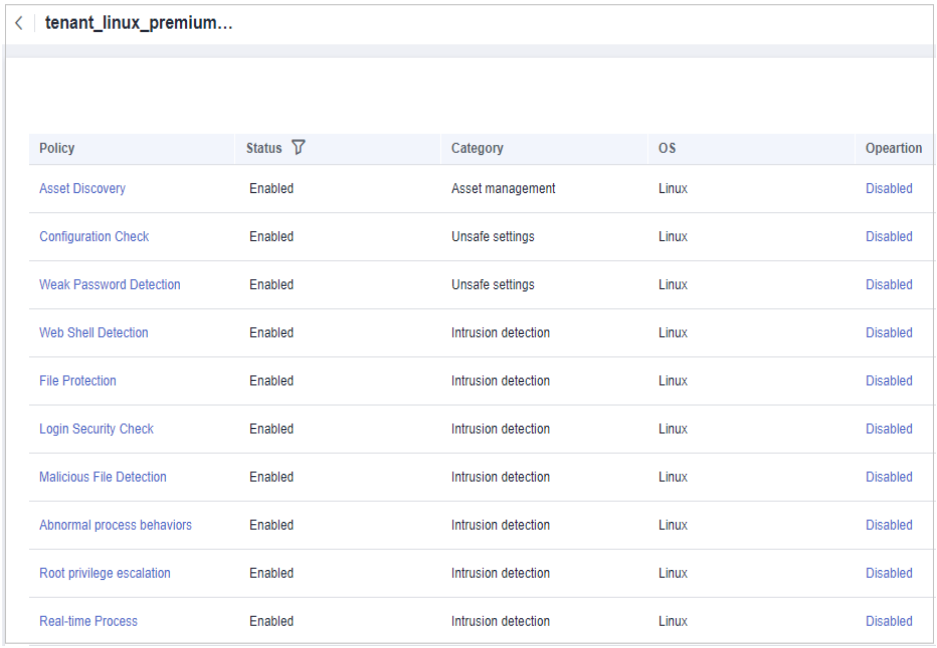
Figura 3-37 Criar um grupo de políticas



Passo 6 Clique em **OK**.

Passo 7 Clique no nome do grupo de políticas que acabou de criar. As políticas no grupo serão exibidas.

Figura 3-38 Políticas em um grupo



Passo 8 Clique em um nome de política e modifique suas configurações conforme necessário. Para mais detalhes, consulte **Modificação de uma política**.

Passo 9 Ative ou desative a política clicando no botão correspondente na coluna **Operation**. Você pode clicar em  para atualizar a página.

----Fim

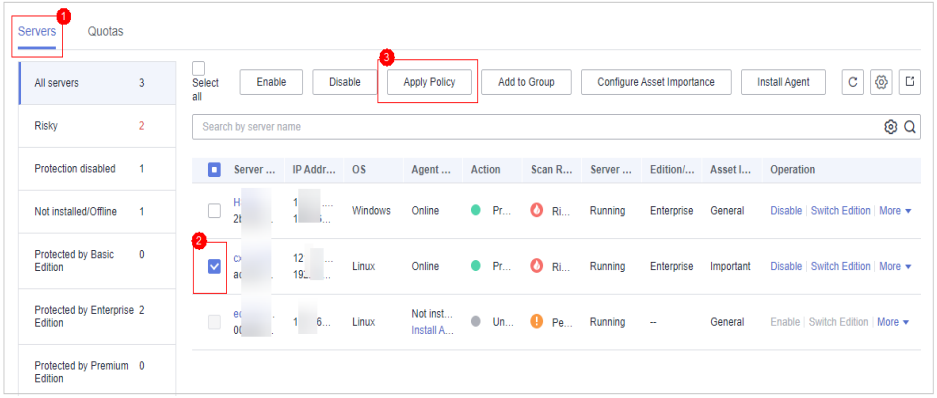
Aplicação de um grupo de políticas

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Servers & Quota** e clique em **Servers**.

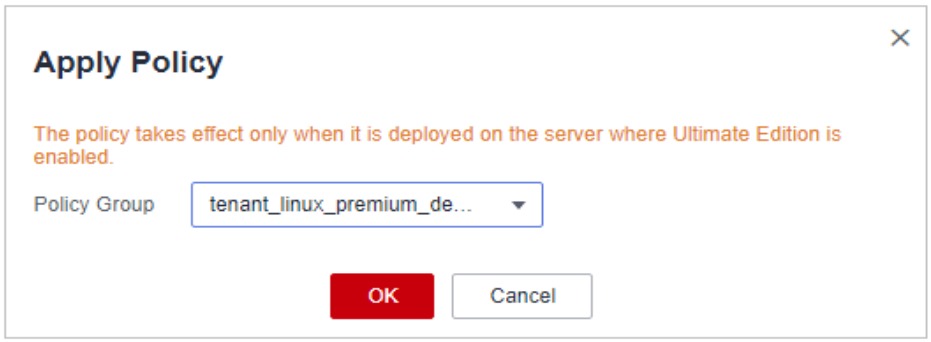
Passo 3 Na página **Devices**, selecione um ou mais hosts de destino e clique em **Apply Policy**.

Figura 3-39 Aplicar uma política



Passo 4 Na caixa de diálogo exibida, selecione um grupo de políticas e clique em **OK**.

Figura 3-40 Selecionar um grupo de políticas



NOTA

- Políticas anteriores aplicadas a um servidor se tornarão inválidas se você aplicar novas políticas ao servidor.
- As políticas são aplicadas aos servidores em 1 minuto.
- As políticas aplicadas aos servidores off-line não entrarão em vigor até que os servidores estejam on-line.
- Em um grupo de políticas implementado, você pode habilitar, desabilitar ou modificar políticas.
- Um grupo de políticas que tenha sido implementado não pode ser excluído.

----Fim

3.4.5 Gerenciamento de grupos de servidores

Para gerenciar servidores por grupo, você pode criar um grupo de servidores e adicionar servidores a ele.

Você pode verificar o número de servidores, servidores inseguros e servidores desprotegidos em um grupo.

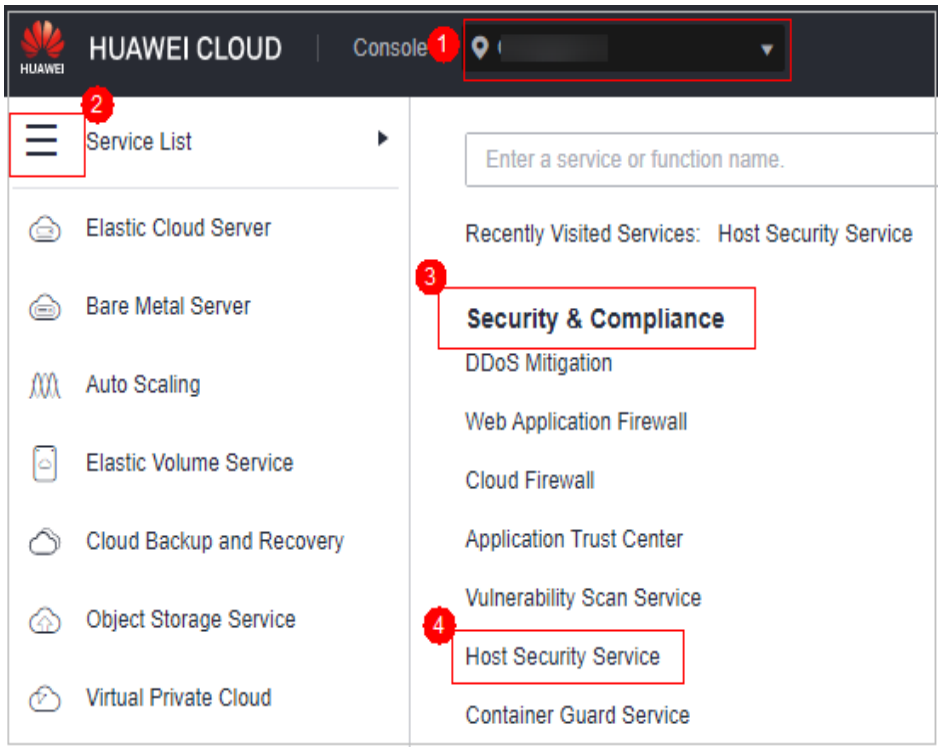
Criação de um grupo de servidores

Depois de criar um grupo de servidores, você pode adicionar servidores ao grupo para gerenciamento unificado.

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 3-41 Acessar o HSS

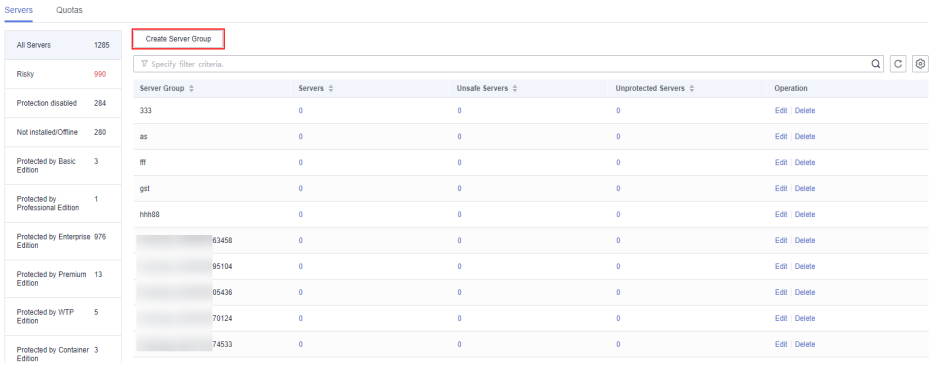


Passo 3 No painel de navegação, escolha **Asset Management** > **Servers & Quota**, clique em **Server Groups** na lista de **Server** e clique em **Create Server Group**.

NOTA

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

Figura 3-42 Acessar a página de grupos de servidores

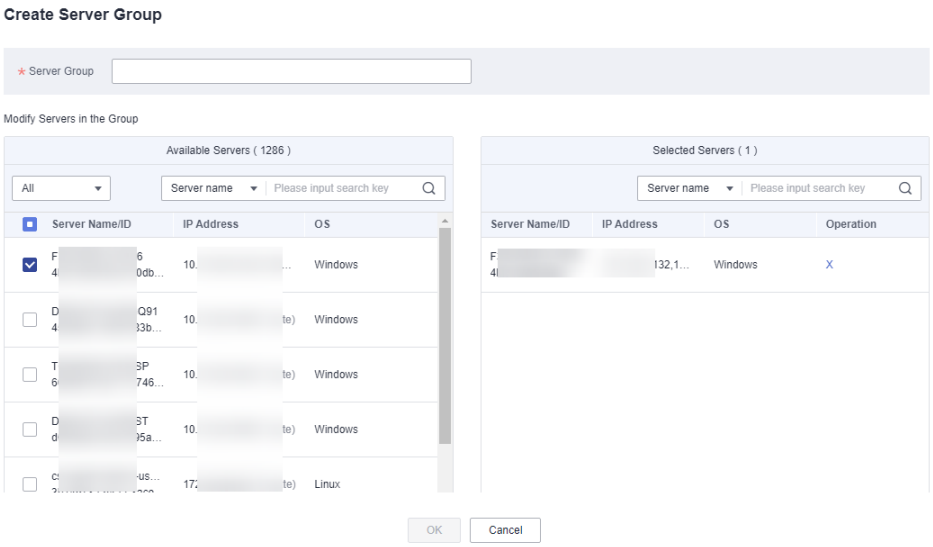


Passo 4 Na caixa de diálogo **Create Server Group**, insira um nome de grupo de servidores e selecione os servidores a serem adicionados ao grupo.

NOTA

- Um nome de grupo de servidores deve ser exclusivo, caso contrário, o grupo não será criado.
- Um nome não pode conter espaços. Ele contém apenas letras, dígitos, sublinhados (_), hifens (-), pontos (.), asteriscos (*) e sinais de adição (+). O comprimento não pode exceder 64 caracteres.

Figura 3-43 Criação de um grupo de servidores



Passo 5 Clique em **OK**.

----Fim

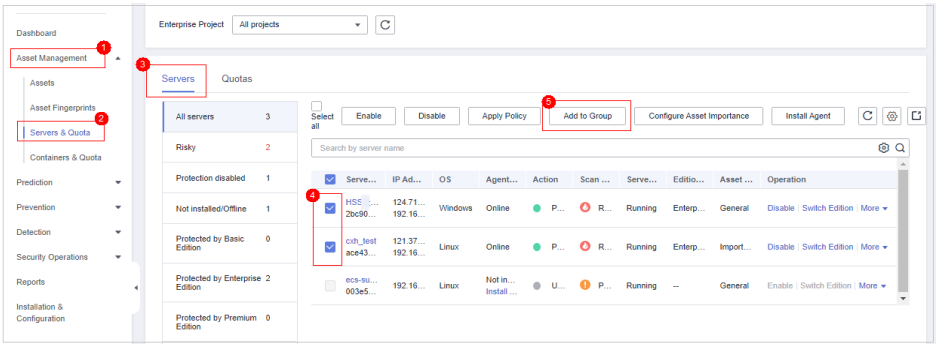
Adição de servidores a grupos

Você pode adicionar servidores a um grupo de servidores existente.

Passo 1 Clique na guia **Server**.

Passo 2 Selecione um ou mais servidores e clique em **Add to Group**.

Figura 3-44 Adicionar servidores a um grupo



NOTA

Para adicionar um servidor a um grupo, você também pode localizar a linha onde o servidor reside, clicar em **More** na coluna **Operation** e escolher **Add to Group**.

Passo 3 Na caixa de diálogo exibida, selecione um grupo de servidores e clique em **OK**.

NOTA

Um servidor pode ser adicionado a apenas um grupo de servidores.

----Fim

Procedimento de acompanhamento

Editar um grupo de servidores

Passo 1 Clique em **Servers & Quota** e clique em **Server Groups** na guia **Servers**.

Passo 2 Localize a linha onde reside um grupo de servidores e clique em **Edit** na coluna **Operation**.

Passo 3 Na caixa de diálogo exibida, altere o nome do grupo de servidores e adicione ou remova servidores do grupo.

Passo 4 Clique em **OK**.

----Fim

Excluir um grupo de servidores

Passo 1 Clique em **Servers & Quota** e clique em **Server Groups** na guia **Servers**.

Passo 2 Localize a linha onde reside um grupo de servidores e clique em **Delete** na coluna **Operation**.

NOTA

Depois que o grupo de servidores for excluído, a coluna **Server Group** dos servidores que estavam no grupo ficará em branco.

----Fim

3.4.6 Configuração da importância do ativo

Por padrão, o HSS considera todos os servidores como ativos gerais. Você pode configurar os níveis de importância dos ativos dos servidores e gerenciar os servidores de acordo.

Os ativos são classificados nos seguintes tipos:

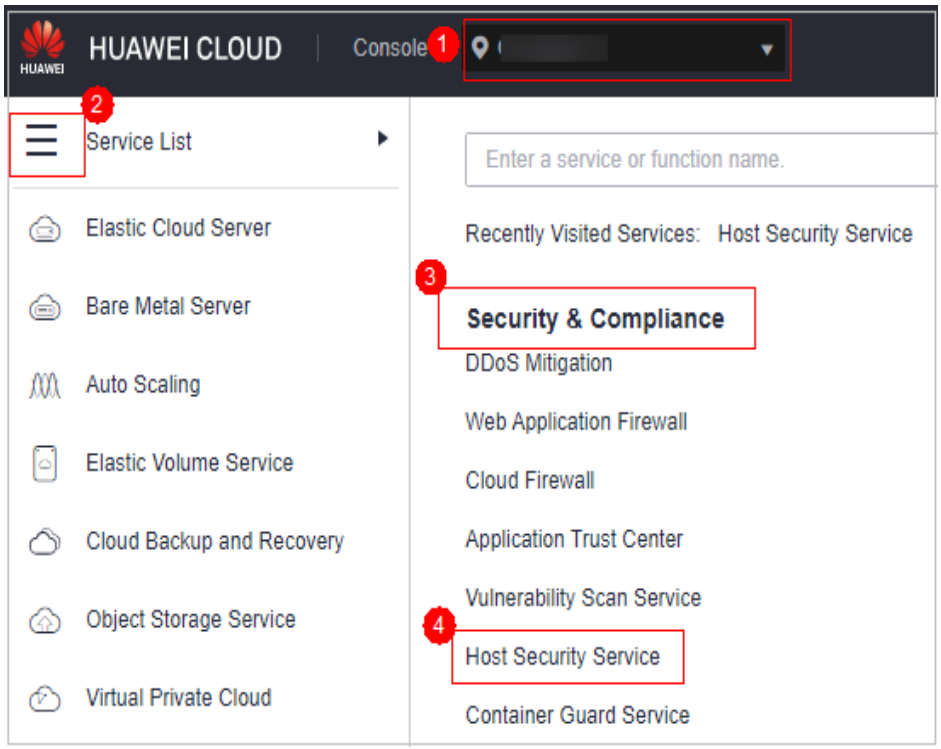
- **Important**. Especifique esse nível para servidores que executam serviços importantes ou armazenam dados importantes.
- **General**. Especifique esse nível para servidores que executam serviços gerais ou armazenam dados gerais.
- **Test**. Especifique esse nível para servidores que executam serviços de teste ou armazenam dados de teste.

Verificação da importância do ativo

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 3-45 Acessar o HSS



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

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 Na parte inferior da página da guia, verifique a importância do ativo. Você pode clicar em **Important**, **General** ou **Test** para exibir os servidores por nível de importância.

----Fim

Especificação da importância do ativo

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Servers & Quota**. Clique na guia **Servers**.

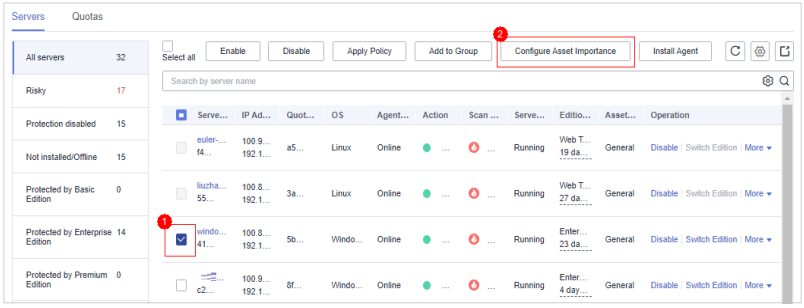
NOTA

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

Passo 3 Configure a importância do ativo.

- Configurar um servidor
  - Método 1: selecionar um servidor e configurar sua importância de ativo.
    i. Selecione um servidor e clique em **Configure Asset Importance**.

Figura 3-46 Selecionar um único servidor



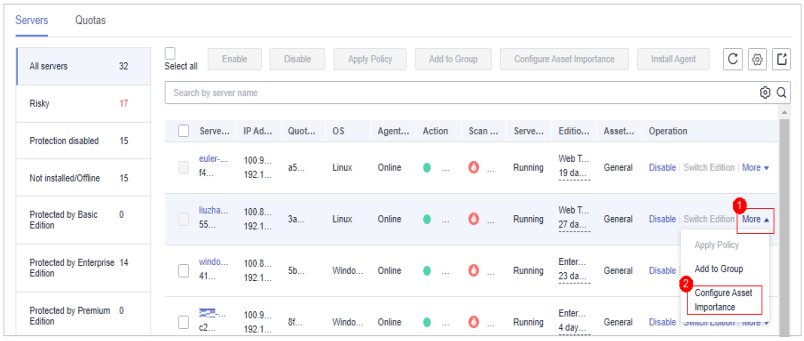
ii. Na caixa de diálogo que é exibida, selecione um nível de importância do ativo.

iii. Confirme as informações e clique em **OK**.

– Método 2: clicar no botão de configuração na coluna **Operation**.

i. Na coluna **Operation** de um servidor, escolha **More** > **Configure Asset Importance**.

Figura 3-47 Selecionar um único servidor



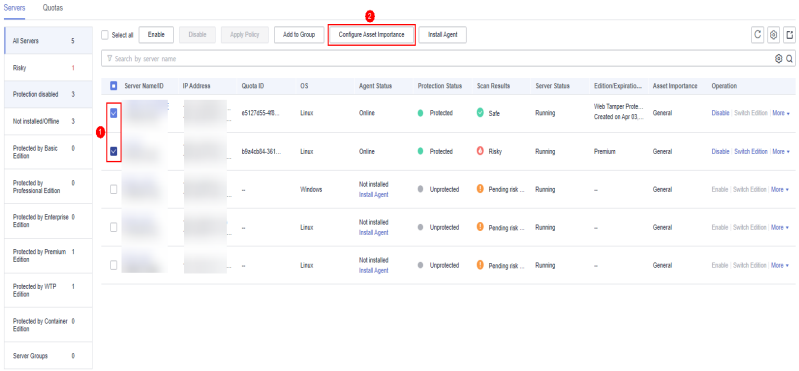
ii. Na caixa de diálogo que é exibida, selecione um nível de importância do ativo.

iii. Confirme as informações e clique em **OK**.

- Configurar servidores em lotes

a. Selecione vários servidores e clique em **Configure Asset Importance**.

Figura 3-48 Selecionar servidores



b. Na caixa de diálogo que é exibida, selecione um nível de importância do ativo.

c. Confirme as informações e clique em **OK**.

----Fim

3.4.7 Instalação do agente em um único servidor em um clique

Se já houver um servidor com um agente on-line, você poderá instalar o agente com um clique em um servidor do Linux na mesma VPC desse servidor.

Pré-requisitos

- Há um servidor com um agente on-line na VPC do servidor do Linux em que o agente será instalado.
- O servidor do Linux suporta logon SSH.
- Você obteve a conta, o número da porta e a senha para efetuar logon no servidor do Linux onde o agente será instalado.
- O status do servidor do Linux no qual o agente será instalado é **Running**.

Restrições

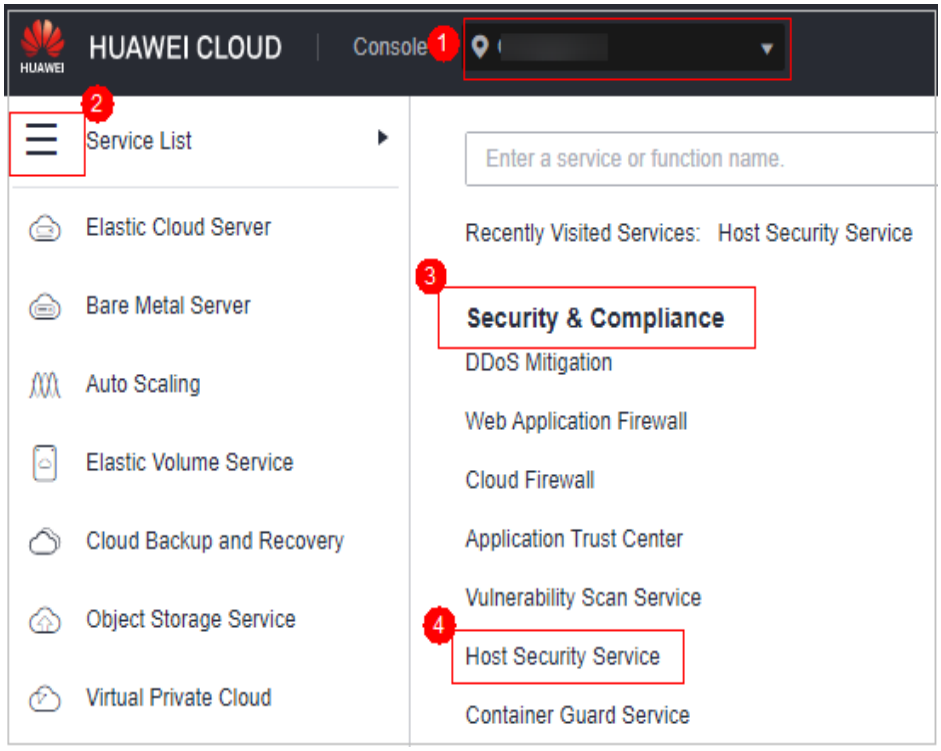
- Para obter detalhes sobre os SOs suportados pelo agente do HSS, consulte **SOs suportados**.
- Atualmente, apenas os servidores do Linux suportam a instalação do agente com um clique. Para obter detalhes sobre como instalar o agente em um servidor do Windows, consulte **Instalação de um agente no Windows**.

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 3-49 Acessar o HSS

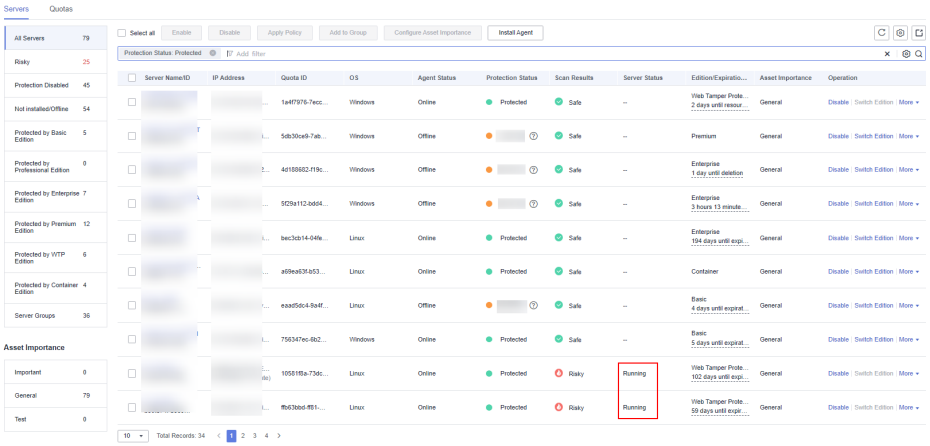


Passo 3 No painel de navegação, escolha **Asset Management** > **Servers & Quota**. Clique na guia **Servers**.

NOTA

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

Figura 3-50 Lista de servidores



Passo 4 Na coluna **Agent Status** de um servidor do Linux, clique em **Install Agent**.

AVISO

- O status do servidor do Linux em que o agente será instalado deve ser **Running**.
- Deve haver um servidor com um agente on-line na VPC do servidor do Linux em que o agente será instalado.

Passo 5 Digite a senha do usuário **root** e a porta para efetuar logon no servidor.

NOTA

A porta padrão do sistema é **22**. Para consultar a porta SSH do Linux, faça logon remotamente no servidor de destino e execute o seguinte comando no servidor do Linux:

```
cat /etc/ssh/sshd_config | grep Port
```

Passo 6 Clique em **OK**. Os agentes serão instalados automaticamente nos servidores selecionados.

Se o status do agente for **Online**, isso indica que o agente foi instalado.

----Fim

3.4.8 Instalação de agentes em lotes (com a mesma conta de servidor e senha)

Depois de criar uma tarefa de instalação do agente em lote, o sistema instalará os agentes automaticamente. Você pode ativar a proteção para os servidores de destino depois que os agentes forem instalados com sucesso.

Pré-requisitos

- Há um servidor com um agente on-line na VPC dos servidores onde o agente será instalado.
- Todos os servidores de destino devem suportar logon SSH.
- Você obteve a conta, o número da porta e a senha para efetuar logon no servidor onde o agente será instalado.
- O status do servidor em que o agente será instalado é **Running**.

Restrições

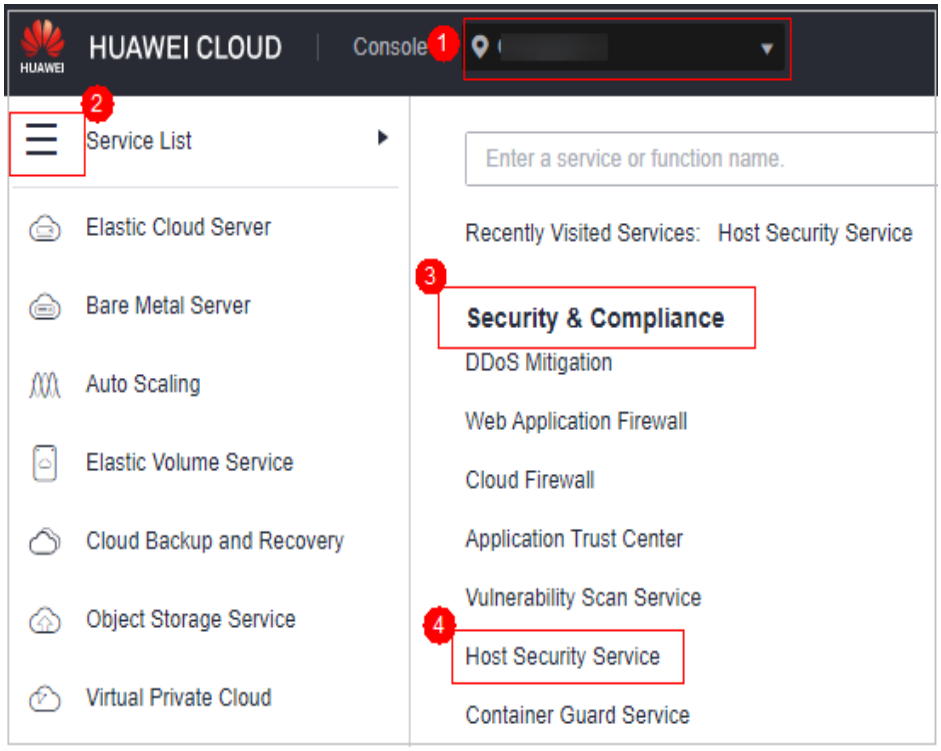
- Atualmente, apenas servidores de Linux podem instalar agentes em lotes.
- Você pode instalar o agente em um máximo de 50 servidores por vez.
- Para obter detalhes sobre os SOs suportados pelo agente, consulte **SOs suportados**.

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 3-51 Acessar o HSS

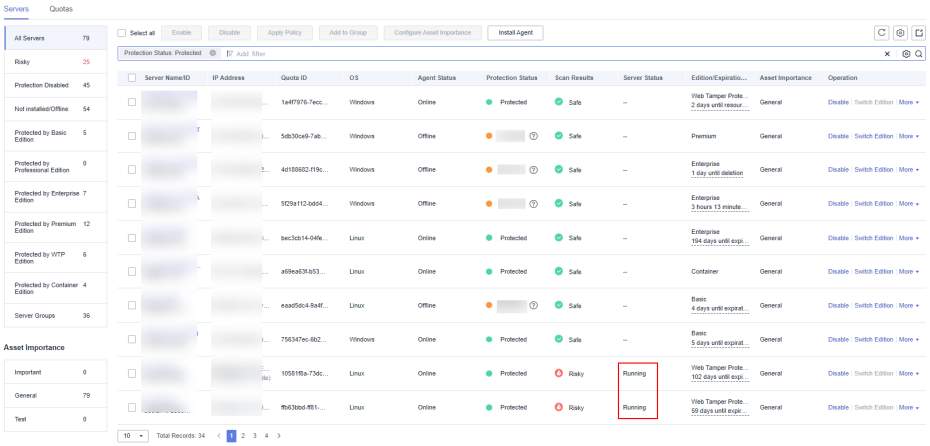


Passo 3 No painel de navegação, escolha **Asset Management** > **Servers & Quota**. Clique na guia **Servers**.

NOTA

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

Figura 3-52 Lista de servidores

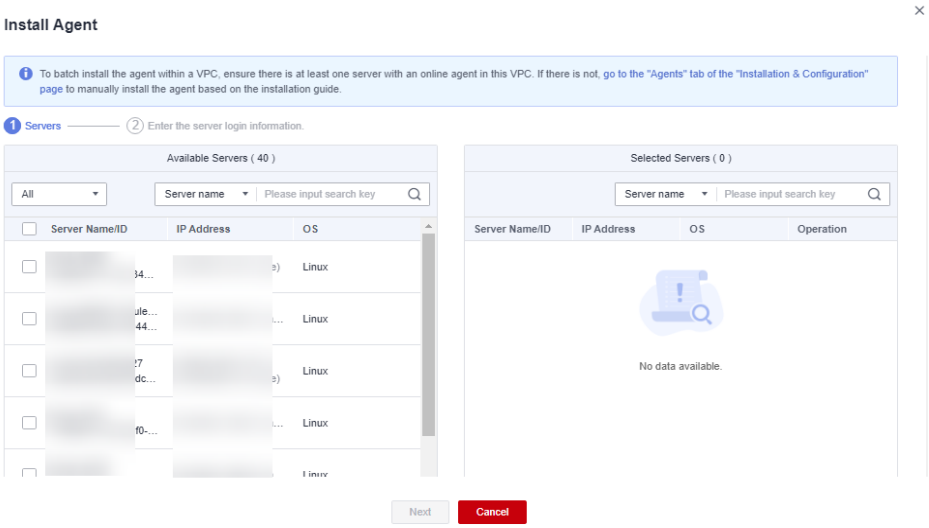


Passo 4 Clique em **Install Agent** na parte superior da página e selecione servidores de destino na página de diálogo exibida.

AVISO

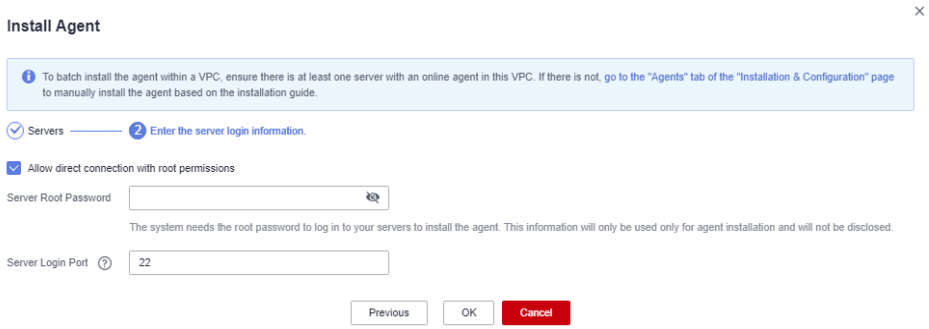
- Todos os servidores de destino devem estar no estado **Running**.
- Na VPC onde os servidores de destino estão localizados, pelo menos um servidor instalou o agente. Caso contrário, a instalação em lote falhará.
- Os servidores selecionados devem usar a mesma senha raiz e o mesmo número de porta. Caso contrário, a instalação em lote falhará.
- Os agentes podem ser instalados em até 50 servidores por vez.

Figura 3-53 Selecionar servidores



Passo 5 Clique em **Next**. Digite a senha raiz do servidor e a porta de logon do servidor.

Figura 3-54 Inserir informações do servidor



NOTA

A porta padrão do sistema é **22**. Para consultar a porta SSH do Linux, faça logon remotamente no servidor de destino e execute o seguinte comando no servidor de Linux:

```
cat /etc/ssh/sshd_config | grep Port
```

Passo 6 Clique em **OK**. Os agentes serão instalados automaticamente nos servidores selecionados.

NOTA

Os agentes serão instalados automaticamente nos servidores selecionados em sequência. Você pode escolher **Asset Management** > **Servers & Quota** e clicar na guia **Servers** para exibir o status do agente. Se o **Agent Status** de um servidor de destino for alterado para **Online**, você poderá ativar a proteção para o servidor.

----Fim

3.5 Gerenciamento de containers

3.5.1 Visualização dos clusters e as cotas de proteção

A página **Container Nodes** exibe a proteção, o nó e o status do Agente dos clusters no Cloud Container Engine (CCE), ajudando você a aprender o status de segurança dos clusters em tempo real.

Restrições

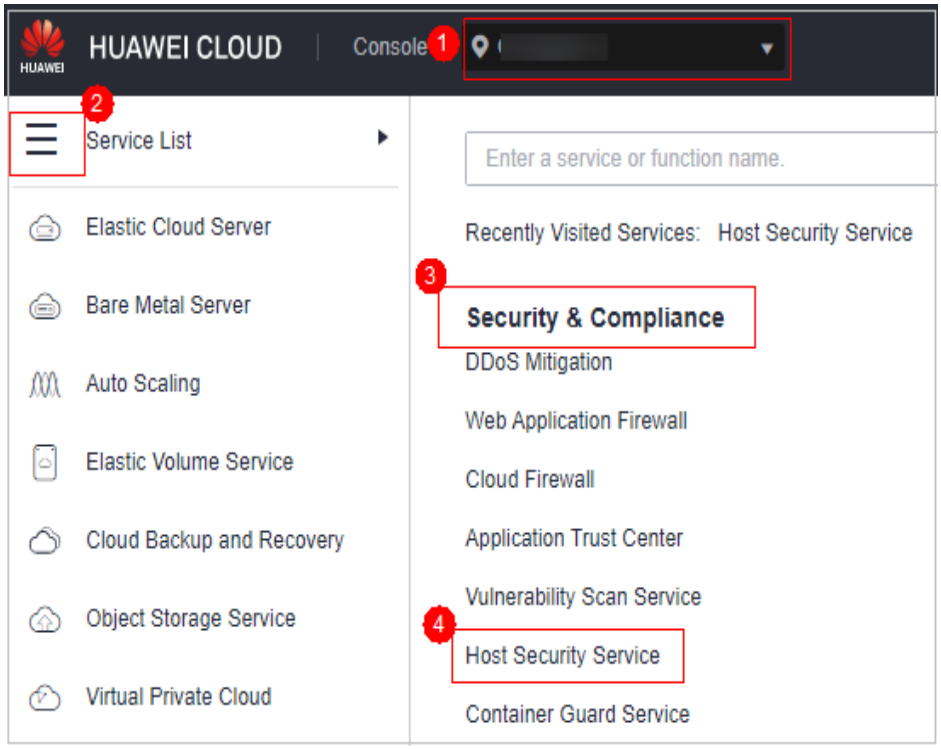
- Somente servidores do Linux são suportados.
- Os servidores que não estão protegidos pelas edições empresarial, premium, WTP ou de container do HSS não podem realizar operações relacionadas a container.

Verificação da lista de nós

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 3-55 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Asset Management** > **Containers & Quota**. Clique em **Container Nodes**.

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 Visualize o status de proteção do nó na página **Nodes**. Você pode obter os detalhes em **Tabela 3-9**.

Figura 3-56 Visualizar o status do nó

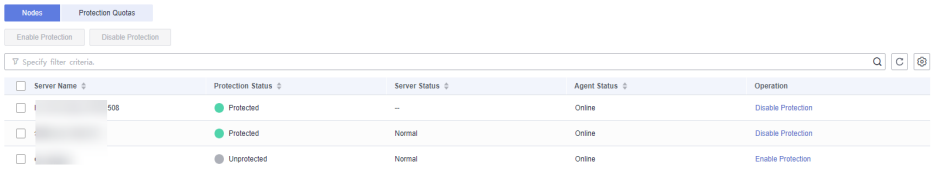


Tabela 3-9 Descrição do parâmetro

Parâmetro	Descrição
Server Name	Nome do servidor de destino
Protection Status	Status de proteção de um nó. As opções são as seguintes: ● Unprotected ● Protected ● Protection interrupted

Parâmetro	Descrição
Server Status	● Running ● Unavailable ● Normal
Agent Status	● Online ● Offline ● Not installed

----Fim

Visualização de cotas de proteção

Na página **Clusters & Quotas**, clique em **Protection Quotas** para visualizar os detalhes da cota.

Figura 3-57 Visualizar as cotas de proteção

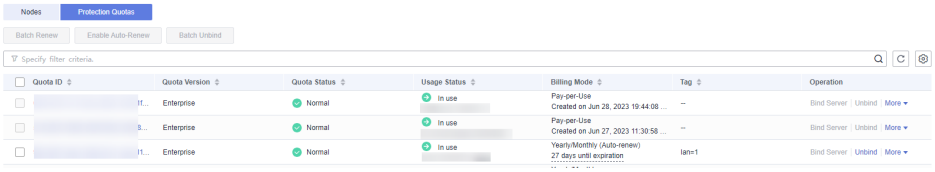


Tabela 3-10 Parâmetros de cota de container

Parâmetro	Descrição
Quota ID	ID da cota
Quota Version	Edição empresarial de segurança de containers
Quota Status	● **Normal**: a cota é normal. ● **Expired**: a cota expirou. Durante esse período, você ainda pode usar a cota. ● **Frozen**: a cota não protege mais seus servidores. Quando o período de congelamento expirar, a cota será permanentemente excluída.
Usage Status	● **In use**: a cota está sendo usada para um servidor. O nome do servidor é exibido abaixo do status. ● **Idle**: a cota não está em uso.
Billing Mode	● Yearly/Monthly ● Pay-per-use
Tag	Tag de categoria de recursos

- Clique nas áreas correspondentes na coluna **Operation** para renovar ou renovar automaticamente as cotas. Para obter detalhes, consulte **Como renovar minhas cotas do CGS?**
- Clique em **Unsubscribe** para cancelar a assinatura da cota do CGS. Para obter detalhes, consulte **Como cancelar a assinatura de uma cota do CGS?**

3.5.2 Ativação da proteção de segurança de containers

Você pode ativar a edição de segurança de container para seus containers.

Para ativar a proteção para um nó de container, você precisa alocar uma cota para o nó. Se a proteção for desativada ou o nó for excluído, a cota poderá ser alocada para outro nó.

Frequência de verificação

O HSS realiza uma verificação completa no início da manhã todos os dias.

Depois de habilitar a proteção do servidor, pode ver os resultados da análise após a verificação automática no início da manhã seguinte.

Pré-requisito

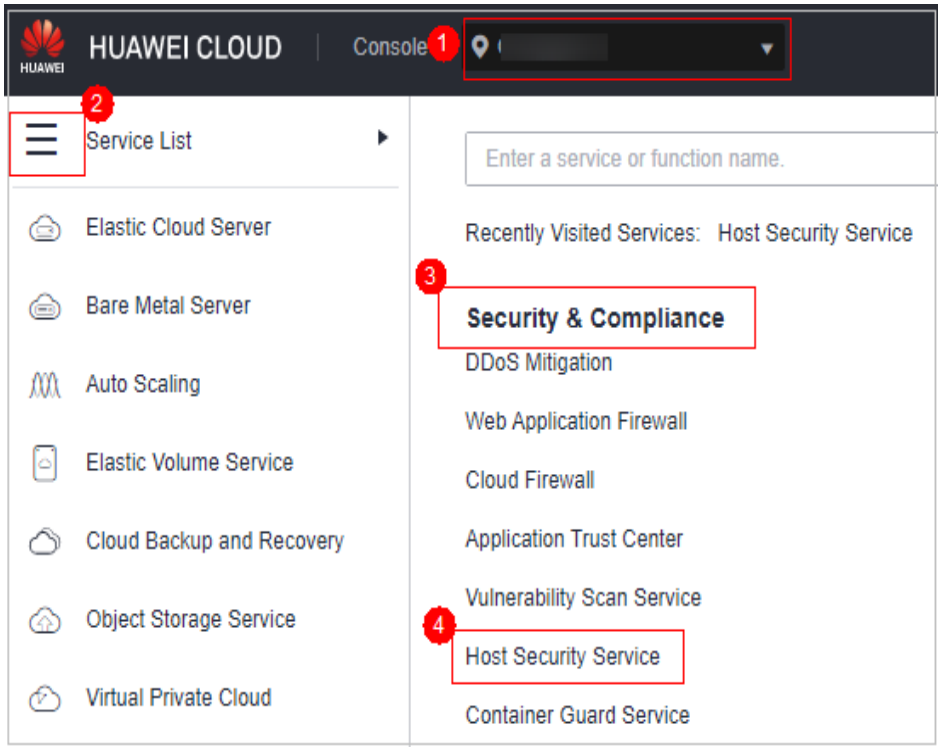
- O **Agent Status** de um servidor é **Online**. Para verificar o status, escolha **Host Security Service** > **Asset Management** > **Containers & Quota**.
- Você criou um nó no CCE.
- O **Protection Status** do nó é **Unprotected**.

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 3-58 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.

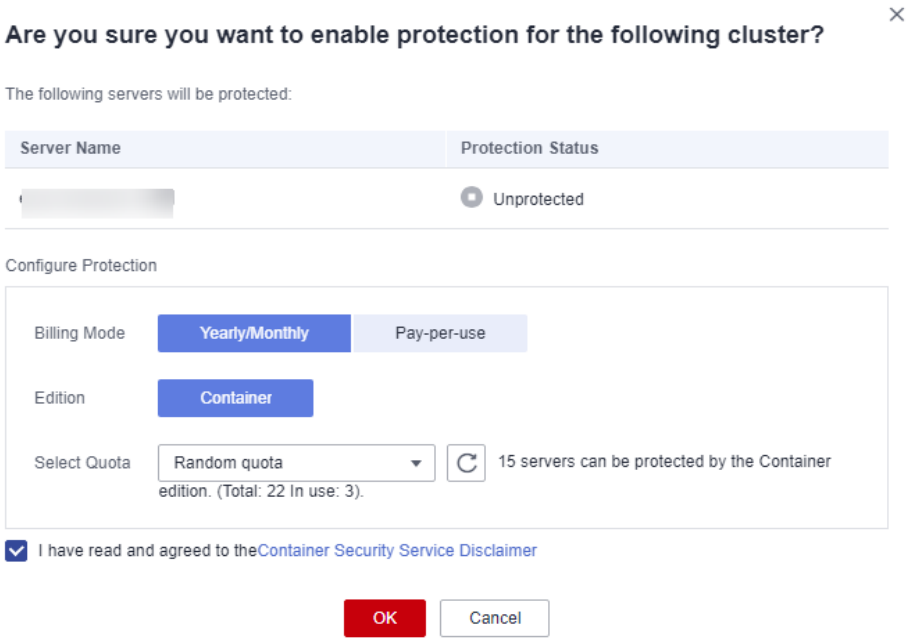
Passo 4 Ative a proteção para um ou vários servidores.

- **Ativar a proteção para um servidor**
  a. Na coluna **Operation** de um servidor, clique em **Enable Protection**.
  b. Na caixa de diálogo exibida, confirme as informações e selecione um modo de cobrança.

  NOTA

  - Para ativar a proteção no modo de cobrança anual/mensal, verifique se você comprou cotas suficientes. Para obter detalhes, consulte **Compra de uma cota de edição de container**. Você também pode ativar a proteção no modo de pagamento por uso sem usar cotas.
  - Uma cota de segurança de container protege um nó de cluster.

Figura 3-59 Confirmar informações de edição de container

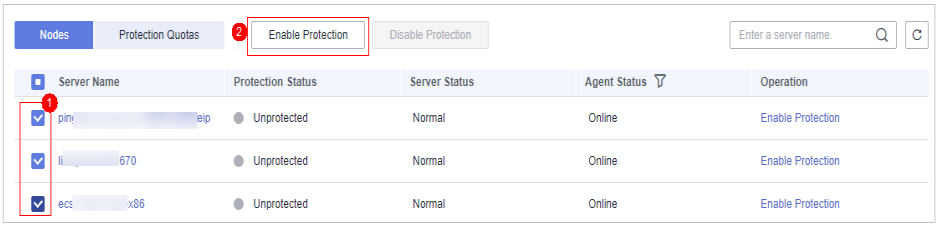


c. Confirme as informações, leia o Aviso de isenção de responsabilidade do Container Guard Service, selecione **I have read and agreed to the Container Guard Service Disclaimer** e clique em **OK**. Se o **Protection Status** na lista de containers mudar para **Protected**, isso indica que a proteção foi ativada.

- **Ativar a proteção em lotes**

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

  Figura 3-60 Selecionar servidores

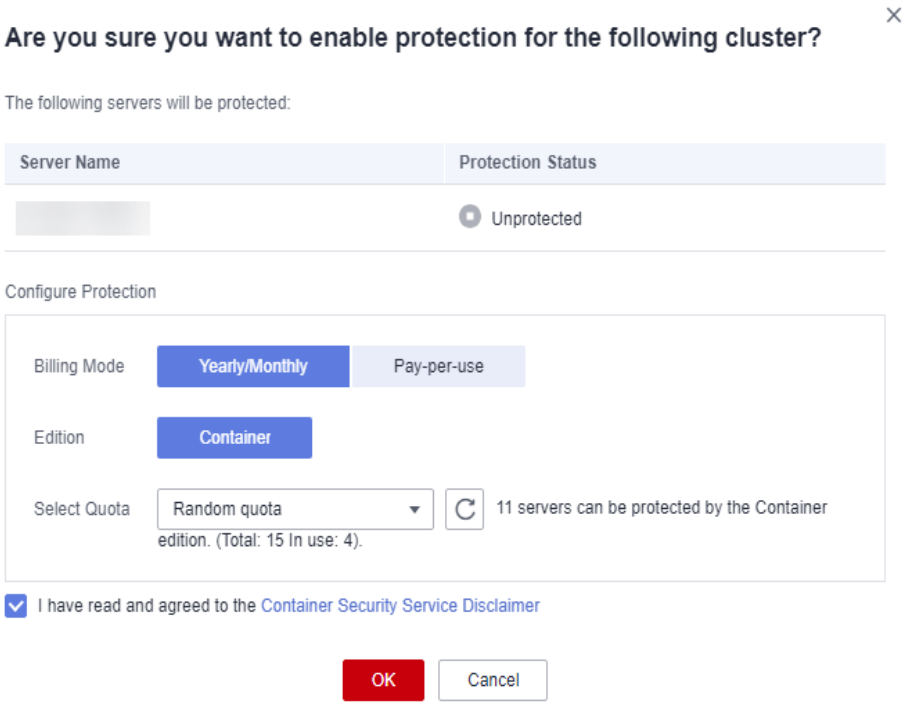
  

  b. Na caixa de diálogo exibida, confirme as informações e selecione um modo de cobrança.

  NOTA

  - Para ativar a proteção no modo de cobrança anual/mensal, verifique se você comprou cotas suficientes. Para obter detalhes, consulte **Compra de uma cota de edição de container**. Você também pode ativar a proteção no modo de pagamento por uso sem usar cotas.
  - Uma cota de segurança de container protege um nó de cluster.

Figura 3-61 Confirmar informações de edição de container sobre vários servidores



c. Confirme as informações, leia o Aviso de isenção de responsabilidade do Container Guard Service, selecione **I have read and agreed to the Container Guard Service Disclaimer** e clique em **OK**. Se o **Protection Status** na lista de containers mudar para **Protected**, isso indica que a proteção foi ativada.

NOTA

A prevenção contra ransomware é ativada automaticamente com a edição de container. Para aprimorar a prevenção contra ransomware, você pode configurar diretórios protegidos e ativar a proteção dinâmica de honeypot, conforme necessário. Você também é aconselhado a ativar o backup para que você possa restaurar os dados no caso de um ataque de ransomware para minimizar as perdas. Para obter detalhes, consulte **Modificação de uma política de proteção** e **Habilitação de backup de ransomware**.

----Fim

Procedimento de acompanhamento

A edição de container suporta proteção contra ransomware. Para obter detalhes sobre como ativar a proteção contra ransomware para seus servidores na edição de container, consulte **Ativação de proteção contra ransomware**.

3.5.3 Desativação da proteção de segurança de container

Você pode desativar a edição de container para um servidor. Uma cota que foi desvinculada de um servidor pode ser vinculada a outro.

Antes de começar

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

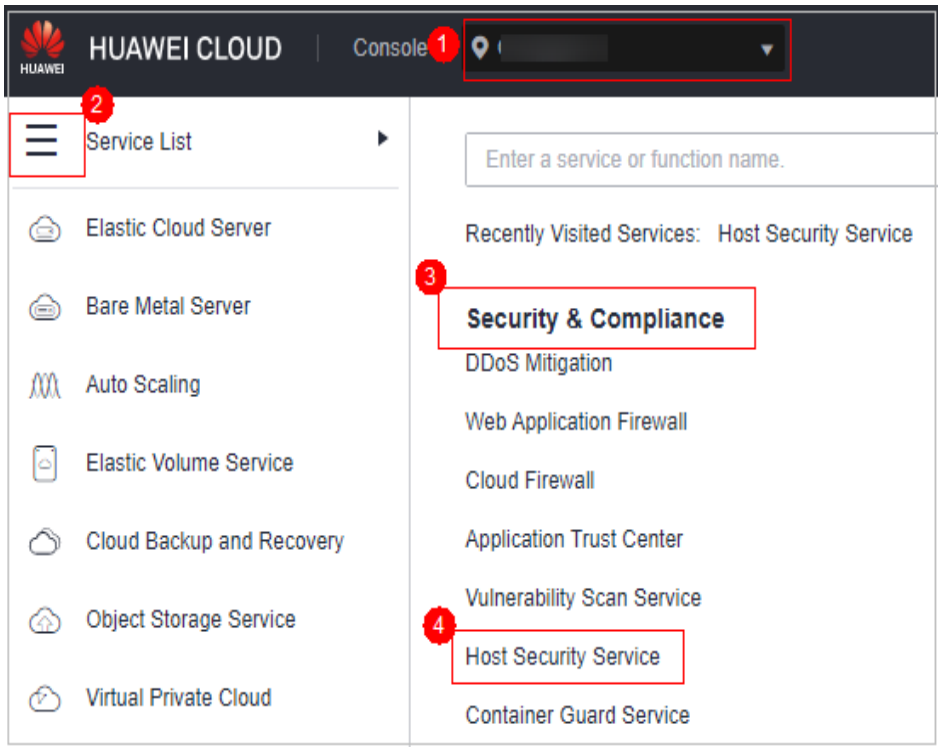
- Para cancelar a assinatura da cota de pagamento por uso da edição de container, você só precisa desativar a proteção.

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 3-62 Acessar o HSS



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

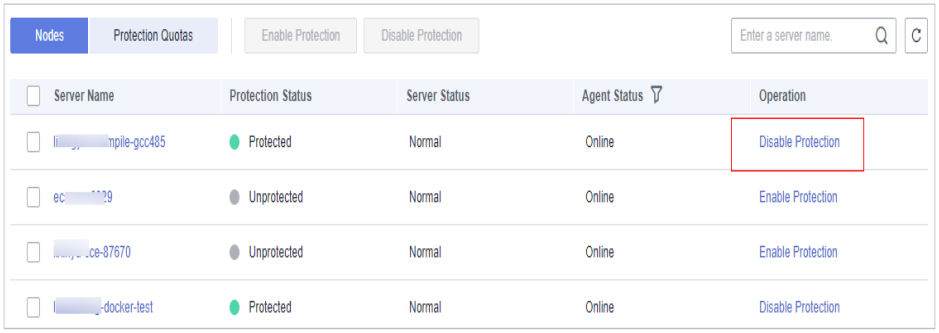
NOTA

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.

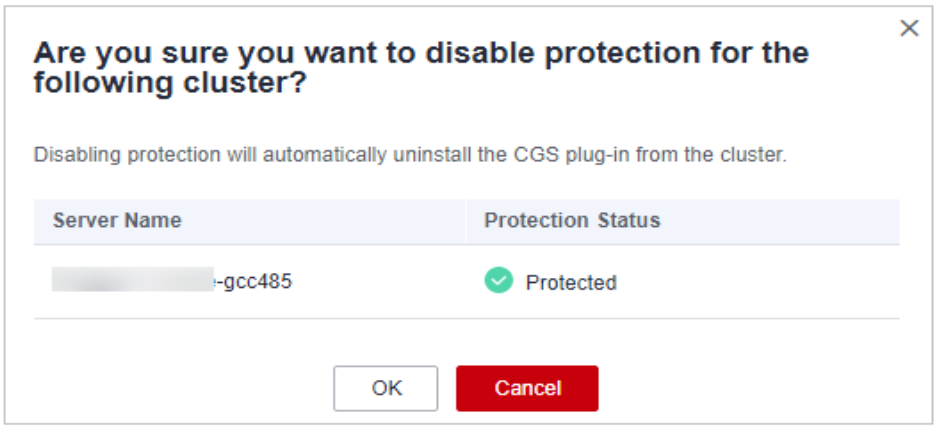
- **Desativar a proteção para um servidor**
  a. Na lista de nós, clique em **Disable Protection** na coluna **Operation** de um servidor.

Figura 3-63 Desativar a proteção do container



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

Figura 3-64 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.

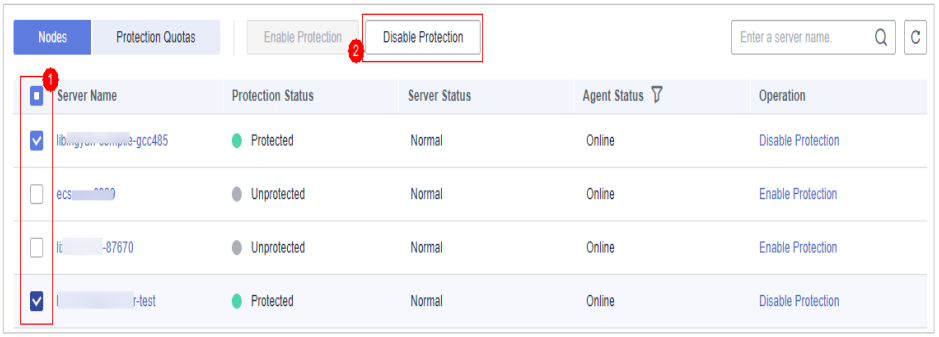
CUIDADO

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

- **Desativar a proteção em lotes**

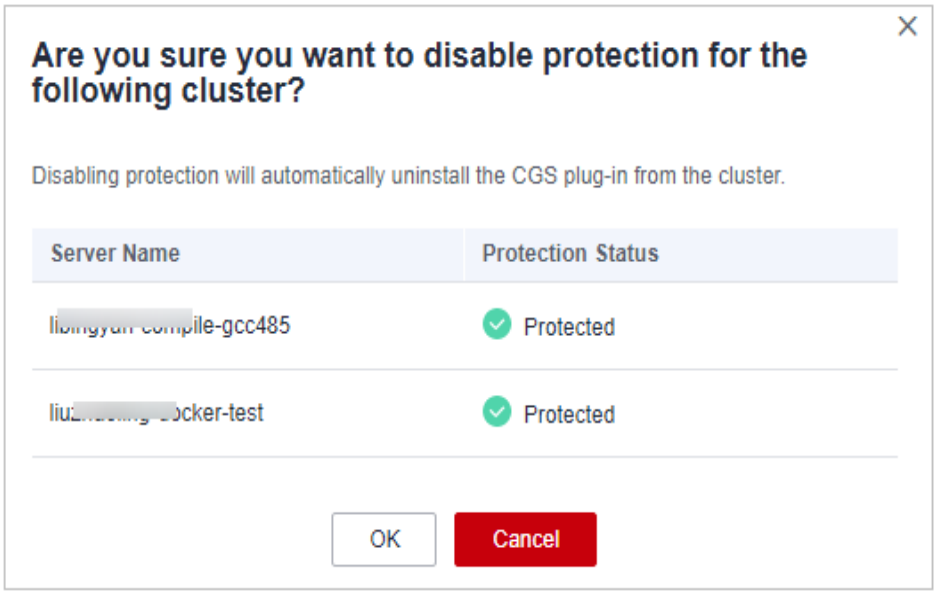
a. Na lista de nós, selecione servidores e clique em **Disable Protection** acima da lista.

Figura 3-65 Selecionar servidores



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

Figura 3-66 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

3.5.4 Imagens do container

3.5.4.1 Imagens locais

Você pode verificar manualmente imagens locais em busca de vulnerabilidades e informações de software e fornece relatórios de verificação. Esta seção descreve como executar verificações de segurança em imagens locais e visualizar relatórios de verificação.

Restrições

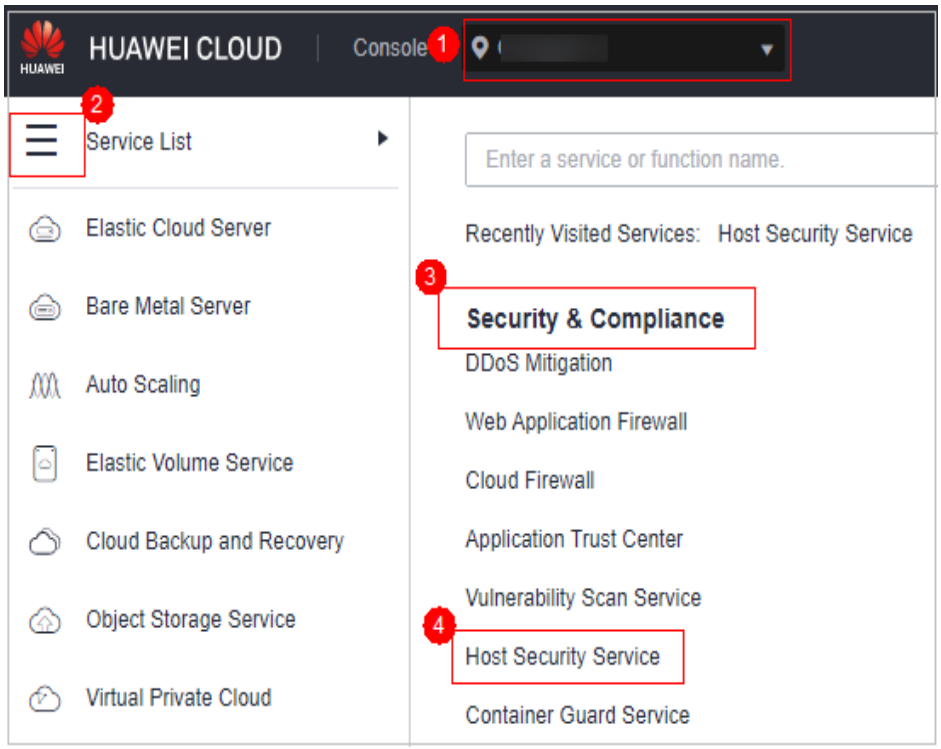
- Somente a edição de container do HSS suporta essa função. Para obter detalhes sobre como comprar e atualizar o HSS, consulte **Compra de uma cota de HSS** e **Atualização de sua edição**.
- Somente as imagens locais do mecanismo Docker podem ser relatadas ao console do HSS.
- As verificações de segurança podem ser executadas apenas em imagens do Linux.

Visualizar imagens locais

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 3-67 Acessar o HSS



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

Passo 4 Clique na guia **Container Images** e clique em **Local image**.

Você pode visualizar o nome, a versão, o tipo e os riscos de segurança de uma imagem.

- Visualização de informações sobre servidores vinculados a uma imagem

  Localize a linha que contém a imagem de destino e clique no número na coluna **Associated Servers**. A página **Associated Servers** é exibida. Você pode visualizar detalhes sobre os servidores vinculados à imagem.

- Visualização de informações sobre containers vinculados a uma imagem

  Localize a linha que contém a imagem de destino e clique no número na coluna **Associated Containers**. A página **Associated Containers** é exibida. Você pode visualizar detalhes sobre os containers vinculados à imagem.

- Visualização de informações sobre componentes de imagem

  Localize a linha que contém a imagem de destino e clique no número na coluna **Components**. A página **Components** é exibida. Você pode visualizar detalhes sobre os componentes da imagem.

----Fim

Verificações de segurança de imagem local

Os itens de verificação de segurança são os seguintes:

Item de verificação	Descrição
Vulnerabilidade	Detecta vulnerabilidades em imagens.
Software instalado	Coleta informações de software em uma imagem.

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e clique em **Local image**.

Passo 4 Executa uma verificação de segurança para uma única imagem ou várias imagens.

- Verificação de segurança de imagem única

  Na coluna **Operation** da imagem de destino, clique em **Scan** para executar a verificação de segurança.

- Verificação de segurança de imagens em lote

  Selecione todas as imagens de destino e clique em **Scan** acima da lista de imagens para executar a verificação de segurança para várias imagens de destino.

- Verificação completa de segurança de imagem

  Clique em **Scan All** acima da lista de imagens para executar uma verificação de segurança para todas as imagens.

Passo 5 A verificação de segurança da imagem está concluída, quando o **Scan Status** é alterado para **Completed** e **Latest Scan Completed** mostra o tempo de execução da tarefa mais recente.

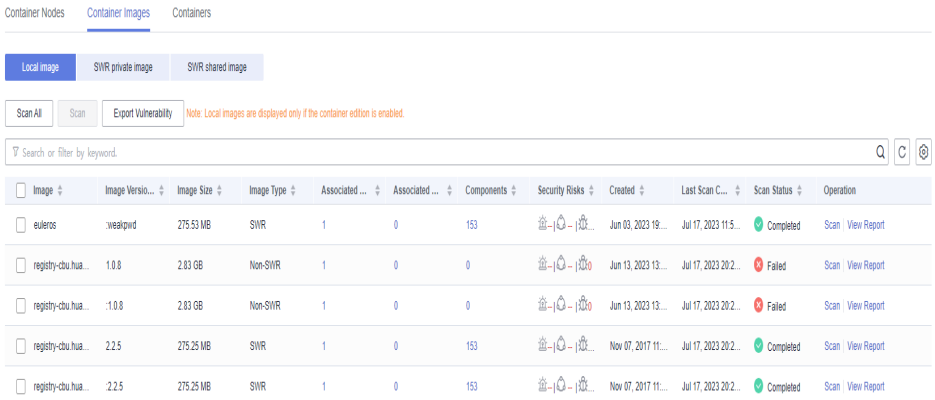
----Fim

Visualização de relatórios de vulnerabilidade de imagem local e informações de software

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação à esquerda, escolha **Asset Management** > **Containers & Quota**. Clique na guia **Container Images** e clique em **Local image** para exibir o resultado da verificação da imagem.

Figura 3-68 Visualização dos resultados da verificação de imagens locais



----Fim

Exportação de relatórios de vulnerabilidade de imagem local

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e clique em **Local image**.

Passo 4 Clique em **Export Vulnerability** acima da lista de imagens.

Se quiser exportar o relatório de vulnerabilidades de uma imagem especificada, selecione o tipo de imagem na caixa de pesquisa e clique em **Export Vulnerability**.

----Fim

3.5.4.2 Gerenciamento de imagens privadas do SWR

As imagens no repositório de imagens privadas vêm de imagens do SWR. Você pode fazer verificações manuais e verificar relatórios sobre conformidade de software, informações de imagem de base, vulnerabilidades, arquivos maliciosos, informações de software, informações de arquivos, verificação de linha de base e informações confidenciais.

Restrições

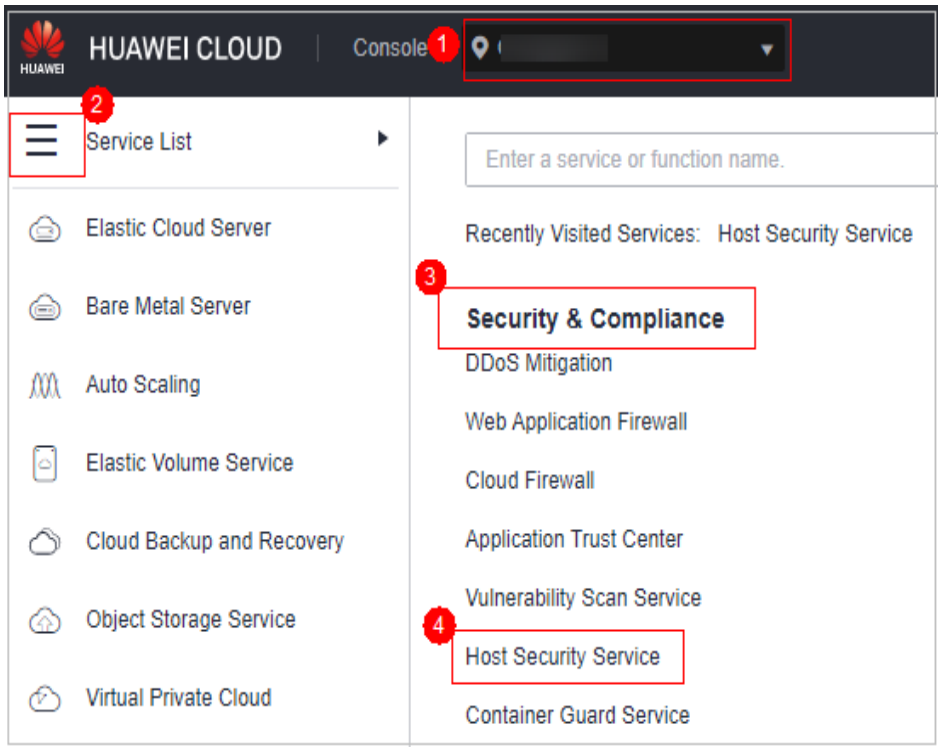
- Somente a edição de container do HSS suporta essa função. Para obter detalhes sobre como comprar e atualizar o HSS, consulte **Compra de uma cota de HSS** e **Atualização de sua edição**.
- As verificações de segurança podem ser executadas apenas em imagens do Linux.

Visualizar imagens privadas

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 3-69 Acessar o HSS

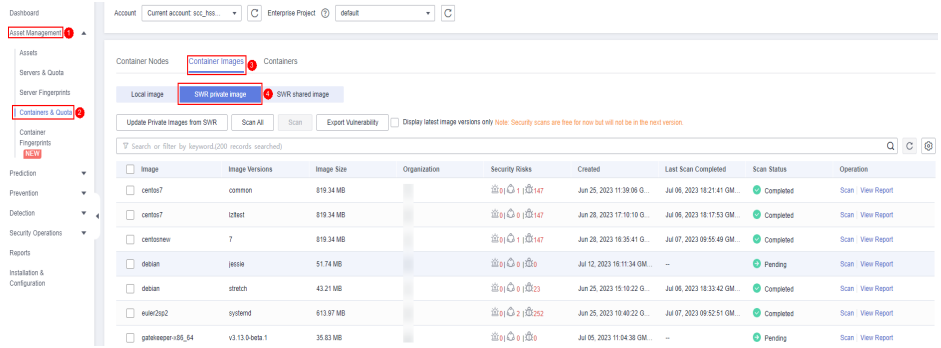


Passo 3 No painel de navegação, escolha **Asset Management** > **Container & Quota**. Na página exibida, clique na guia **Container Images** e clique em **SWR private image**.

NOTA

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

Figura 3-70 Acessar a lista de imagens privadas



Passo 4 Você pode clicar em **Update Private Images from SWR** para atualizar imagens próprias do SWR.

NOTA

As imagens podem ser sincronizadas somente após serem autorizadas pelo SWR. Para obter detalhes, consulte **Métodos de autorização de SWR**.

----Fim

Verificar uma imagem privada

Você pode escolher todas as imagens, várias imagens ou uma única imagem e iniciar manualmente uma verificação. A duração de uma verificação de segurança depende do tamanho da imagem verificada. Geralmente, a verificação de uma imagem leva menos de 3 minutos. Depois que a verificação for concluída, clique em **View Report** para verificar o relatório.

Os itens de verificação de imagens privadas no SWR são os seguintes:

Item de verificação	Descrição
Vulnerabilidade	Detecta vulnerabilidades em imagens.
Arquivo malicioso	Detecta arquivos maliciosos em imagens.
Informações sobre o software	Coleta informações de software em uma imagem.
Informações do arquivo	Coleta informações de arquivo em uma imagem.
Configuração insegura	● Verificação de configuração: – Verifica as configurações de imagens do CentOS 7, Debian 10, EulerOS e Ubuntu16. – Verifica as configurações de SSH. ● Verificação de senha fraca: detecta senhas fracas em imagens. ● Verificação de complexidade de senha: detecta políticas de complexidade de senha inseguras em imagens.

Item de verificação	Descrição
Informações confidenciais	Detecta arquivos que contêm informações confidenciais em imagens. ● Os caminhos que não são verificados por padrão são os seguintes: – /usr/* – /lib/* – /lib32/* – /bin/* – /sbin/* – /var/lib/* – /var/log/* – */node_modules/*/*.md – */node_modules/*/test/* – */service/iam/examples_test.go – */grafana/public/build/*.js **NOTA** Na guia **View Report** > **Sensitive Information**, clique em **Configure Sensitive File Path** para definir o caminho do Linux do arquivo que não precisa ser verificado. Um máximo de 20 caminhos podem ser adicionados. ● Nenhuma verificação é executada nos seguintes cenários: – O tamanho do arquivo é maior que 20 MB. – O tipo de arquivo pode ser binário, processo comum ou geração automática.
Conformidade de software	Detecta softwares e ferramentas que não podem ser usados.
Informações básicas da imagem	Detecta imagens de serviço que não são criadas usando imagens de base.

Passo 1 Faça logon no console de gerenciamento do HSS.

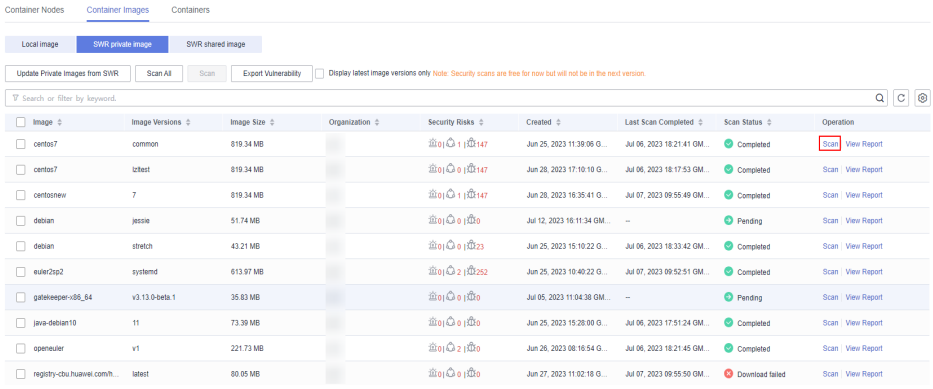
Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e selecione **SWR private image**. Na coluna **Operation** de uma imagem, clique em **Scan**.

NOTA

Imagens com várias arquiteturas não suportam verificação em lote ou verificação completa.

Figura 3-71 Verificação de segurança



Passo 4 Na caixa de diálogo exibida, clique em **OK** para iniciar o trabalho de verificação.

Passo 5 **Scanned** na coluna **Scan Status** indica que a verificação da imagem de destino foi concluída.

----Fim

Verificar o relatório de segurança de imagens privadas

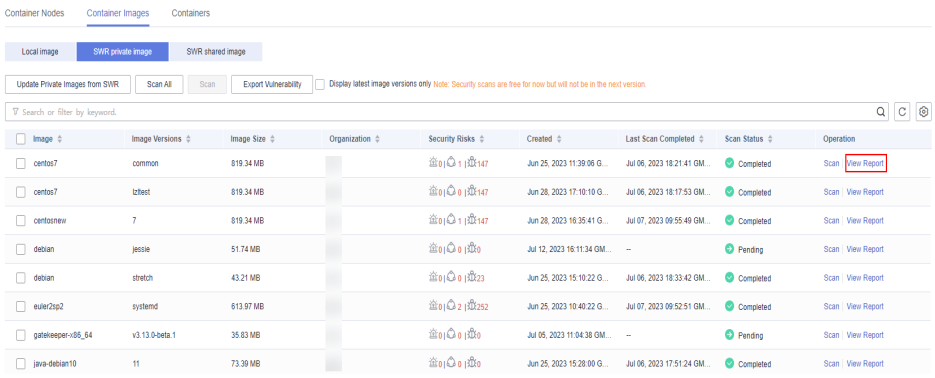
Após a conclusão da verificação, você poderá visualizar os relatórios de segurança.

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e selecione **SWR private image**. Na coluna **Operation** de uma imagem, clique em **View Report**.

Figura 3-72 Relatório de segurança



----Fim

Visualizar o relatório de arquivo malicioso de uma imagem privada

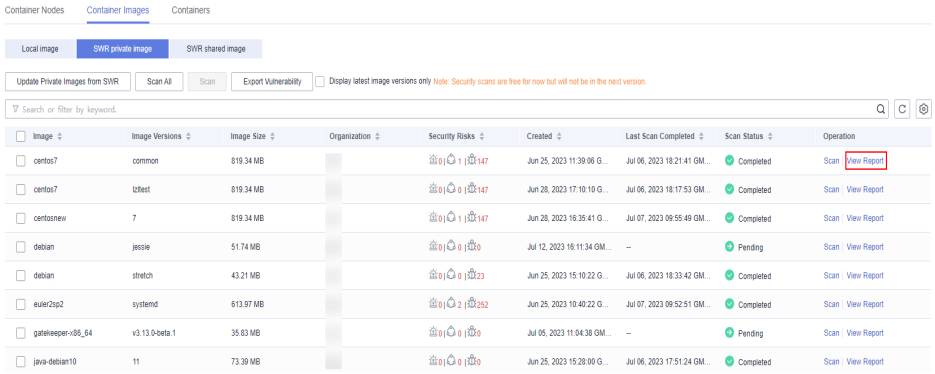
Depois que as imagens forem verificadas, você poderá visualizar arquivos maliciosos nelas. Esta seção descreve como visualizar arquivos maliciosos em uma versão de imagem.

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

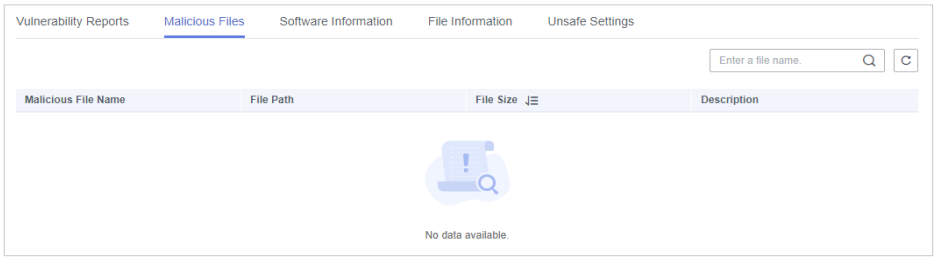
Passo 3 Clique na guia **Container Images** e selecione **SWR private image**. Na coluna **Operation** de uma imagem, clique em **View Report**.

Figura 3-73 Relatório de segurança



Passo 4 Clique em **Malicious Files** para visualizar arquivos maliciosos na imagem.

Figura 3-74 Arquivo malicioso em imagens privadas



----Fim

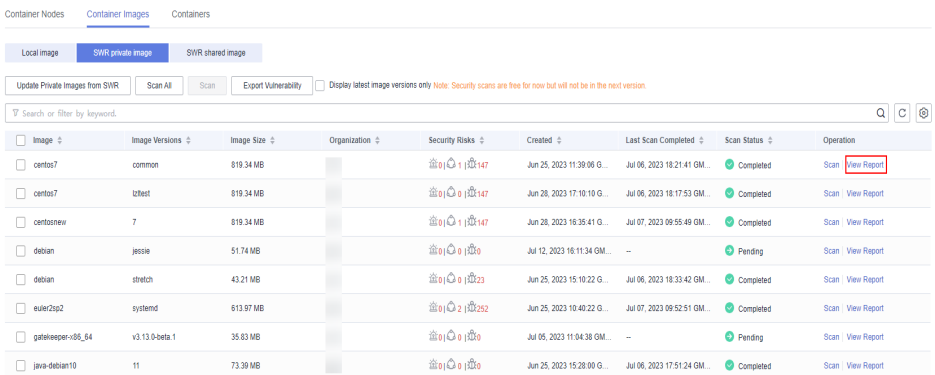
Visualizar informações de software sobre uma imagem privada

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

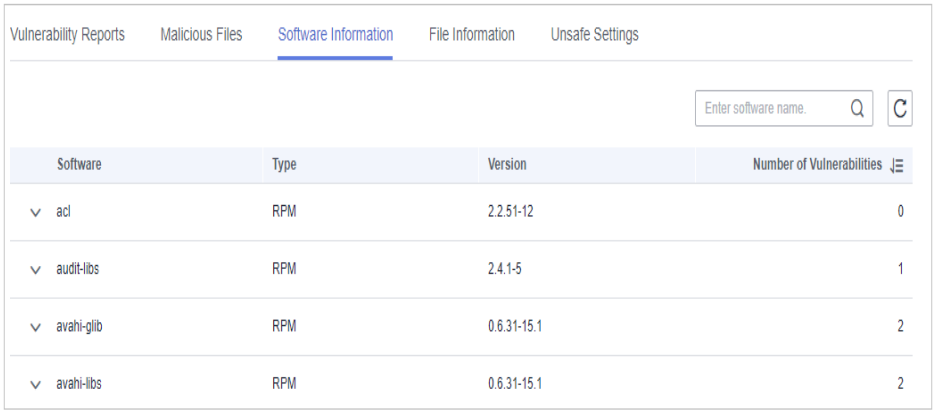
Passo 3 Clique na guia **Container Images** e selecione **SWR private image**. Na coluna **Operation** de uma imagem, clique em **View Report**.

Figura 3-75 Relatório de segurança



Passo 4 Clique em **Software Information** para visualizar o software contido na versão da imagem, o tipo de software e o número de vulnerabilidades no software.

Figura 3-76 Informações sobre o software



Passo 5 Clique em ao lado de um nome de software para exibir o nome da vulnerabilidade do software, a urgência de reparo e a solução.

----Fim

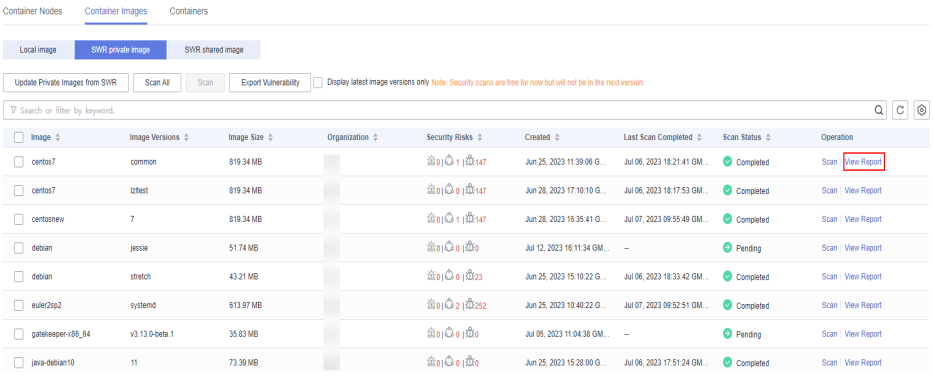
Visualizar informações do arquivo sobre uma imagem privada

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e selecione **SWR private image**. Na coluna **Operation** de uma imagem, clique em **View Report**.

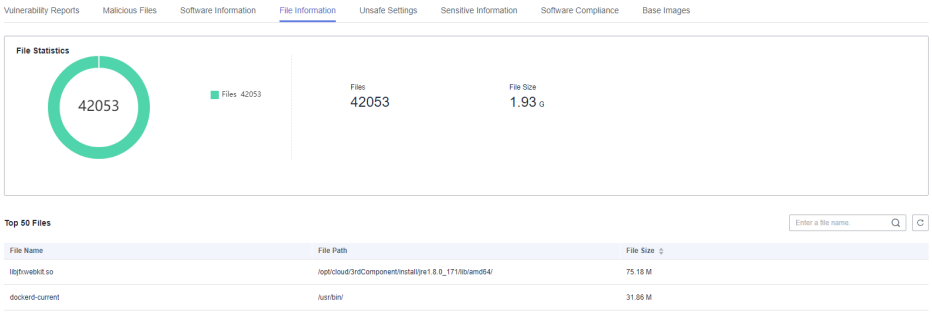
Figura 3-77 Relatório de segurança



Passo 4 Clique em **File Information** para exibir as informações do arquivo sobre a imagem.

Incluindo o número de arquivos, tamanho total do arquivo e detalhes sobre os 50 principais arquivos.

Figura 3-78 Informações do arquivo



----Fim

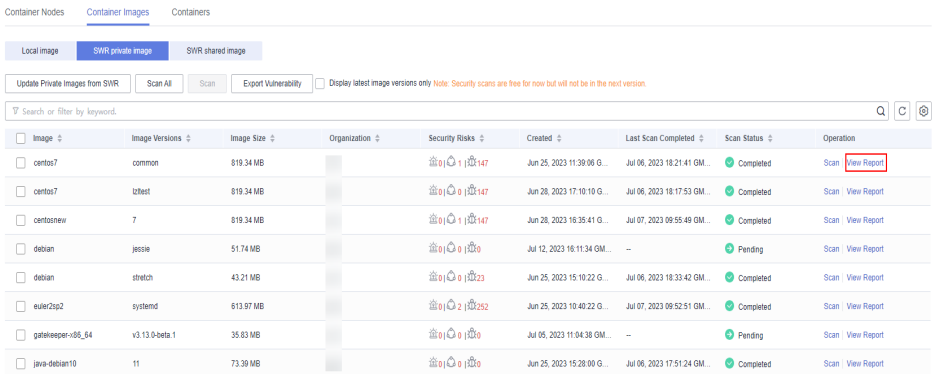
Visualizar as configurações inseguras de uma imagem privada

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e selecione **SWR private image**. Na coluna **Operation** de uma imagem, clique em **View Report**.

Figura 3-79 Relatório de segurança

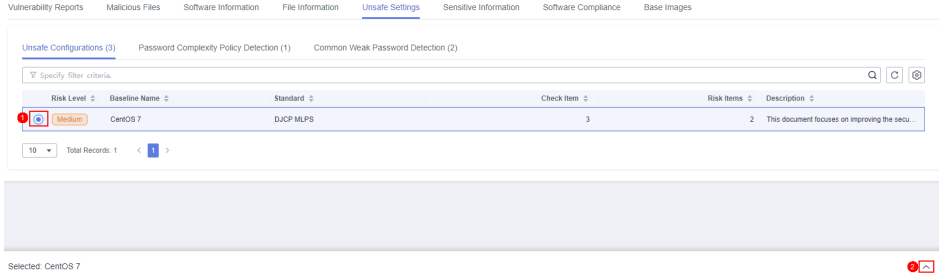


Passo 4 Selecione **Unsafe Settings** para exibir o relatório de verificação da linha de base.

Você pode visualizar as configurações inseguras, a detecção de política de complexidade de senha e os resultados comuns de detecção de senha fraca da imagem de destino.

- Visualizar configurações inseguras e sugestões de modificação
  a. Na página de guia **Unsafe Configurations**, selecione a linha de base de destino e clique em ^ .

Figura 3-80 Visualizar detalhes de configurações inseguras



b. Na coluna do item de detecção do item de detecção de destino, clique em **Description** para visualizar a descrição do item de detecção e as sugestões de modificação.

- Detecção de senha fraca comum

  a. Clique em **Common Weak Password Detection**.

  b. Configure senhas fracas e clique em **OK**.

----Fim

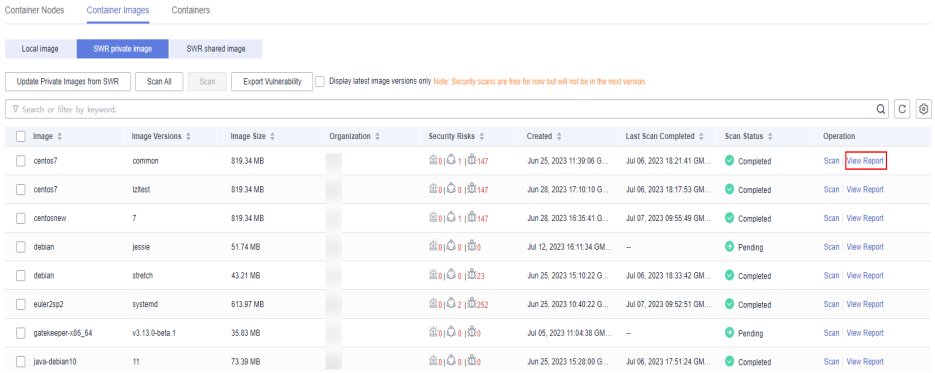
Visualizar o relatório de informações confidenciais de uma imagem privada

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e selecione **SWR private image**. Na coluna **Operation** de uma imagem, clique em **View Report**.

Figura 3-81 Relatório de segurança



Passo 4 Clique na guia **Sensitive Information** para exibir detalhes sobre informações de imagens confidenciais e ignorar alarmes de risco.

Passo 5 Clique em **Configure Sensitive File Path** para exibir e editar a lista branca de caminho de arquivo personalizado.

Figura 3-82 Editar a lista branca de arquivos confidenciais

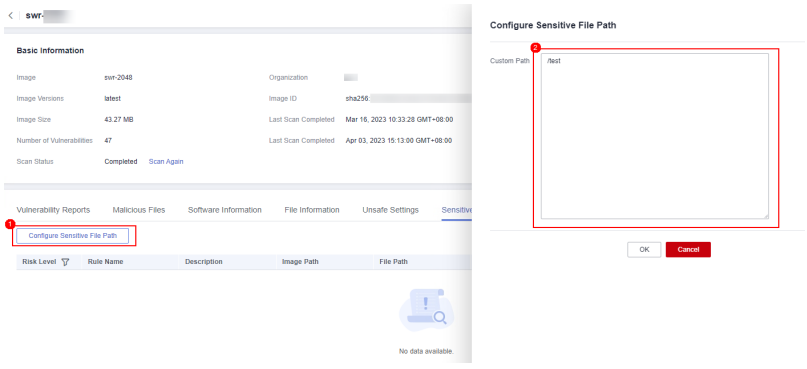


Tabela 3-11 Descrição do caminho personalizado

Item de especificação de caminho	Descrição	Exemplo de valor
SO	Somente Linux é suportado.	-
Requisito	Um máximo de 20 caminhos podem ser especificados. Um caminho ocupa uma linha.	/usr/ /lib/test.txt
Caminho de lista branca padrão	Os seguintes diretórios de lista branca ou formatos de arquivo são suportados por padrão e não precisam ser configurados: /usr/* /lib/* /lib32/* /bin/* /sbin/* /var/lib/* /var/log/* */node_modules/*/*.md */node_modules/*/test/* */service/iam/examples_test.go */grafana/public/build/*.js	-
Cenário sem verificação	● O tamanho do arquivo é maior que 20 MB. ● Os seguintes tipos de arquivos não são verificados: – Arquivos binários comuns – Arquivos de programas comuns – Arquivos gerados automaticamente	● jpg|png|gif|mov|avi|mpeg|pdf|mp4|mp3|svg|tar|gz|zip ● js|jar|java||md|cpp|cxx|scala|pl ● [0-9a-zA-Z_-]{32,64}

----Fim

Visualizar o relatório de conformidade de software sobre uma imagem privada

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e clique em **SWR private image**.

Passo 4 Na coluna **Operation** da imagem de destino, clique em **View Report**. A página de relatório de verificação de segurança é exibida.

Passo 5 Escolha **Software Compliance** para exibir o relatório.

Você pode visualizar o nome, o caminho e a camada de imagem do software não compatível.

----Fim

Visualizar o relatório de imagem base de uma imagem privada

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e clique em **SWR private image**.

Passo 4 Na coluna **Operation** da imagem de destino, clique em **View Report**. A página de relatório de verificação de segurança é exibida.

Passo 5 Clique na guia **Base Images** e visualize relatórios.

Você pode visualizar o nome, a versão e o caminho da camada de imagem de uma imagem de serviço que não é criada usando uma imagem base.

----Fim

Exportar relatórios de vulnerabilidade de imagem privada

NOTA

Os relatórios de vulnerabilidade não podem ser exportados para imagens com várias arquiteturas.

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e clique em **SWR private image**.

Passo 4 Clique em **Export Vulnerability** acima da lista de imagens.

Se quiser exportar o relatório de vulnerabilidades de uma imagem especificada, selecione o tipo de imagem na caixa de pesquisa e clique em **Export Vulnerability**.

----Fim

3.5.4.3 Gerenciamento de imagens compartilhadas do SWR

Você pode fazer verificações manuais e verificar relatórios sobre conformidade de software, informações de imagem de base, vulnerabilidades, arquivos maliciosos, informações de software, informações de arquivo, verificação de linha de base e informações confidenciais. Esta seção descreve como executar verificações de segurança em imagens compartilhadas do SWR e exibir relatórios de verificação.

Restrições

- Somente a edição de container do HSS suporta essa função. Para obter detalhes sobre como comprar e atualizar o HSS, consulte **Compra de uma cota de HSS** e **Atualização de sua edição**.

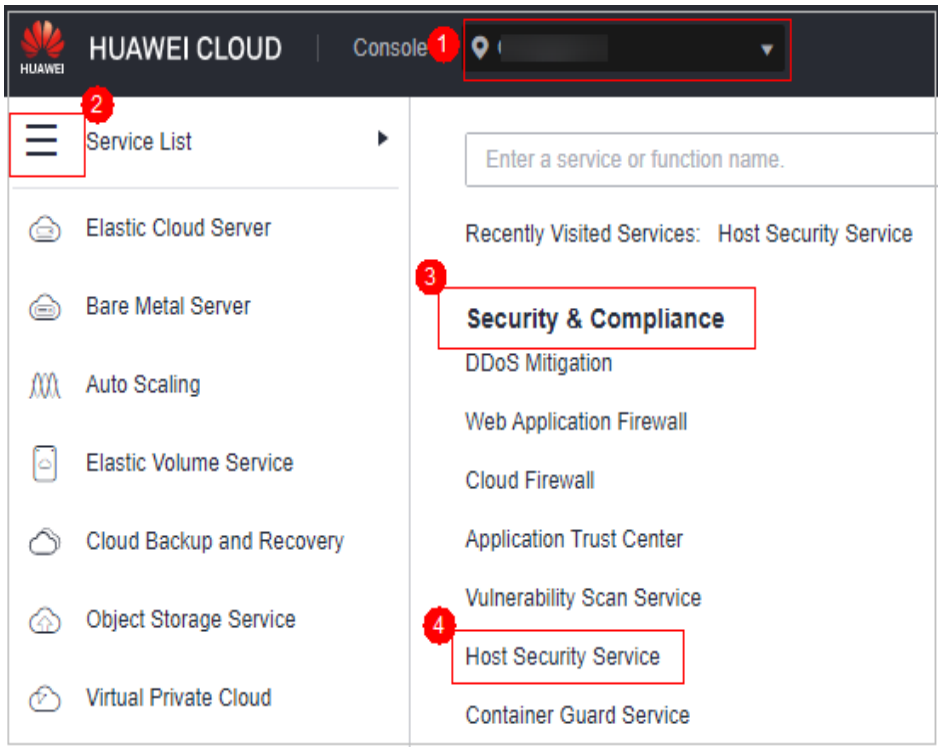
- As verificações de segurança podem ser executadas apenas em imagens do Linux.

Visualização de imagens compartilhadas do SWR

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 3-83 Acessar o HSS

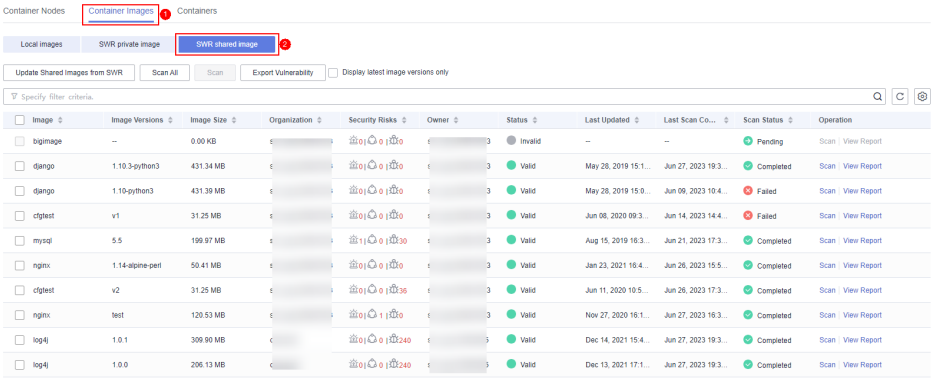


Passo 3 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 4 Clique na guia **Container Images** e clique em **SWR shared image** para exibir a lista de imagens compartilhadas.

Você pode visualizar a versão, o tamanho, a organização, os riscos de segurança e o proprietário de uma imagem compartilhada.

Figura 3-84 Visualização de imagens compartilhadas



- Atualizar uma imagem compartilhada

  Clique em **Update Shared Images from SWR** para atualizar a lista de imagens compartilhadas.
- Filtrar imagens da versão mais recente

  Se você selecionar **Display latest image versions only**, poderá filtrar as imagens mais recentes de todas as imagens.

----Fim

Verificação de segurança de imagem compartilhada

Você pode verificar manualmente uma imagem compartilhada do SWR no estado **Valid**. Os itens de verificação são os seguintes:

Item de verificação	Descrição
Vulnerabilidade	Detecta vulnerabilidades em imagens.
Arquivo malicioso	Detecta arquivos maliciosos em imagens.
Informações sobre o software	Coleta informações de software em uma imagem.
Informações do arquivo	Coleta informações de arquivo em uma imagem.
Configuração insegura	• Verificação de configuração: – Verifica as configurações de imagens do CentOS 7, Debian 10, EulerOS e Ubuntu16. – Verifica as configurações de SSH. • Verificação de senha fraca: detecta senhas fracas em imagens. • Verificação de complexidade de senha: detecta políticas de complexidade de senha inseguras em imagens.

Item de verificação	Descrição
Informações confidenciais	Detecta arquivos que contêm informações confidenciais em imagens. ● Os caminhos que não são verificados por padrão são os seguintes: – /usr/* – /lib/* – /lib32/* – /bin/* – /sbin/* – /var/lib/* – /var/log/* – */node_modules/*/*.md – */node_modules/*/test/* – */service/iam/examples_test.go – */grafana/public/build/*.js **NOTA** Na guia **View Report** > **Sensitive Information**, clique em **Configure Sensitive File Path** para definir o caminho do Linux do arquivo que não precisa ser verificado. Um máximo de 20 caminhos podem ser adicionados. ● Nenhuma verificação é executada nos seguintes cenários: – O tamanho do arquivo é maior que 20 MB. – O tipo de arquivo pode ser binário, processo comum ou geração automática.
Conformidade de software	Detecta softwares e ferramentas que não podem ser usados.
Informações básicas da imagem	Detecta imagens de serviço que não são criadas usando imagens de base.

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e clique em **SWR shared image**.

Passo 4 Execute uma verificação de segurança para uma única imagem ou várias imagens.

NOTA

- Você pode executar uma verificação de segurança somente quando o status for **Valid**.
- Imagens com várias arquiteturas não suportam verificação em lote ou verificação completa.

- Verificação de segurança de imagem única

  Na coluna **Operation** da imagem de destino, clique em **Scan** para executar a verificação de segurança.

- Verificação de segurança de imagens em lote

  Selecione todas as imagens de destino e clique em **Scan** acima da lista de imagens para executar a verificação de segurança para várias imagens de destino.

- Verificação completa de segurança da imagem

  Clique em **Scan All** acima da lista de imagens para executar uma verificação de segurança para todas as imagens.

Passo 5 A verificação de segurança da imagem está concluída, quando o **Scan Status** é alterado para **Completed** e **Latest Scan Completed** mostra o tempo de execução da tarefa mais recente.

----Fim

Visualização do relatório de verificação de vulnerabilidade de imagem compartilhada do SWR

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e clique em **SWR shared image**.

Passo 4 Na coluna **Operation** da imagem de destino, clique em **View Report**. A página de relatório de verificação de segurança é exibida.

Passo 5 Escolha **Vulnerability Reports** para exibir o relatório de vulnerabilidades.

- Visualizar detalhes de uma vulnerabilidade

  Clique no nome da vulnerabilidade para acessar a página de detalhes da vulnerabilidade e visualizar as informações básicas e as imagens afetadas.

- Visualizar o **CVE ID**, **CVSS Score** e **Disclosed Time** de uma vulnerabilidade

  Clique em na frente do nome da vulnerabilidade de destino para exibir o **CVE ID**, **CVSS Score** e **Disclosed Time**.

- Visualizar soluções de vulnerabilidade

  Na coluna **Operation** da linha que contém a vulnerabilidade de destino, clique em **Solution** para exibir os detalhes da solução de vulnerabilidade.

----Fim

Visualização do relatório de arquivos maliciosos de imagens compartilhadas do SWR

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e clique em **SWR shared image**.

Passo 4 Na coluna **Operation** da imagem de destino, clique em **View Report**. A página de relatório de verificação de segurança é exibida.

Passo 5 Selecione **Malicious Files** para exibir o relatório de arquivos maliciosos.

Você pode visualizar o nome, o caminho, o tamanho e a descrição do arquivo malicioso na imagem de destino.

----Fim

Visualização do relatório de informações de software de imagem compartilhada do SWR

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e clique em **SWR shared image**.

Passo 4 Na coluna **Operation** da imagem de destino, clique em **View Report**. A página de relatório de verificação de segurança é exibida.

Passo 5 Escolha **Software Information** para exibir o relatório.

Você pode visualizar o nome, o tipo, a versão e o número de vulnerabilidades do software na imagem.

----Fim

Visualização do relatório de informações do arquivo de imagem compartilhada do SWR

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e clique em **SWR shared image**.

Passo 4 Na coluna **Operation** da imagem de destino, clique em **View Report**. A página de relatório de verificação de segurança é exibida.

Passo 5 Escolha **File Information** para exibir o relatório.

Você pode visualizar o número de arquivos na imagem de destino, o tamanho total do arquivo e os detalhes sobre os 50 principais arquivos em tamanho.

----Fim

Visualização do relatório de verificação de linha de base de imagem compartilhada do SWR

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e clique em **SWR shared image**.

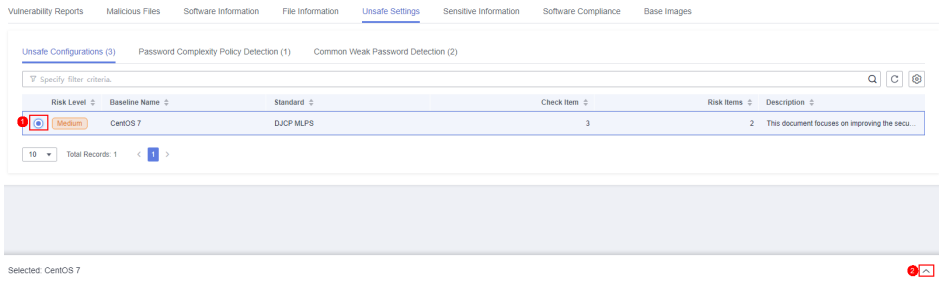
Passo 4 Na coluna **Operation** da imagem de destino, clique em **View Report**. A página de relatório de verificação de segurança é exibida.

Passo 5 Selecione **Unsafe Settings** para exibir o relatório de verificação da linha de base.

Você pode visualizar as configurações inseguras, a detecção de política de complexidade de senha e os resultados comuns de detecção de senha fraca da imagem de destino.

- Visualizar configurações inseguras e sugestões de modificação
  a. Na página de guia **Unsafe Configurations**, selecione a linha de base de destino e clique em .

  Figura 3-85 Visualizar detalhes de configurações inseguras

  b. Na coluna do item de detecção do item de detecção de destino, clique em **Description** para visualizar a descrição do item de detecção e as sugestões de modificação.
- Detecção de senha fraca comum
  a. Clique em **Common Weak Password Detection**.
  b. Configure senhas fracas e clique em **OK**.

----Fim

Visualização do relatório de informações confidenciais de imagem compartilhada do SWR

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e clique em **SWR shared image**.

Passo 4 Na coluna **Operation** da imagem de destino, clique em **View Report**. A página de relatório de verificação de segurança é exibida.

Passo 5 Clique na guia **Sensitive Information** para exibir o relatório.

Você pode visualizar o caminho, as informações confidenciais e o nível de risco do arquivo que contém informações confidenciais na imagem de destino.

- Prompt para ignorar informações confidenciais

  Na coluna **Operation** do arquivo de informações confidenciais de destino, clique em **Ignore** para ignorar as informações confidenciais que você considera seguras.
- Configurar o caminho do arquivo confidencial
  a. Clique em **Configure Sensitive File Path**. A página de gerenciamento de caminho de arquivo é exibida à direita.
  b. Na caixa de diálogo exibida, defina o caminho do Linux do arquivo que não precisa ser verificado e clique em **OK**.

Um máximo de 20 caminhos podem ser especificados. Um caminho ocupa uma linha.

----Fim

Visualização do relatório de conformidade do software de imagem compartilhada do SWR

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e clique em **SWR shared image**.

Passo 4 Na coluna **Operation** da imagem de destino, clique em **View Report**. A página de relatório de verificação de segurança é exibida.

Passo 5 Escolha **Software Compliance** para exibir o relatório.

Você pode visualizar o nome, o caminho e a camada de imagem do software não compatível.

----Fim

Visualização do relatório de informações sobre imagens de base de imagens compartilhadas do SWR

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e clique em **SWR shared image**.

Passo 4 Na coluna **Operation** da imagem de destino, clique em **View Report**. A página de relatório de verificação de segurança é exibida.

Passo 5 Escolha **Base Images** para exibir o relatório.

Você pode visualizar o nome, a versão e o caminho da camada de imagem de uma imagem de serviço que não é criada usando uma imagem de base.

----Fim

Exportação do relatório de vulnerabilidades de imagem compartilhada do SWR

NOTA

Os relatórios de vulnerabilidades não podem ser exportados para imagens de várias arquiteturas.

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Asset Management** > **Containers & Quota**.

Passo 3 Clique na guia **Container Images** e clique em **SWR shared image**.

Passo 4 Clique em **Export Vulnerability** acima da lista de imagens.

Se quiser exportar o relatório de vulnerabilidades de uma imagem especificada, selecione o tipo de imagem na caixa de pesquisa e clique em **Export Vulnerability**.

----Fim

3.5.5 Visualização de informações do container

Você pode visualizar as informações do container na página **Containers** para saber mais sobre o status do container, o cluster e os riscos. Esta seção descreve como visualizar informações de container.

Restrições

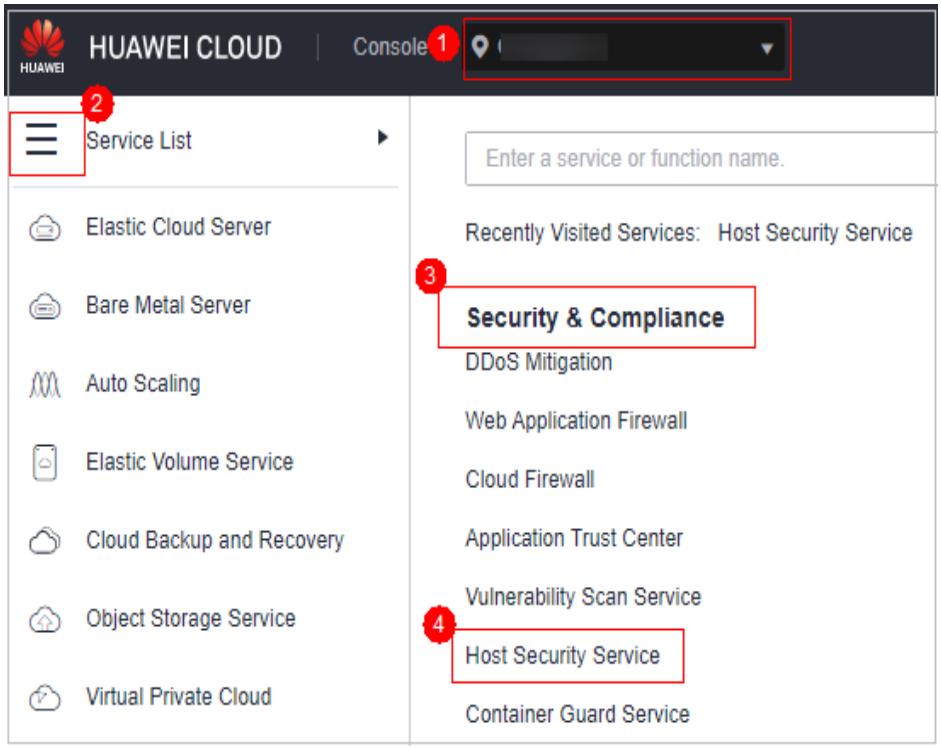
- Somente a edição de container do HSS suporta essa função. Para obter detalhes sobre como comprar e atualizar o HSS, consulte **Compra de uma cota de HSS** e **Atualização de sua edição**.
- Somente as imagens locais do mecanismo Docker podem ser relatadas ao console do HSS.
- As verificações de segurança podem ser executadas apenas em imagens do Linux.

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 3-86 Acessar o HSS



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

Passo 4 Escolha **Containers**. A página do container é exibida.

Passo 5 Visualize as informações do container e o status de segurança.

Na lista de containers, você pode visualizar o nome do container, o status, os riscos, os tempos de reinicialização, o POD e o cluster.

- Visualizar detalhes do container.

  Clique no nome do container de destino. Na página de detalhes do container exibida, visualize as informações de imagem, processo, porta e caminho de montagem do container.

- Visualizar a distribuição de risco do container.

  Visualize o número de riscos de baixo risco, médio risco, alto risco e riscos críticos no container.

----Fim

3.5.6 Manuseio de containers de risco

Cenário

O HSS pode detectar riscos de segurança de containers e classificá-los nos seguintes tipos:

- Crítica: programa malicioso
- Alto risco: ataques de ransomware, programas maliciosos, shells reversos, ataques de escape e comandos perigosos
- Médio risco: web shell, inicialização anormal, exceção de processo e acesso a arquivos confidenciais
- Baixo risco: ataque de força bruta

Para evitar que containers com riscos de segurança médios ou mais altos afetem outros containers, você pode isolar, suspender ou eliminar containers de risco.

Restrições

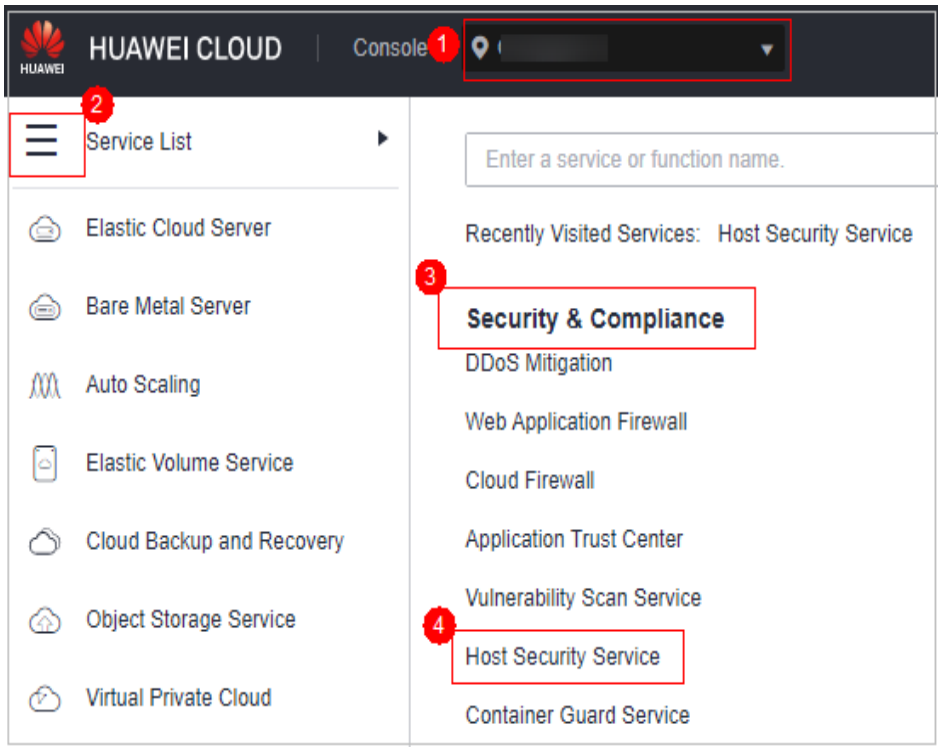
- Somente a edição de container do HSS suporta essa função. Para obter detalhes sobre como comprar e atualizar o HSS, consulte **Compra de uma cota de HSS** e **Atualização de sua edição**.
- Somente containers do Linux são suportados.
- Somente containers com riscos de segurança médios ou mais altos podem ser manuseados.

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 3-87 Acessar o HSS



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

Passo 4 Escolha **Containers**. A página do container é exibida.

Passo 5 Digite **Risk** na caixa de pesquisa e clique em para filtrar containers com riscos de segurança.

Passo 6 Na coluna **Operation** do container de risco de destino, selecione a operação a ser executada.

Containers de cluster podem ser eliminados. Os containers de nó único podem ser isolados, suspensos e eliminados.

NOTA

Somente containers com riscos médios ou mais altos podem ser manuseados. Você pode visualizar a distribuição de risco de segurança.

- **Isolar containers**: depois que um container é isolado, você não pode acessar o container quando o container está em execução e o container não pode acessar o diretório de montagem do host ou o arquivo de sistema do container.
  a. Clique em **Isolate**.
  b. Na caixa de diálogo exibida, clique em **OK**.
- **Suspender containers**: congelar os processos em execução no container.
  a. Clique em **Suspend**.
  b. Na caixa de diálogo exibida, clique em **OK**.
- **Eliminar containers**: terminar um processo de container em execução. Se **autoremove** estiver configurado para o container, o container não poderá ser retomado.
  a. Clique em **Kill** para eliminar o container.

b. Na caixa de diálogo exibida, clique em **OK**.

----Fim

Procedimento de acompanhamento

Restaurar um container para o estado em execução

Restaura um container do estado **Isolate**, **Waiting** ou **Terminated** para o estado **Running**.

NOTA

Se **autoremove** estiver configurado para um container terminado, o container não poderá ser retomado.

Passo 1 Na linha que contém o container de destino, clique em **Restore** na coluna **Operation**.

Passo 2 Na caixa de diálogo exibida, clique em **OK**.

----Fim

3.5.7 Gerenciamento de agentes de cluster

3.5.7.1 Instalação de um agente

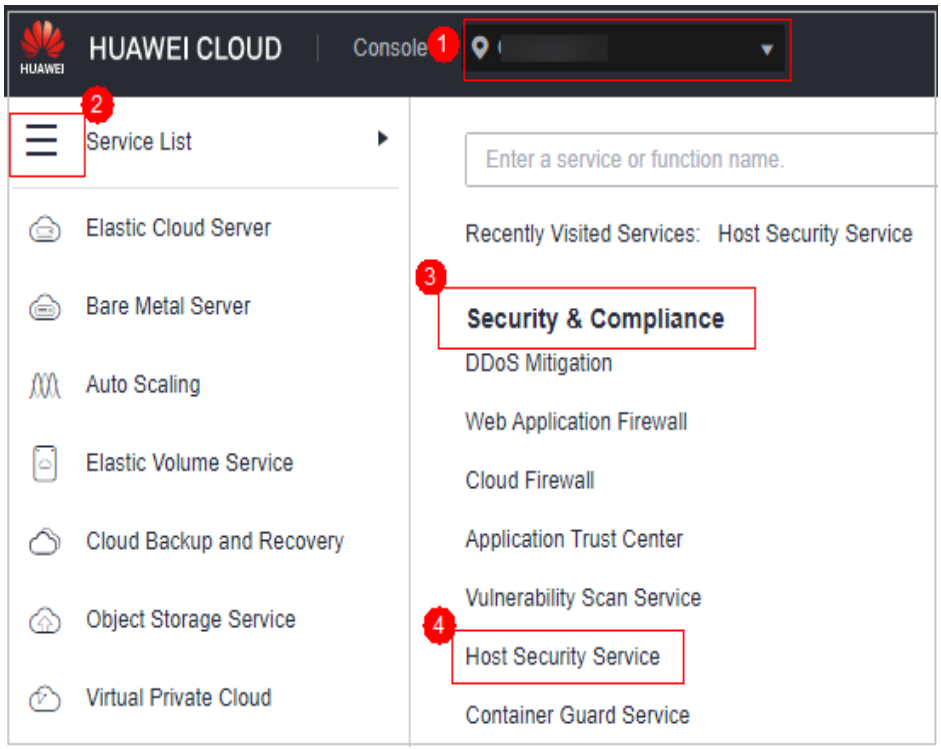
Para conectar todos os nós de container em um cluster ao HSS e ativar a proteção, instale um agente para o cluster.

Instalação de um agente em um cluster de CCE

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 3-88 Acessar o HSS



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

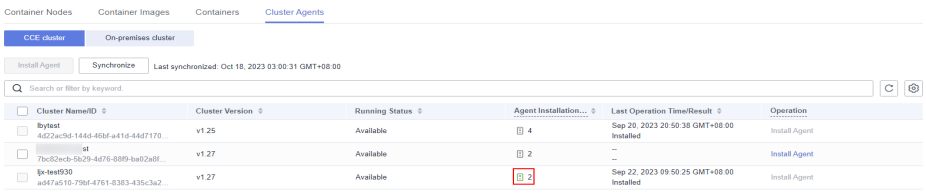
Passo 4 Clique na guia **Cluster Agents** e clique em **CCE cluster**.

Passo 5 Na coluna **Operation** de um cluster, clique em **Install Agent**.

Você também pode selecionar vários clusters e clicar em **Install Agent** no canto superior esquerdo da lista.

Passo 6 Na caixa de diálogo exibida, clique em **OK**.

A instalação demora cerca de 10 minutos. Verifique o status da instalação posteriormente.



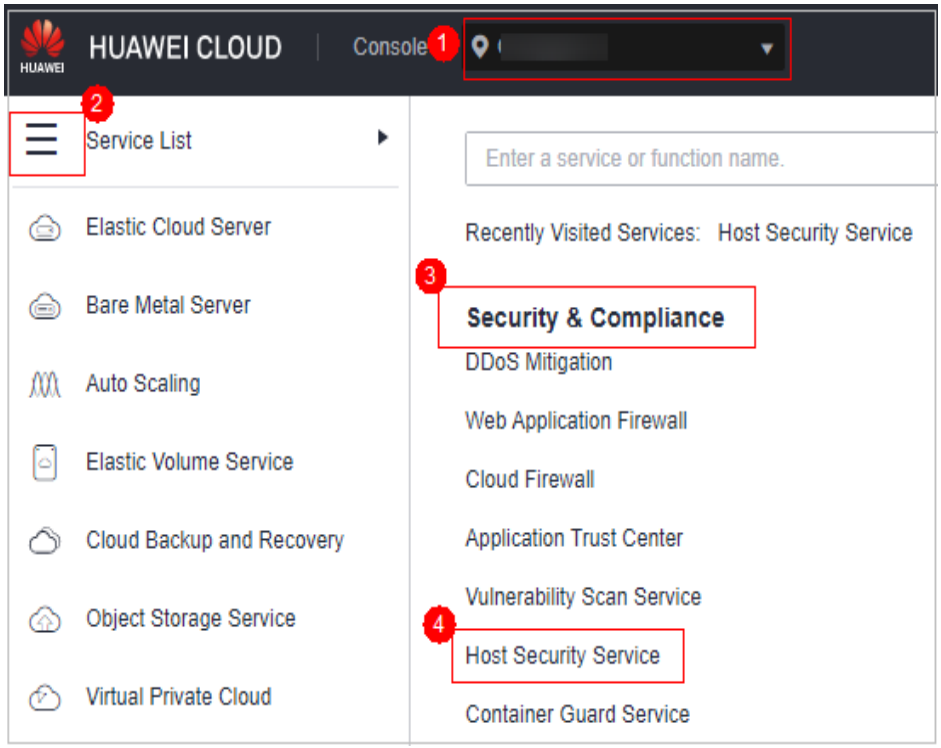
----Fim

Instalação de um agente em um cluster local

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 3-89 Acessar o HSS



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

Passo 4 Clique na guia **Cluster Agents** e clique em **On-premises cluster**.

Passo 5 Clique em **Add On-Premises Cluster**.

Passo 6 Na caixa de diálogo exibida, insira as informações do cluster e clique em **Generate Command**.

Na caixa de diálogo exibida, clique em **Save**.

Passo 7 Crie um arquivo YAML, por exemplo, **abcd.yaml**, no servidor onde os comandos do Kubernetes podem ser executados.

Passo 8 Copie o comando gerado para **abcd.yaml**.

Passo 9 Execute o seguinte comando no servidor para executar **abcd.yaml** e instalar o agente. Esta etapa leva cerca de 10 minutos.

kubectl apply -f abcd.yaml

Passo 10 Retorne ao console do HSS.

Passo 11 No painel de navegação, escolha **Installation & Configuration**.

Passo 12 Clique na guia **Agents** e clique em **Online**. Se o status do agente do servidor de cluster for **Online**, o agente foi instalado.

----Fim

Operações relacionadas

- Para modificar as informações do cluster local ou exibir comandos, clique em **Edit** na coluna **Operation**.

- Para remover as informações sobre um cluster local, clique em **Remove** na coluna **Operation**.

3.5.7.2 Desinstalação de um agente de um cluster

Se você não precisar mais do HSS para proteger os containers no cluster, desinstale o agente do cluster. Depois que o agente for desinstalado, o HSS deixará de verificar e proteger os containers e as informações sobre alarmes e vulnerabilidades detectadas serão excluídas.

Desinstalação de um agente de um cluster do CCE

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

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Containers** > **Cloud Container Engine**. O console do CCE é exibido.

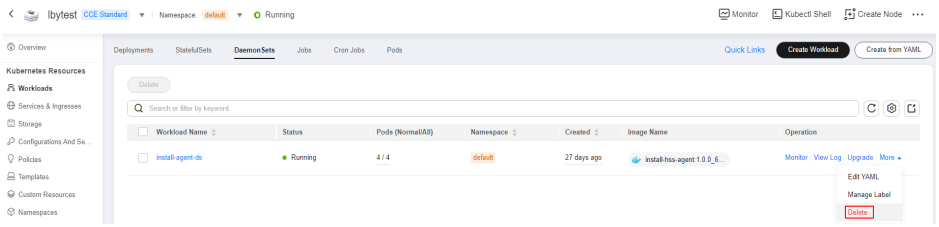
Passo 3 Clique no nome de um cluster para inserir sua página de detalhes.

Passo 4 No painel de navegação, escolha **Workloads**.

Passo 5 Clique na guia **DaemonSet** e exclua a carga de trabalho **install-agent-ds**.

Na coluna **Operation** da carga de trabalho, escolha **More** > **Delete**.

Figura 3-90 Exclusão de install-agent-ds



Passo 6 No canto superior esquerdo da página, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Passo 7 No painel de navegação, escolha **Installation & Configuration**.

Passo 8 Clique na guia **Agents** e clique em **Online**. Desinstale o agente de todos os nós de container no cluster do CCE.

Para mais detalhes, consulte **Desinstalação de um agente**.

----Fim

Desinstalação de um agente de um cluster local

Passo 1 Faça logon no cluster do Kubernetes.

Passo 2 Execute o seguinte comando para excluir a carga de trabalho **install-agent-ds**:

kubectl delete ds install-agent-ds -n default

Passo 3 **Faça logon no console de gerenciamento**.

Passo 4 No canto superior esquerdo da página, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Passo 5 No painel de navegação, escolha **Installation & Configuration**.

Passo 6 Clique na guia **Agents** e clique em **Online**. Desinstale o agente de todos os nós de container no cluster.

Para mais detalhes, consulte **Desinstalação de um agente**.

----Fim

3.6 Gerenciamento de cotas de proteção

3.6.1 Visualização de cotas

Você pode verificar, renovar e cancelar a assinatura de sua cota na lista de servidores.

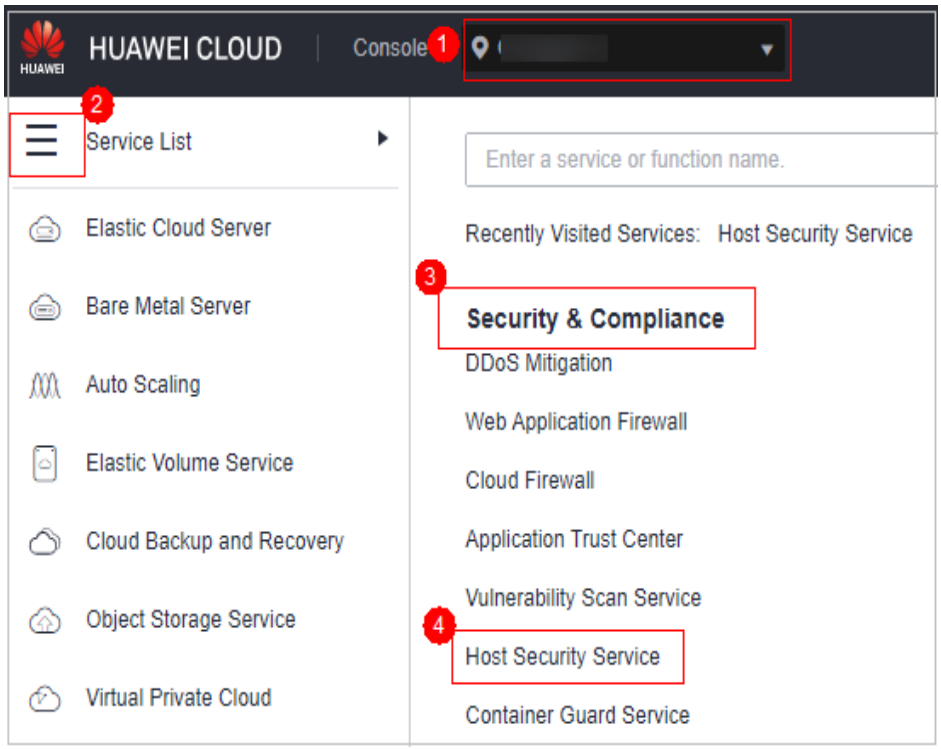
Somente a cota comprada na região selecionada é exibida. Se sua cota não for encontrada, verifique se você mudou para a região correta e pesquise novamente.

Visualização de cotas do 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 3-91 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Asset Management** > **Servers & Quota**. Na página exibida, clique na guia **Quotas**. Na página **Quotas**, clique nos diferentes botões de opção para filtrar e visualizar a lista de cotas de destino.

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 Na página de guia **Quotas**, visualize cotas de HSS. **Tabela 3-12** lista os parâmetros relacionados.

Tabela 3-12 Descrição do parâmetro

Parâmetro	Descrição
Quota ID	ID exclusivo de uma cota.
Edition	● Basic ● Professional Edition ● Enterprise ● Premium ● Web Tamper Protection (WTP)
Usage Status	● **In use**: a cota está sendo usada para um servidor. O nome do servidor é exibido abaixo do status. ● **Idle**: a cota não está em uso.
Quota Status	● **Normal**: a cota não expirou e pode ser usada corretamente. ● **Expired**: a cota expirou. Durante esse período, você ainda pode usar a cota. ● **Frozen**: a cota não protege mais seus servidores. Quando o período de congelamento expirar, a cota será permanentemente excluída.
Billing Mode	● Yearly/Monthly ● Pay-per-use
Enterprise Project Name	Nome do projeto empresarial ao qual a cota de destino pertence
Tag	Tag da categoria de recurso.

NOTA

- Vinculação de cota a um servidor

  Como alternativa, escolha **Asset Management** > **Servers & Quota** no painel de navegação esquerdo e clique na guia **Quotas**. Na lista de cotas exibida, clique em **Bind Server** na coluna **Operation** para vincular uma cota a um servidor. O HSS protegerá automaticamente o servidor.

  Uma cota pode ser vinculada a um servidor para protegê-lo, com a condição de que o agente no servidor esteja on-line.

- Desvinculação

  Na guia **Quotas** da página **Servers & Quota**, clique em **Unbind** na coluna **Operation** de uma cota. O HSS não protegerá mais o servidor e o status da cota mudará para **Idle**.

- Exportar a lista de cotas

  Clique em  no canto superior direito da lista de cotas para exportar as informações da cota na página atual.

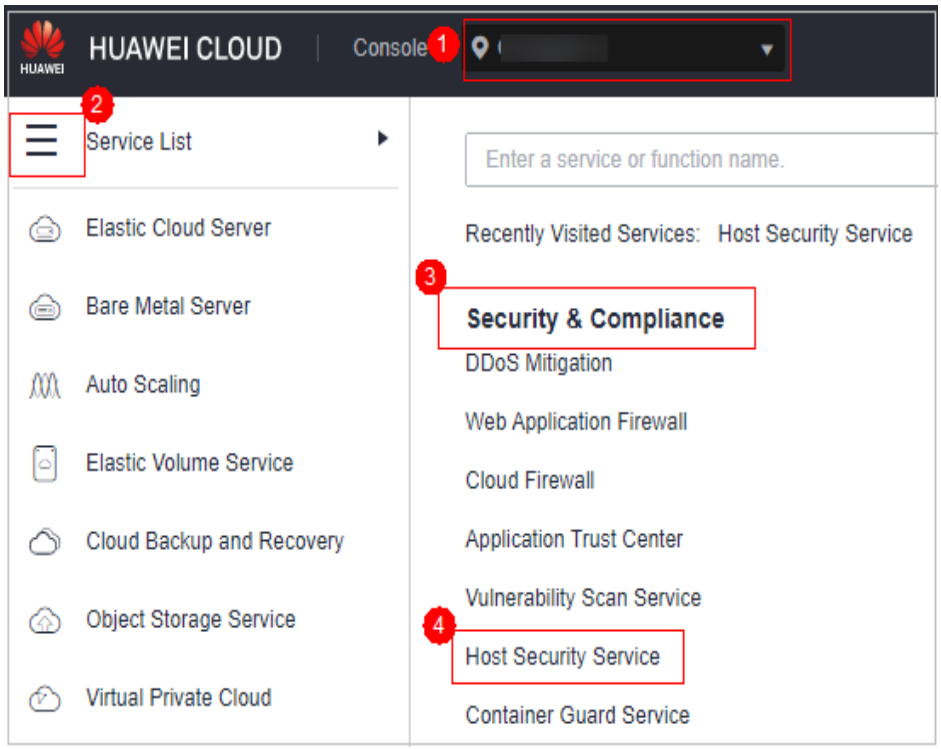
----Fim

Visualização de cotas de container

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

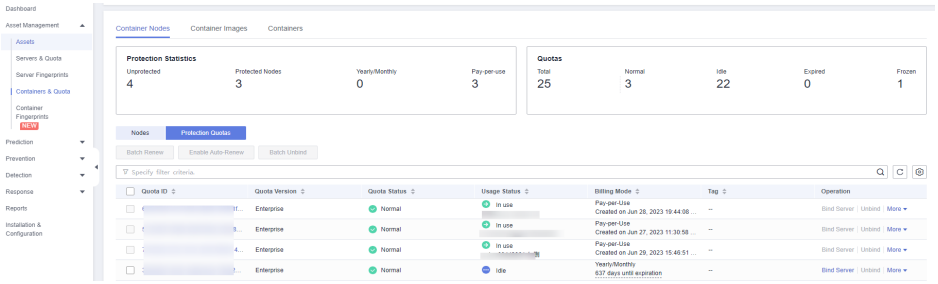
Passo 2 No canto superior esquerdo da página, selecione uma região, clique em  e escolha **Security & Compliance** > **Host Security Service**.

Figura 3-92 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Asset Management** > **Containers & Quota**. Na página exibida, clique na guia **Protection Quotas**.

Figura 3-93 Acessar a página de guia Protection Quotas



Passo 4 Na página de guia **Protection Quotas**, visualize cotas de proteção do HSS. **Tabela 3-13** lista os parâmetros relacionados.

Tabela 3-13 Descrição do parâmetro

Parâmetro	Descrição
Quota ID	ID da cota
Quota Version	Edição empresarial
Quota Status	● **Normal**: a cota é normal. ● **Expired**: a cota expirou. Durante esse período, você ainda pode usar a cota. ● **Frozen**: a cota não protege mais seus servidores. Quando o período de congelamento expirar, a cota será permanentemente excluída.
Usage Status	● **In use**: a cota está sendo usada para um servidor. O nome do servidor é exibido abaixo do status. ● **Idle**: a cota não está em uso.
Billing Mode	● Yearly/Monthly ● Pay-per-use
Tag	Tag da categoria de recurso.

NOTA

- Renovação

  Você pode clicar em **Renew** na coluna **Operation** da cota para renová-la. Para obter detalhes, consulte **Como renovar o HSS?**

- Cancelamento da assinatura

  Você pode clicar em **Unsubscribe** na coluna **Operation** da cota para cancelar a assinatura. Para obter detalhes, consulte **Como cancelar a assinatura de cotas do HSS?**

----Fim

3.6.2 Vinculação de uma cota de proteção

Você pode vincular uma cota que você comprou a um servidor para protegê-lo.

Pré-requisitos

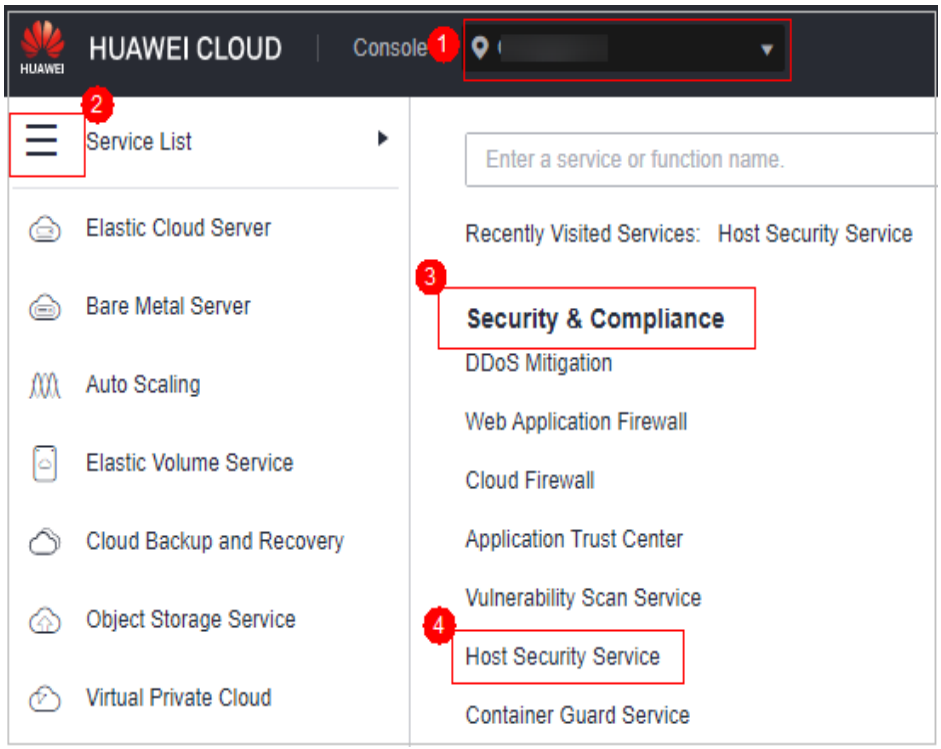
- O agente foi instalado no servidor que você deseja proteger.
- A cota está no estado **Normal** e seu **Usage Status** é **Idle**.
- Uma cota pode ser vinculada a um servidor para protegê-lo, com a condição de que o agente no servidor esteja on-line.

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 3-94 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Asset Management** > **Servers & Quota**. Na página exibida, clique na guia **Quotas**. Na página **Quotas**, clique nos diferentes botões de opção para filtrar e visualizar a lista de cotas de destino.

NOTA

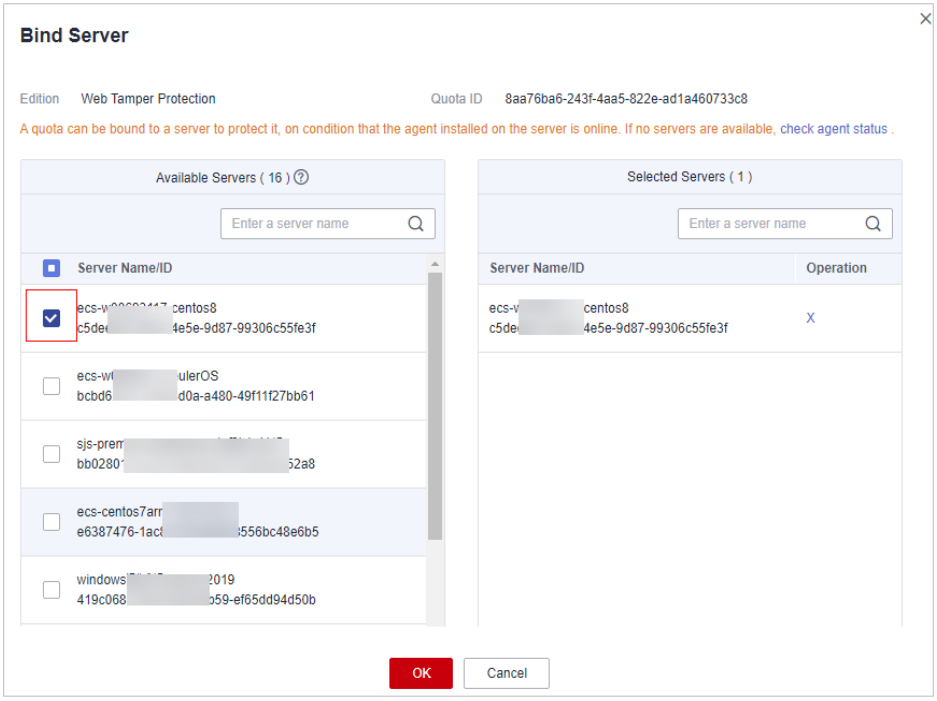
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Passo 4 Na página de guia **Quotas**, localize a linha que contém a cota de destino e clique em **Bind Server** na coluna **Operation**.

> **NOTA**
>
> Para vincular uma cota de WTP a um servidor, escolha **Prevention** > **Web Tamper Protection** no painel de navegação à esquerda. Na página de guia **Servers** exibida, localize a linha que contém o servidor desejado e clique em **Enable Protection** na coluna **Operation**. O HSS habilita automaticamente a WTP para o servidor.

Passo 5 Selecione um servidor.

Figura 3-95 Selecionar um servidor a ser vinculado



Passo 6 Clique em **OK**. O HSS ativará automaticamente a proteção para o servidor.

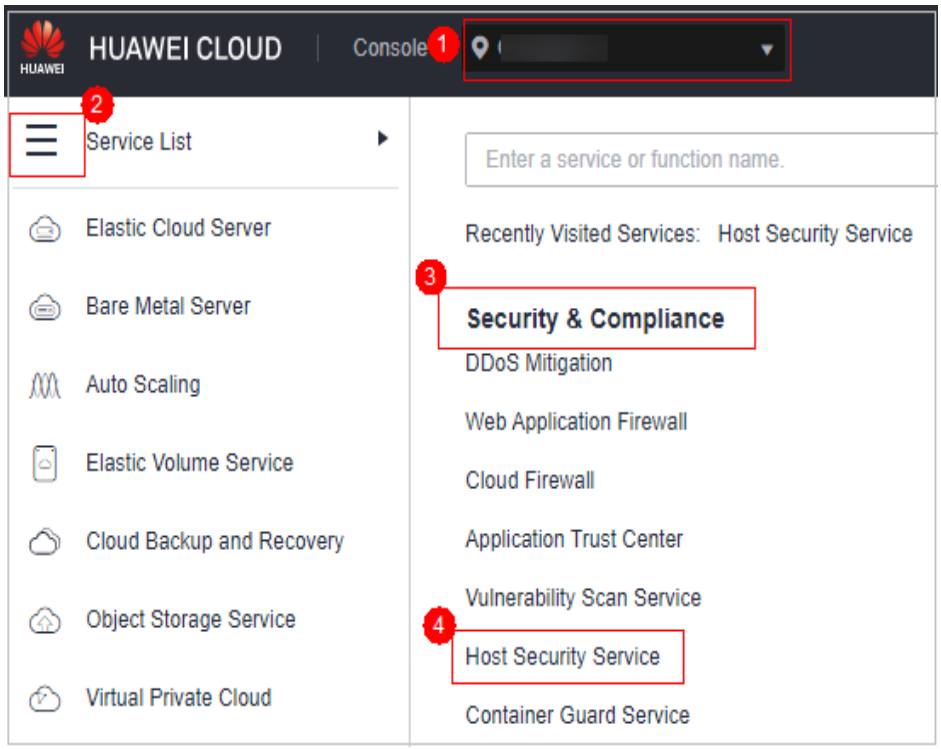
----Fim

Vinculação de cotas a containers

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 3-96 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Asset Management** > **Servers & Quota**. Na página exibida, clique na guia **Quotas**. Na página **Quotas**, clique nos diferentes botões de opção para filtrar e visualizar a lista de cotas de destino.

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 Na página de guia **Quotas**, localize a linha que contém a cota de destino e clique em **Bind Server** na coluna **Operation**.

Passo 5 Selecione um servidor.

Passo 6 Clique em **OK**. O HSS ativará automaticamente a proteção.

----Fim

3.6.3 Desvinculação de uma cota de um servidor

Você pode desvincular cotas de servidores que não precisam mais ser protegidos. Tenha cuidado ao executar esta operação, porque os servidores desprotegidos estão expostos a riscos de segurança.

Depois de desvincular uma cota, você pode vinculá-la a outro servidor ou cancelar a assinatura dela para reduzir o custo.

Pré-requisito

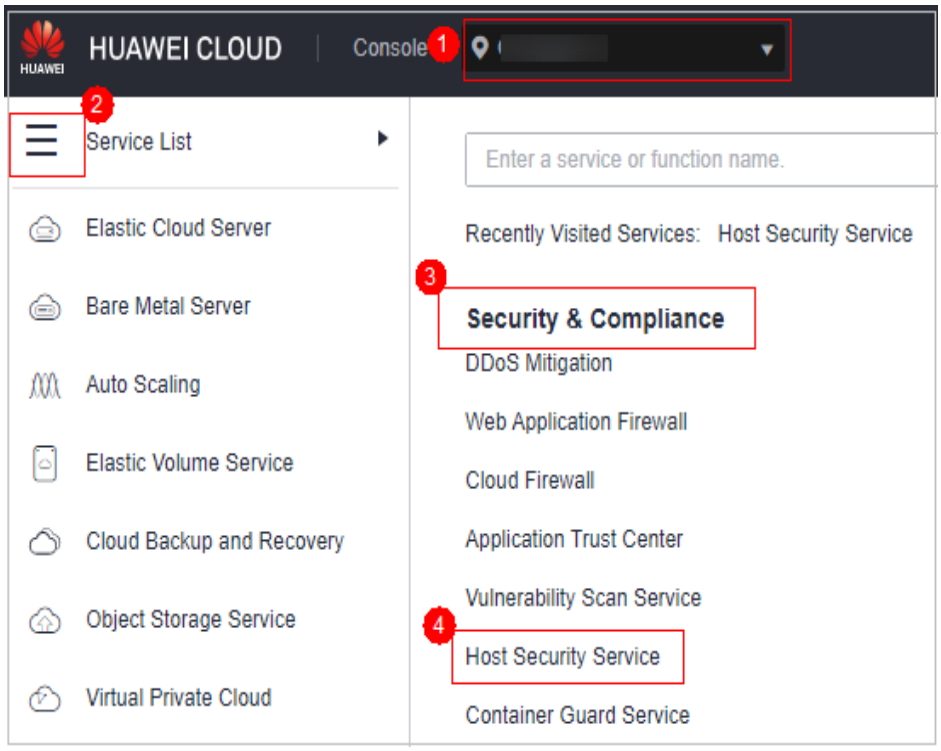
As cotas a serem desvinculadas estão em uso.

Desvinculação de uma cota de um 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 3-97 Acessar o HSS



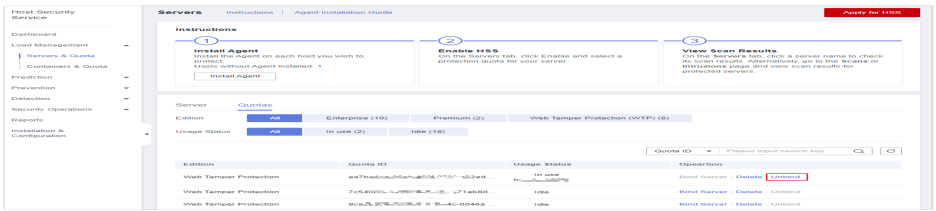
Passo 3 No painel de navegação à esquerda, escolha **Asset Management** > **Servers & Quota**. Na página exibida, clique na guia **Quotas**. Na página **Quotas**, clique nos diferentes botões de opção para filtrar e visualizar a lista de cotas de destino.

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 Na página **Quotas**, clique em **Unbind** na coluna **Operation** de uma cota.

Figura 3-98 Desvinculação de cotas



NOTA

Tenha cuidado ao executar esta operação, porque os servidores desprotegidos estão expostos a riscos de segurança.

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

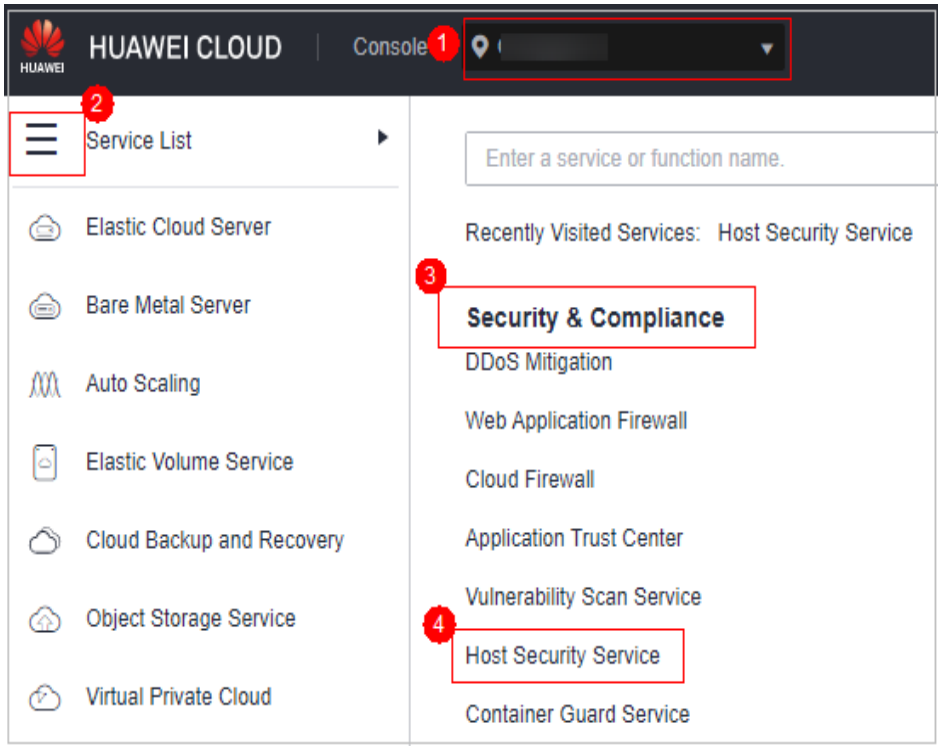
----Fim

Desvinculação de uma cota de container

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 3-99 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Asset Management** > **Servers & Quota**. Na página exibida, clique na guia **Quotas**. Na página **Quotas**, clique nos diferentes botões de opção para filtrar e visualizar a lista de cotas de destino.

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 Na página **Quotas**, clique em **Unbind** na coluna **Operation** de uma cota.

Para desvincular cotas em lotes, selecione os servidores aos quais elas estão vinculadas e clique em **Batch Unbind** acima da lista de cotas.

NOTA

Tenha cuidado ao executar esta operação, porque os servidores desprotegidos estão expostos a riscos de segurança.

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

----Fim

3.6.4 Atualização de sua edição

Você pode atualizar para uma edição superior e desfrutar de recursos de segurança mais fortes.

Precauções

- **Premium**, **Web Tamper Protection** e **Container** são edições de alta configuração e não podem ser atualizadas. Você pode comprar essas cotas separadamente.
- **Basic**, **Professional** e **Enterprise** podem ser atualizadas para uma edição de cota superior.
  - **Basic**: pode ser atualizada para **Professional**, **Enterprise** ou **Premium**.
  - **Professional**: pode ser atualizada para **Enterprise** ou **Premium**.
  - **Enterprise**: pode ser atualizada para **Premium**.

Pré-requisito

- O **Usage Status** de uma cota deve ser **Idle**.
- O **Quota Status** de uma cota deve ser **Normal**.

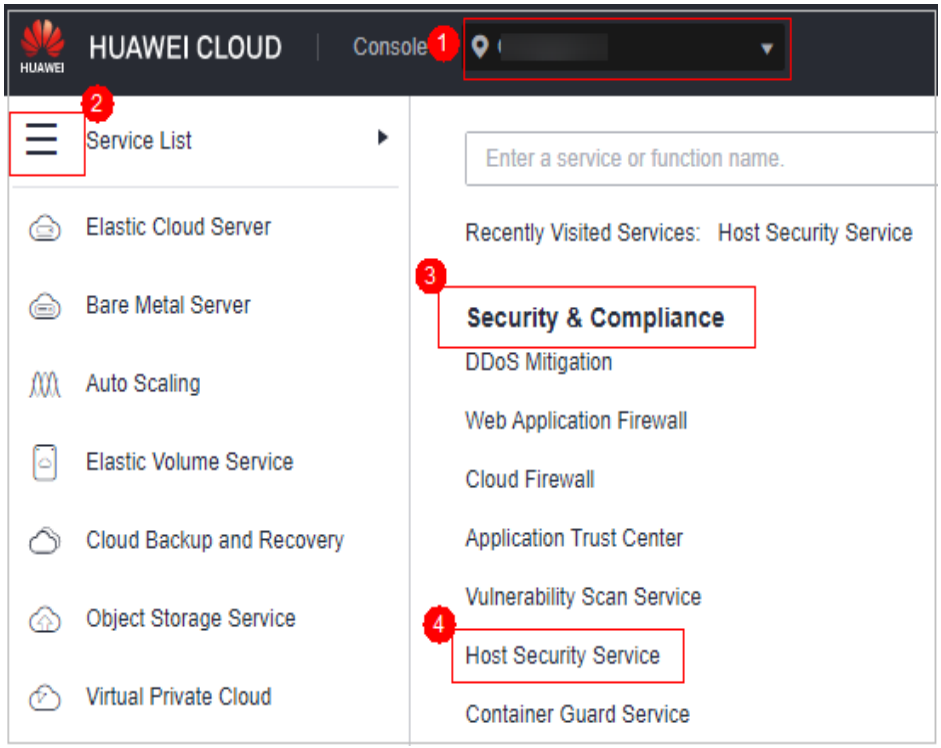
Atualizar para a edição Professional/Enterprise/Premium

Para atualizar uma cota que está sendo usada para proteger um servidor, desvincule-a do servidor primeiro.

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 3-100 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Asset Management** > **Servers & Quota**. Na página exibida, clique na guia **Quotas**. Na página **Quotas**, clique nos diferentes botões de opção para filtrar e visualizar a lista de cotas de destino.

NOTA

Se os servidores forem gerenciados por projetos empresariais, você poderá selecionar o projeto empresarial de destino para visualizar ou operar as informações sobre ativos e detecção.

Passo 4 Na lista de cotas, filtre as cotas ociosas da edição básica ou empresarial. Selecione uma cota e clique em **Upgrade**.

NOTA

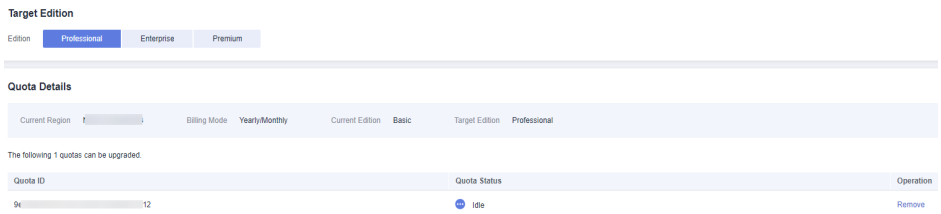
- Antes de atualizar uma cota em uso, **desvincule-a** do servidor que ela protege.
- A desvinculação não afeta os serviços.

Passo 5 Configure as informações de upgrade.

NOTA

A edição básica pode ser atualizada para a edição empresarial ou premium. A edição empresarial é atualizada para a edição premium por padrão.

Figura 3-101 Confirmar informações de upgrade



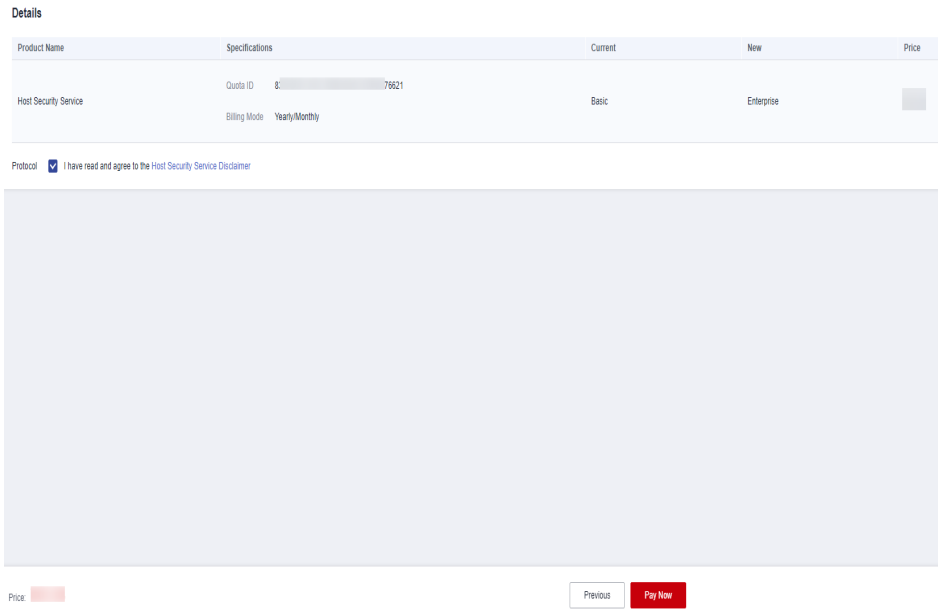
Passo 6 Confirme a versão de atualização e clique em **Next**.

NOTA

Quando você paga pelo upgrade, você só precisa compensar a diferença.

Passo 7 Confirme as informações de compra, selecione **I have read and agree to the Host Security Service Disclaimer** e clique em **Pay Now**.

Figura 3-102 Confirmar informações do pedido



Passo 8 Aguarde até que o pagamento seja concluído. Retorne à **lista de cotas**. Localize a cota pelo seu ID e verifique sua edição.

Passo 9 **Vincule a cota** a um servidor e ative a proteção.

----Fim

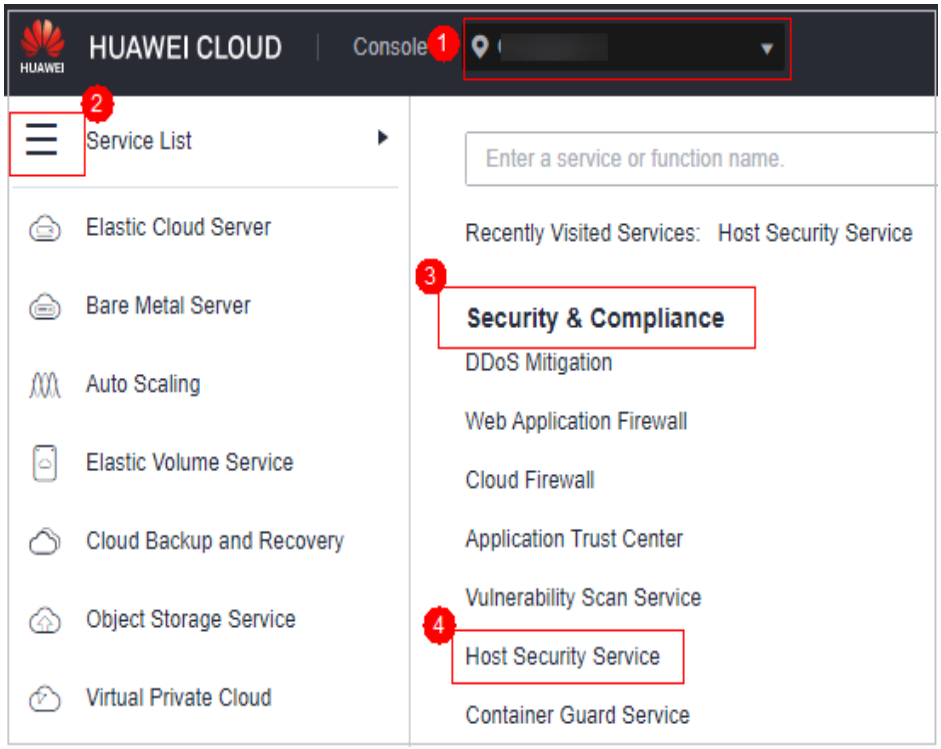
Atualizar para a edição WTP

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.

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 3-103 Acessar o HSS



Passo 3 No canto superior direito da página **Dashboard**, clique em **Buy HSS**.

Passo 4 Na página **Buy HSS**, selecione a edição WTP.

Tabela 3-14 Parâmetros para compra de HSS

Parâmetro	Descrição	Exemplo de valor
Billing Mode	Selecione o modo de cobrança **Yearly/Monthly** ou **Pay-per-use** com base em suas necessidades. ● Yearly/Monthly: você pode selecionar a edição básica, profissional, empresarial, premium, WTP ou de container. Você pode comprar a edição por um período fixo de tempo. A taxa é 30% menor do que a do pagamento por uso. Se você usar a edição por um longo tempo, você é aconselhado a comprar pacotes anuais/mensais. ● Pay-per-use: somente a edição empresarial pode ser comprada. Você precisa ativar esta edição na lista de servidores. Você paga pelo tempo de uso dos recursos. Os preços são calculados por hora, e nenhuma taxa mínima é necessária. **NOTA** Procedimento para ativar a cota de pagamento por uso: 1. Na página de compra, selecione **Pay-per-use**. A edição **Enterprise** será selecionada automaticamente. No canto inferior direito, clique em **Enable Now**. Você será redirecionado para a lista de servidores. 2. Na lista de servidores, clique em **Enable** na coluna **Operation**. Defina o **Billing Mode** para **Pay-per-use** e **Edition** para **Enterprise**. 3. Confirme as informações e clique em **OK**.	Yearly/ Monthly
Region	● Para minimizar os problemas de conexão, compre a cota na região de seus servidores.	CN-Hong Kong
Edition	As edições básica, profissional, empresarial, premium, WTP e de container são suportadas. Para detalhes sobre as diferenças entre as edições, consulte **Edições**. **AVISO** ● Se você ativar a edição básica do HSS pela primeira vez, poderá aproveitar o teste gratuito por 30 dias e comprá-lo após o teste. ● Se você comprou a edição básica, empresarial ou premium, ative-a na página **Asset Management** > **Servers & Quota**. ● Se você comprou a edição WTP, ative-a na lista de servidores na página **Prevention** > **Web Tamper Protection**. ● Se você comprou a edição de container, escolha **Asset Management** > **Containers & Quota** e ative a proteção na guia **Container Nodes**.	Enterprise

Parâmetro	Descrição	Exemplo de valor
Enterprise Project	Essa opção só está disponível quando você estiver conectado usando uma conta empresarial ou quando tiver ativado projetos empresariais. Para ativar essa função, entre em contato com seu gerente de clientes. Um projeto empresarial fornece um modo de gerenciamento de recursos de nuvem, no qual os recursos e os membros da nuvem são gerenciados centralmente pelo projeto. Selecione um projeto empresarial na lista suspensa. **NOTA** ● Os recursos e as despesas incorridas são gerenciados sob o projeto empresarial selecionado. ● Valor **default** indica o projeto empresarial padrão. Os recursos que não estão alocados a nenhum projeto empresarial na sua conta são exibidos no projeto empresarial padrão. ● A opção **default** está disponível na lista suspensa **Enterprise Project** somente depois que você comprou o HSS com sua Huawei ID.	default
Required duration	● Selecione uma duração com base em suas necessidades. No modo **Pay-per-use**, você não precisa selecionar uma duração. ● 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
Server Quota	Insira o número de cotas de HSS a serem compradas. No modo **Pay-per-use**, você não precisa configurar essa opção. **AVISO** ● Todos os seus servidores devem ser protegidos, de modo que, se um vírus (como ransomware ou um programa de mineração) infectar um deles, ele não será capaz de se espalhar para outros e danificar toda a sua rede. ● Não é possível modificar a cota de uma edição após a conclusão da compra. Você pode cancelar a assinatura e comprar novamente.	20
Tag	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). Para usar essa função, sua conta deve ter a permissão **TMS administrator**. Sem essa permissão, você não pode adicionar tags às cotas de proteção e a mensagem de erro "permission error" será exibida. Você não precisa definir este parâmetro no modo de pagamento por uso.	data

Passo 5 No canto inferior direito da página, clique em **Next**.

Para obter detalhes sobre preços, consulte **Detalhes de preços de produtos**.

Passo 6 Depois de confirmar o pedido, selecione **I have read and agree to the Host Security Service Disclaimer** e clique em **Pay Now**.

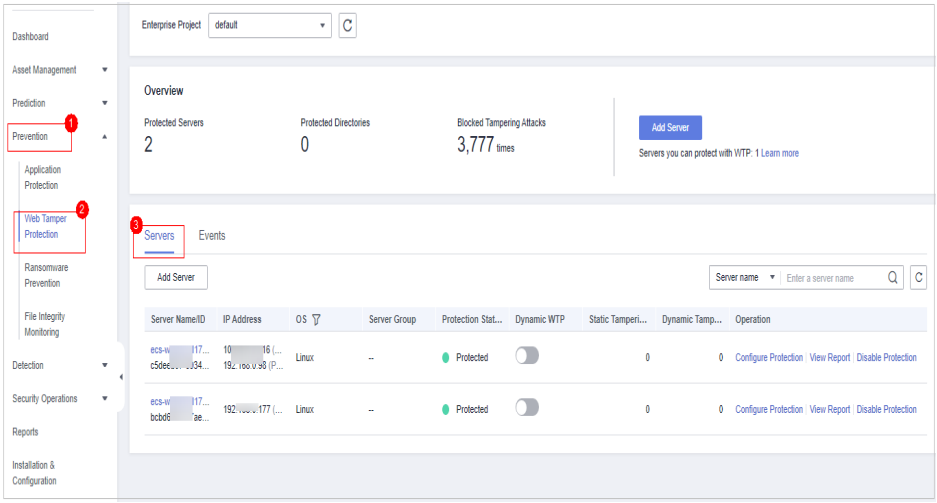
Passo 7 Na caixa de diálogo exibida, selecione um modo de verificação, clique em **Send Code**, insira o código de verificação recebido e clique em **OK**.

Passo 8 No painel de navegação, escolha **Prevention** > **Web Tamper Protection**. Na guia **Servers**, clique em **Add Server**.

AVISO

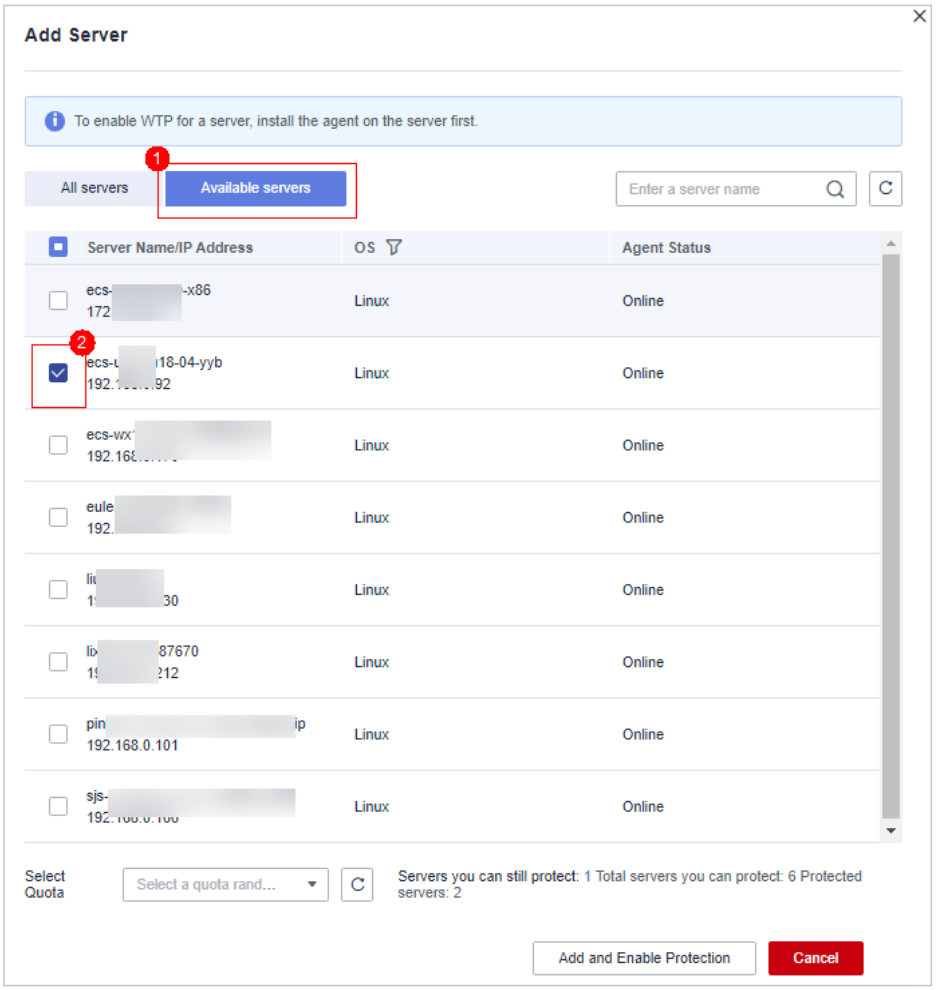
- Certifique-se de que o servidor a ser protegido pela WTP não esteja vinculado a outras cotas. Escolha **Asset Management** > **Servers & Quota** e clique na guia **Servers**. Se o status de proteção do servidor for **Protected**, isso indica que o servidor está vinculado a outra cota. Nesse caso, clique em **Disable** na coluna **Operation**.
- Desvincular um servidor de uma cota não afeta os serviços.

Figura 3-104 Página de configuração da proteção



Passo 9 Clique em **Add Server**, selecione um servidor e clique em **Add and Enable Protection**.

Figura 3-105 Selecionar um servidor



Passo 10 Verifique as configurações de WTP. Escolha **Asset Management** > **Servers & Quota** e clique na guia **Servers**. Se **WTP** for exibida na coluna **Edition/Expiration Date**, a edição WTP foi ativada.

NOTA

Se você não precisar que a cota seja substituída pela WTP, poderá cancelar a assinatura dela. Escolha **Asset Management** > **Servers & Quota** e clique em **Quotas**. Na coluna **Operation** da cota, escolha **More** > **Unsubscribe**.

----Fim

4 Prevenção de riscos

4.1 Gerenciamento de vulnerabilidades

4.1.1 Visão geral do gerenciamento de vulnerabilidades

O gerenciamento de vulnerabilidades pode detectar vulnerabilidades do Linux, Windows, Web-CMS e de aplicações e fornecer sugestões, ajudando você a aprender sobre as vulnerabilidades do servidor em tempo real. As vulnerabilidades do Linux e do Windows podem ser corrigidas no modo de um clique. Esta seção descreve como as vulnerabilidades são detectadas e as vulnerabilidades que podem ser verificadas e corrigidas em cada edição do HSS.

NOTA

A lista de vulnerabilidades exibe as vulnerabilidades detectadas nos últimos sete dias. Depois que uma vulnerabilidade for detectada em um servidor, se você alterar o nome do servidor e não executar uma verificação de vulnerabilidade novamente, a lista de vulnerabilidades ainda exibirá o nome do servidor original.

Como funciona a verificação de vulnerabilidades

Tabela 4-1 descreve como diferentes tipos de vulnerabilidades são detectados.

Tabela 4-1 Como funciona a verificação de vulnerabilidades

Tipo	Mecanismo
Vulnerabilidade do Linux	Com base no banco de dados de vulnerabilidades, verifica e manipula vulnerabilidades no software (como kernel, OpenSSL, vim, glibc) que você obteve de fontes oficiais do Linux e não compilou, relata os resultados para o console de gerenciamento e gera alarmes.
Vulnerabilidade do Windows	Sincroniza patches oficiais da Microsoft, verifica se os patches no servidor foram atualizados, faz push de patches oficiais da Microsoft, relata os resultados para o console de gerenciamento e gera alarmes de vulnerabilidade.

Tipo	Mecanismo
Vulnerabilidade de Web-CMS	Verifica diretórios e arquivos da Web em busca de vulnerabilidades de Web-CMS, relata os resultados ao console de gerenciamento e gera alarmes de vulnerabilidade.
Vulnerabilidade da aplicação	Detecta as vulnerabilidades no software e nos pacotes de dependência em execução no servidor, relata vulnerabilidades arriscadas para o console e exibe alarmes de vulnerabilidade.

Restrições

- A edição básica suporta verificação automática e visualização de vulnerabilidades do Linux e do Windows, mas não suporta a comutação de visualização do servidor ou o tratamento de vulnerabilidades.
- Se a versão do agente em um SO Windows for 4.0.18 ou posterior, as vulnerabilidades da aplicação podem ser verificadas. Para obter detalhes sobre como atualizar o agente, consulte **Atualização do agente**.
- O **Server Status** está **Running**, **Agent Status** está **Online** e **Protection Status** está **Protected**. Caso contrário, a verificação de vulnerabilidades não poderá ser executada.
- **Tabela 4-2** descreve os SOs que suportam verificação e correção de vulnerabilidades.

Tabela 4-2 SOs que suportam verificação e correção de vulnerabilidades

Tipo de SO	SO suportado
Windows	● Windows Server 2019 Datacenter 64-bit English (40 GB) ● Windows Server 2019 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 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)
Linux	● EulerOS: 2.2, 2.3, 2.5, 2.8, 2.9 (64-bit) ● CentOS 7.4, 7.5, 7.6, 7.7, 7.8 and 7.9 (64-bit) ● Ubuntu 16.04, 18.04, 20.04 (64-bit) ● Debian 9, 10, and 11 (64-bit) ● Kylin V10 (64-bit) ● SUSE Linux 12 SP5, 15 SP2 and 15.5 (64-bit) ● UnionTech OS V20 server E and V20 server D (64-bit)

Tipos de vulnerabilidades que podem ser verificados e corrigidos

Para obter detalhes sobre os tipos de vulnerabilidades que podem ser verificados e corrigidos em diferentes edições do HSS, consulte **Tabela 4-3**.

Os significados dos símbolos na tabela são os seguintes:

- √: suportado
- ×: não suportado

Tabela 4-3 Tipos de vulnerabilidades que podem ser verificadas e corrigidas em cada edição do HSS

Tipo de vulnerabilidade	Função	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição de Proteção contra adulteração na Web	Edição de container
Vulnerabilidade do Linux	Verificação automática de vulnerabilidades (uma vez por semana por padrão)	√	√	√	√	√	√
	Configuração da política de vulnerabilidades	×	√	√	√	√	√
	Verificação manual de vulnerabilidades	×	√	√	√	√	√
	Correção de vulnerabilidade com um clique	×	√ (Um máximo de 50 vulnerabilidades podem ser corrigidas por vez.)	√ (Um máximo de 50 vulnerabilidades podem ser corrigidas por vez.)	√	√	√

Tipo de vulnerabilidade	Função	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição de Proteção contra adulteração na Web	Edição de container
Vulnerabilidade do Windows	Verificação automática de vulnerabilidades (uma vez por semana por padrão)	√	√	√	√	√	×
	Configuração da política de vulnerabilidades	×	√	√	√	√	×
	Verificação manual de vulnerabilidades	×	√	√	√	√	×
	Correção de vulnerabilidade com um clique	×	√ (Um máximo de 50 vulnerabilidades podem ser corrigidas por vez.)	√ (Um máximo de 50 vulnerabilidades podem ser corrigidas por vez.)	√	√	×
Vulnerabilidade de Web-CMS	Verificação automática de vulnerabilidades (uma vez por semana por padrão)	×	√	√	√	√	√
	Configuração da política de vulnerabilidades	×	√	√	√	√	√

Tipo de vulnerabilidade	Função	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição de Proteção contra adulteração na Web	Edição de container
	Verificação manual de vulnerabilidades	×	√	√	√	√	√
	Correção de vulnerabilidade com um clique	×	×	×	×	×	×
Vulnerabilidade da aplicação	Verificação automática de vulnerabilidades (uma vez por semana por padrão)	×	×	√	√	√	√
	Configuração da política de vulnerabilidades	×	×	√	√	√	√
	Verificação manual de vulnerabilidades	×	×	√	√	√	√
	Correção de vulnerabilidade com um clique	×	×	×	×	×	×

NOTA

- O HSS pode fazer a verificação de vulnerabilidades de Web-CMS e de aplicações, mas não pode corrigi-las. Você pode fazer logon no servidor para corrigir manualmente a vulnerabilidade consultando as sugestões exibidas na página de detalhes da vulnerabilidade.
- Você pode configurar o período de verificação automática, o escopo da verificação automática e a lista branca de vulnerabilidades. Para obter detalhes sobre como configurar o período de verificação automática e o escopo da verificação automática, consulte **Verificação automática de vulnerabilidades**. Para obter detalhes sobre como configurar a lista branca de vulnerabilidades, consulte **Gerenciamento da lista branca de vulnerabilidades**.

4.1.2 Verificação de vulnerabilidade

O HSS pode fazer a verificação de vulnerabilidades em Linux, Windows, Web-CMS e aplicações. Verificações automáticas e manuais são suportadas.

- Verificação automática: você pode configurar o período e o escopo da verificação para verificar periodicamente vulnerabilidades nos servidores.
- Verificação manual: para visualizar vulnerabilidades em tempo real de um servidor, você pode procurar vulnerabilidades manualmente.

Esta seção descreve como definir uma política de verificação automática e fazer verificação manual de vulnerabilidades.

Restrições

- A edição básica pode verificar automaticamente apenas vulnerabilidades do Linux e do Windows. A edição profissional não pode fazer verificação de vulnerabilidades de aplicações.
- Se a versão do agente em um SO Windows for 4.0.18 ou posterior, as vulnerabilidades da aplicação podem ser verificadas. Para obter detalhes sobre como atualizar o agente, consulte **Atualização do agente**.
- O **Server Status** está **Running**, **Agent Status** está **Online** e **Protection Status** está **Protected**. Caso contrário, a verificação de vulnerabilidades não poderá ser executada.
- Para obter detalhes sobre os tipos de vulnerabilidades que podem ser verificados por diferentes edições do HSS, consulte **Tipos de vulnerabilidades que podem ser verificados e corrigidos**.
- **Tabela 4-4** descreve os SOs que suportam a verificação de vulnerabilidades.

Tabela 4-4 SOs que suportam verificação de vulnerabilidades

Tipo de SO	SO suportado
Windows	• Windows Server 2019 Datacenter 64-bit English (40 GB) • Windows Server 2019 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 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)

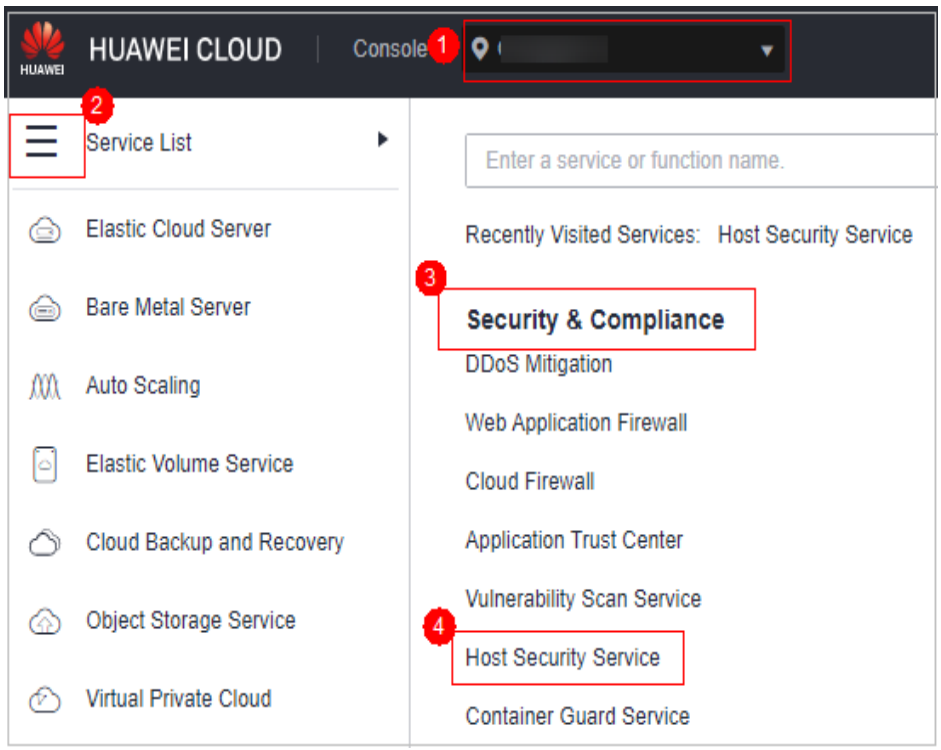
Tipo de SO	SO suportado
Linux	● EulerOS 2.2, 2.3, 2.5, 2.8, and 2.9 (64-bit) ● CentOS 7.4, 7.5, 7.6, 7.7, 7.8 and 7.9 (64-bit) ● Ubuntu 16.04, 18.04, and 20.04 (64-bit) ● Debian 9 and 10 (64-bit) ● Kylin V10 (64-bit) ● SUSE 12 and 15 (64-bit) ● UnionTech OS V20 server E and V20 server D (64-bit)

Verificação manual 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 4-1 Acessar o HSS



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

Passo 4 Clique em **Scan** no canto superior direito da página **Vulnerabilities**.

Passo 5 Na caixa de diálogo **Scan for Vulnerability** exibida, selecione o tipo de vulnerabilidade e o escopo a serem verificados. Para obter mais informações, consulte **Tabela 4-5**.

Tabela 4-5 Parâmetros para vulnerabilidades de verificação manual

Parâmetro	Descrição
Type	Selecione um ou mais tipos de vulnerabilidades a serem verificados. Os valores possíveis são os seguintes: ● **Linux** ● **Windows** ● **Web-CMS** ● **Application**
Scan	Selecione os servidores a serem verificados. Os valores possíveis são os seguintes: ● **All servers** ● **Selected servers** Você pode selecionar um grupo de servidores ou pesquisar o servidor de destino por nome de servidor, ID, EIP ou endereço IP privado. **NOTA** Os seguintes servidores não podem ser selecionados para verificação de vulnerabilidades: ● Servidores que usam a edição básica do HSS ● Servidores que não estão no estado **Running** ● Servidores cujo status de agente é **Offline**

Passo 6 Clique em **OK**.

Passo 7 Clique em **Manage Task** no canto superior direito da página **Vulnerabilities**. No painel deslizante **Manage Task** exibido, clique na guia **Scan Tasks** para visualizar o status e o resultado da verificação da tarefa de verificação de vulnerabilidade.

Clique no número ao lado da figura vermelha na coluna **Scan Result** para exibir as informações sobre os servidores que falham na verificação.

NOTA

Você também pode selecionar **Asset Management** > **Servers & Quota** e verificar se há vulnerabilidades em um único servidor na guia **Servers**. O procedimento é o seguinte:

1. Clique em um nome de servidor.
2. Escolha **Vulnerabilities**.
3. Escolha o tipo de vulnerabilidade a ser verificada e clique em **Scan**.

----Fim

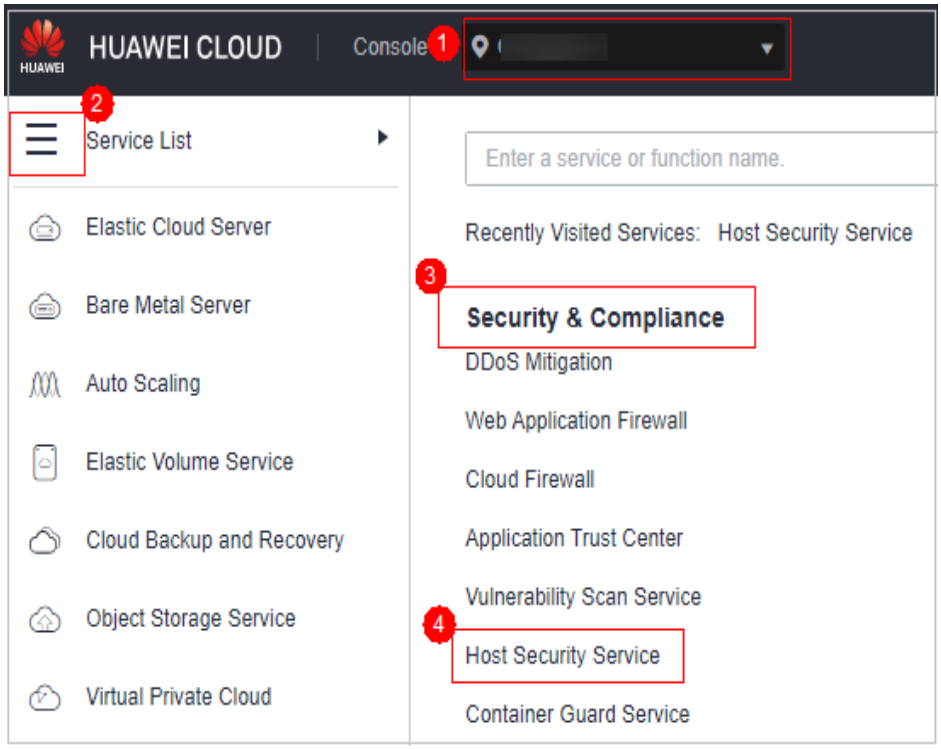
Verificação automática de vulnerabilidades

- Por padrão, a edição básica verifica automaticamente vulnerabilidades do Linux e do Windows no início da manhã todos os dias. Mas você não pode configurar o período e o escopo da verificação.
- Para as edições profissional ou superior, você pode configurar o período e o escopo da verificação para verificar periodicamente vulnerabilidades nos servidores.

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 4-2 Acessar o HSS



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

Passo 4 No canto superior direito da página **Vulnerabilities**, clique em **Configure Policy** para definir o período e o escopo da verificação de vulnerabilidades.

- **Scan Period**
  - **Scan period**: o valor padrão é **00:00:00 - 07:00:00** e não pode ser alterado.
  - **Scan Period**: selecione **Every day**, **Every three days** ou **Every week**.
- **Scan**
  - Ativar ou desativar a verificação do servidor:  indica que a verificação do servidor está ativada.
  - Selecionar os servidores a serem verificados: clique em **Select Server to Scan**. Na página de gerenciamento do servidor exibida, selecione os servidores a serem verificados.

    NOTA

    Os seguintes servidores não podem ser selecionados para verificação de vulnerabilidades:
    - Servidores que usam a edição básica do HSS
    - Servidores que não estão no estado **Running**
    - Servidores cujo status de agente é **Offline**

Passo 5 Clique em **Manage Task** no canto superior direito da página **Vulnerabilities**. No painel deslizante **Manage Task** exibido, clique na guia **Scan Tasks** para visualizar o status e o resultado da verificação da tarefa de verificação de vulnerabilidade.

Clique no número ao lado da figura vermelha na coluna **Scan Result** para exibir as informações sobre os servidores que falham na verificação.

----Fim

4.1.3 Visualização de detalhes da vulnerabilidade

Você pode visualizar as vulnerabilidades dos seus ativos na página **Vulnerabilities**.

Restrições

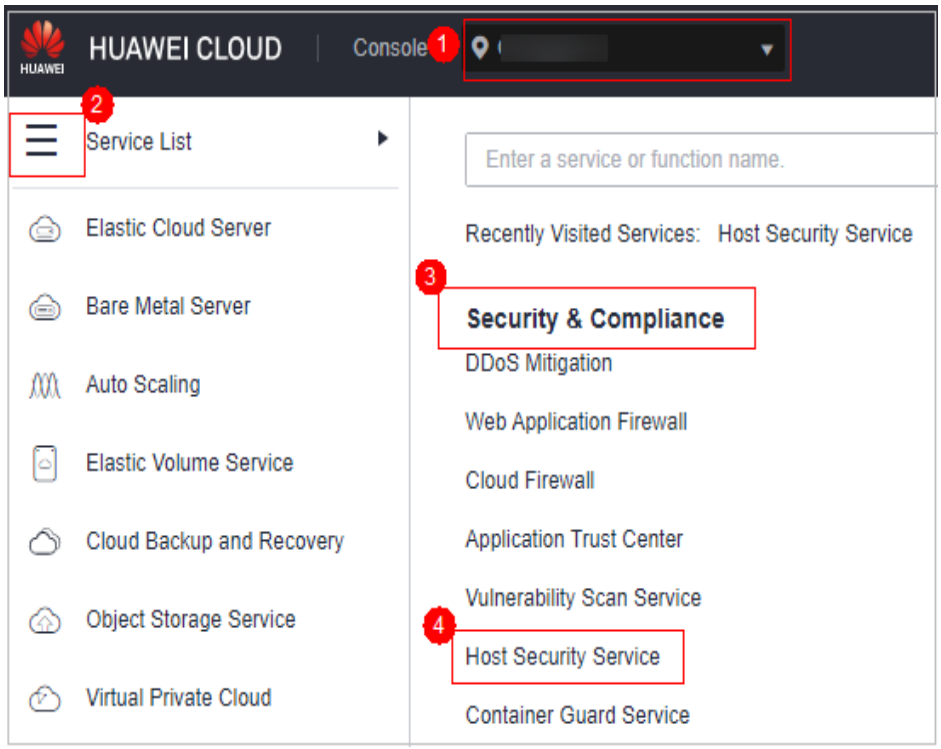
- Os servidores que não são protegidos pelo HSS não suportam esta função.
- O **Server Status** está **Running**, **Agent Status** está **Online** e **Protection Status** está **Protected**. Caso contrário, a verificação de vulnerabilidades não poderá ser executada.
- Atualmente, o HCE 2.0 não oferece suporte à detecção de vulnerabilidades e à detecção de configuração. Essas funções serão suportadas em versões posteriores.

Visualização de detalhes da vulnerabilidade

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**.

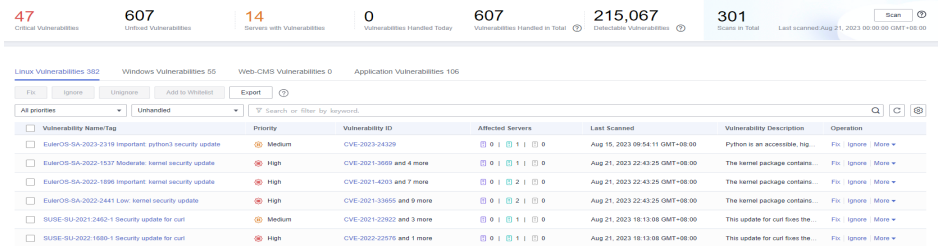
Figura 4-3 Acessar o HSS



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

Passo 4 Visualize informações sobre vulnerabilidades na página **Vulnerabilities**.

Figura 4-4 Visualização de detalhes da vulnerabilidade



- Visualização de resultados da verificação de vulnerabilidades

  Na área de estatísticas de vulnerabilidade na parte superior da página **Vulnerabilities**, visualize os resultados da verificação de vulnerabilidades. **Tabela 4-6** descreve os parâmetros relacionados.

  Tabela 4-6 Parâmetros de verificação de vulnerabilidade

Parâmetro	Descrição
Critical Vulnerabilities	Clique no número em **Critical vulnerabilities**. No painel deslizante exibido, você pode ver todos os tipos de vulnerabilidades a serem corrigidas com urgência.
Unfixed Vulnerabilities	Clique no número em **Unfixed Vulnerabilities**. No painel deslizante exibido, você pode visualizar todos os tipos de vulnerabilidades que não são corrigidas.
Servers with Vulnerabilities	Clique no número em **Servers with Vulnerabilities**. Você pode ver os servidores com vulnerabilidades na parte inferior da página **Vulnerabilities**.
Vulnerabilities Handled Today	Clique no número em **Vulnerabilities Handled Today**. No painel deslizante exibido, você pode ver todos os tipos de vulnerabilidades que foram manipuladas hoje.
Vulnerabilities Handled in Total	Clique no número em **Vulnerabilities Handled in Total**. No painel deslizante exibido, você pode ver todos os tipos de vulnerabilidades que foram tratadas. O número é apenas a quantidade de vulnerabilidades tratadas em um ano.
Detectable Vulnerabilities	Exibe o número de vulnerabilidades que podem ser detectadas pelo HSS.
Scans in Total	Exibe o número de verificações de vulnerabilidade. Clique em **Scan** para verificar manualmente as vulnerabilidades nos servidores.

- Visualização da importância dos ativos afetados por uma vulnerabilidade

  Na lista de vulnerabilidades na parte inferior da página, visualize a importância do ativo afetado por uma vulnerabilidade na coluna **Affected Servers**.

  - : principal ativo
  - : ativo menor
  - : ativo de teste
- Visualização de detalhes da vulnerabilidade

  Clique no nome de uma vulnerabilidade de destino. No painel deslizante de detalhes da vulnerabilidade exibido, é possível visualizar as sugestões de reparo, os detalhes de CVE, os servidores afetados e os registros históricos de tratamento da vulnerabilidade.
- Visualização de vulnerabilidades manipuladas ou vulnerabilidades a serem manipuladas

  Acima da lista de vulnerabilidades, selecione **Unhandled** ou **Handled** na lista suspensa de status de manipulação de vulnerabilidades para filtrar vulnerabilidades a serem manipuladas ou que foram manipuladas.
- Exportação da lista de vulnerabilidades

  Clique em **Export** acima da lista de vulnerabilidades para exportar dados de vulnerabilidade com apenas um clique. Em seguida, você pode visualizar as informações de vulnerabilidade em seu PC local.

  NOTA

  Um máximo de 30.000 vulnerabilidades podem ser exportadas por vez.

----Fim

Visualização de detalhes de vulnerabilidade (visualização do servidor)

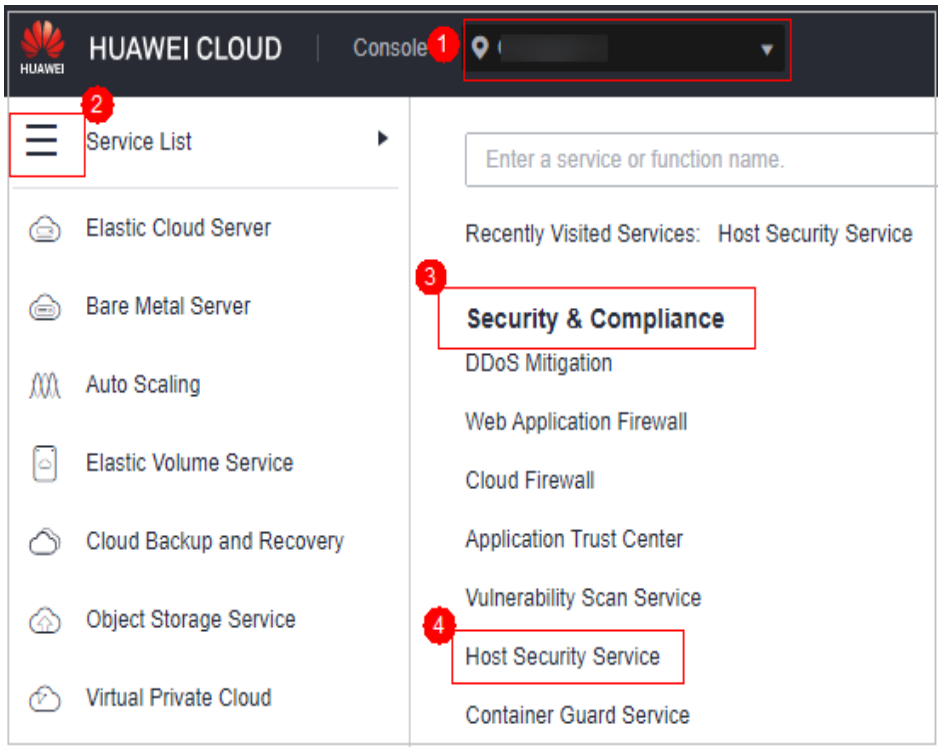
NOTA

A edição básica não suporta esta operação.

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**.

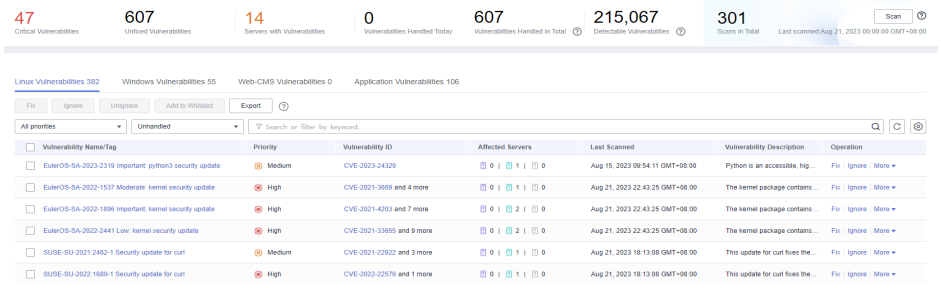
Figura 4-5 Acessar o HSS



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

Passo 4 No canto superior direito da página **Vulnerabilities**, clique em **Server view** para ver as informações sobre vulnerabilidades.

Figura 4-6 Visualização de detalhes da vulnerabilidade



- Visualização de resultados da verificação de vulnerabilidades

  Na área de estatísticas de vulnerabilidade na parte superior da página **Vulnerabilities**, visualize os resultados da verificação de vulnerabilidades. **Tabela 4-7** descreve os parâmetros relacionados.

Tabela 4-7 Parâmetros de verificação de vulnerabilidade

Parâmetro	Descrição
Critical vulnerabilities	Clique no número em **Critical vulnerabilities**. No painel deslizante exibido, você pode ver todos os tipos de vulnerabilidades a serem corrigidas com urgência.

Parâmetro	Descrição
Unfixed Vulnerabilities	Clique no número em **Unfixed Vulnerabilities**. No painel deslizante exibido, você pode visualizar todos os tipos de vulnerabilidades que não são corrigidas.
Servers with Vulnerabilities	Exibe o número de servidores com vulnerabilidades.
Vulnerabilities Handled Today	Clique no número em **Vulnerabilities Handled Today**. No painel deslizante exibido, você pode ver todos os tipos de vulnerabilidades que foram manipuladas hoje.
Vulnerabilities Handled in Total	Clique no número em **Vulnerabilities Handled in Total**. No painel deslizante exibido, você pode ver todos os tipos de vulnerabilidades que foram tratadas.
Detectable Vulnerabilities	Exibe o número de vulnerabilidades que podem ser detectadas pelo HSS.
Scans in Total	Exibe o número de verificações de vulnerabilidade. Clique em **Scan** para verificar manualmente as vulnerabilidades nos servidores.

- Visualização de detalhes do servidor e vulnerabilidades em servidores
  a. Clique no nome de um servidor de destino. No painel deslizante de detalhes do servidor exibido, você pode visualizar detalhes sobre o servidor e as vulnerabilidades no servidor.
  b. Clique no nome de uma vulnerabilidade de destino. No painel deslizante de detalhes da vulnerabilidade exibido, é possível visualizar os detalhes de CVE, os servidores afetados e os registros históricos de tratamento da vulnerabilidade.
- Visualização de vulnerabilidades manipuladas ou vulnerabilidades a serem manipuladas

  Acima da lista de vulnerabilidades, selecione **Unhandled** ou **Handled** na lista suspensa de status de manipulação de vulnerabilidades para filtrar vulnerabilidades a serem manipuladas ou que foram manipuladas.
- Exportação da lista de servidores com vulnerabilidades

  Clique em **Export** acima da lista de vulnerabilidades para exportar dados de vulnerabilidade com apenas um clique. Em seguida, você pode visualizar as informações de vulnerabilidade em seu PC local.

  NOTA

  Um máximo de 30.000 vulnerabilidades podem ser exportadas por vez.

----Fim

4.1.4 Manipulação de vulnerabilidades

- Vulnerabilidades do Linux ou Windows

  Você pode selecionar servidores e clicar em **Handle** para corrigir as vulnerabilidades ou corrigi-las manualmente com base nas sugestões fornecidas.

Em seguida, você pode usar a função de verificação para verificar rapidamente se a vulnerabilidade foi corrigida.

AVISO

Para corrigir vulnerabilidades do Windows, você precisa se conectar à Internet.

- Vulnerabilidades de Web-CMS

  Corrigi-las manualmente com base nas sugestões fornecidas na página.
- Vulnerabilidades de aplicações

  Corrigi-las manualmente com base nas sugestões fornecidas na página.

Restrições

- Os servidores que não são protegidos ou protegidos pela edição básica não suportam esta função.
- O **Server Status** está **Running**, **Agent Status** está **Online** e **Protection Status** está **Protected**.

Precauções

- As operações de correção de vulnerabilidades não podem ser revertidas. Se uma vulnerabilidade não for corrigida, os serviços provavelmente serão interrompidos e problemas de incompatibilidade provavelmente ocorrerão em middleware ou aplicações de camada superior. Para evitar consequências inesperadas, é recomendável usar o CSBS para fazer backup de ECSs. Para obter detalhes, consulte **Criação de um backup do CSBS**. Em seguida, use servidores ociosos para simular o ambiente de produção e testar a correção da vulnerabilidade. Se a correção de teste for bem-sucedida, corrija a vulnerabilidade em servidores em execução no ambiente de produção.
- Os servidores precisam acessar a Internet e usar fontes externas de imagem para corrigir vulnerabilidades. Se seus servidores não puderem acessar a Internet ou as fontes externas de imagem não puderem fornecer serviços estáveis, você poderá usar a fonte de imagem fornecida pela HUAWEI CLOUD para corrigir vulnerabilidades.

  Antes de corrigir vulnerabilidades on-line, configure as fontes de imagem da Huawei Cloud que correspondem aos seus SOs de servidor. Para obter detalhes, consulte **Gerenciamento da fonte de imagens**.

Prioridade de correção de vulnerabilidades

O sistema de verificação de vulnerabilidades do HSS classifica as prioridades de correção de vulnerabilidades em quatro níveis: crítico, alto, médio e baixo. Você pode consultar as prioridades para corrigir as vulnerabilidades que têm impacto significativo no seu servidor primeiro.

- **Critical**: essa vulnerabilidade deve ser corrigida imediatamente. Os atacantes podem explorar esta vulnerabilidade para causar grandes danos ao servidor.
- **High**: essa vulnerabilidade deve ser corrigida o mais rápido possível. Os atacantes podem explorar esta vulnerabilidade para danificar o servidor.
- **Medium**: é aconselhável corrigir a vulnerabilidade para melhorar a segurança do seu servidor.

- **Low**: esta vulnerabilidade tem uma pequena ameaça à segurança do servidor. Você pode optar por corrigi-la ou ignorá-la.

Exibição de vulnerabilidades

As vulnerabilidades detectadas serão exibidas na lista de vulnerabilidades por sete dias, independentemente de você ter lidado com elas.

Correção automática de vulnerabilidades (visualização de vulnerabilidades)

Você só pode corrigir vulnerabilidades do Linux e do Windows com um clique no console.

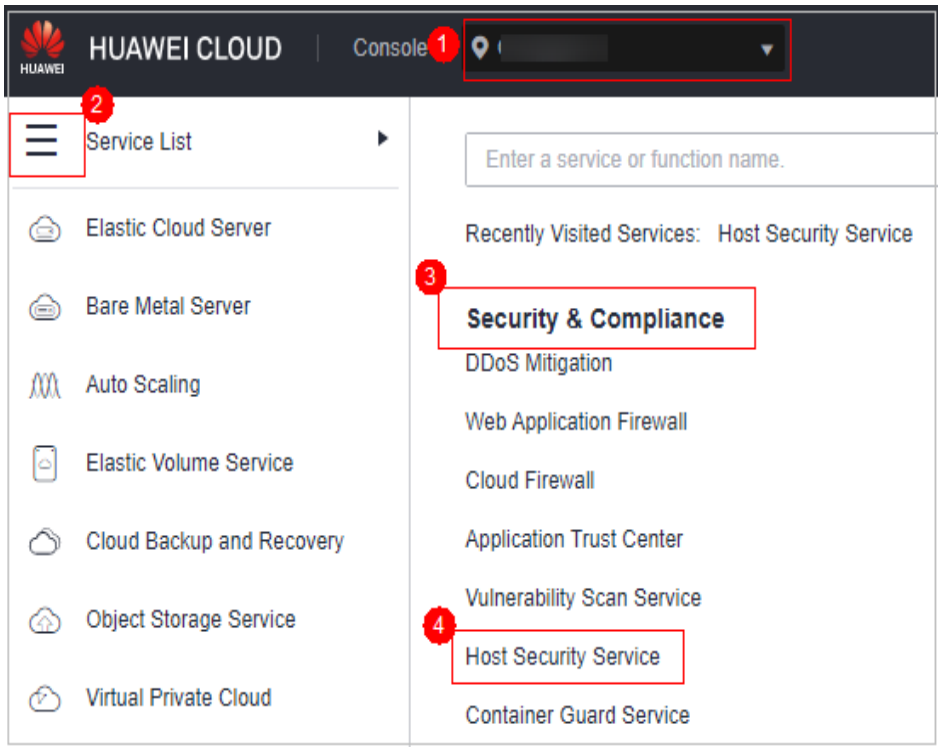
NOTA

Um máximo de 1.000 vulnerabilidades de servidor podem ser corrigidas por vez. Se houver mais de 1.000 vulnerabilidades, corrija-as em lotes.

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 4-7 Acessar o HSS



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

Passo 4 Na página **Vulnerabilities** exibida, localize as vulnerabilidades que você deseja corrigir e corrija os servidores com as vulnerabilidades.

- Correção de todos os servidores afetados por uma vulnerabilidade

  Localize a linha que contém uma vulnerabilidade de destino e clique em **Fix** na coluna **Operation**. Como alternativa, você pode selecionar todas as vulnerabilidades de destino

e clicar em **Fix** no canto superior esquerdo da lista de vulnerabilidades para corrigir vulnerabilidades em lotes.

- Corrigir um ou mais servidores afetados por uma vulnerabilidade

  a. Clique em um nome de vulnerabilidade.

  b. No painel deslizante de detalhes da vulnerabilidade exibido, clique na guia **Affected**, localize a linha que contém o servidor de destino e clique em **Fix** na coluna **Operation**.

     Você também pode selecionar todos os servidores de destino e clicar em **Fix** acima da lista de servidores para corrigir vulnerabilidades para os servidores em lotes.

Passo 5 Na caixa de diálogo **Fix** exibida, selecione **I am aware that if I have not backed up my ECSs before fixing vulnerabilities, services may be interrupted and fail to be rolled back during maintenance.** e clique em **Auto Fix**.

Para corrigir todas as vulnerabilidades do Linux ou do Windows, selecione **Select all Linux vulnerabilities** ou **Select all Windows vulnerabilities** na caixa de diálogo **Fix**.

Passo 6 Clique em um nome de vulnerabilidade.

Passo 7 Clique na guia **Handling History** para exibir o status de correção da vulnerabilidade de destino na coluna **Status**. Tabela 4-8 descreve os status de correção de vulnerabilidade.

Tabela 4-8 Status de correção de vulnerabilidade

Status	Descrição
Unhandled	A vulnerabilidade não é corrigida.
Ignored	A vulnerabilidade não afeta seus serviços. Você ignorou a vulnerabilidade.
Verifying	O HSS está verificando se uma vulnerabilidade corrigida foi corrigida com sucesso.
Fixing	O HSS está corrigindo a vulnerabilidade.
Fixed	A vulnerabilidade foi corrigida com sucesso.
Restart required	A vulnerabilidade foi corrigida com sucesso. Você precisa reiniciar o servidor o mais rápido possível.
Failed	A vulnerabilidade não pode ser corrigida. A possível causa é que a vulnerabilidade não existe ou foi alterada.
Restart the server and try again	Esse status é exibido apenas para vulnerabilidades que existem em servidores do Windows. A vulnerabilidade não foi corrigida no servidor do Windows por um longo tempo. Como resultado, o patch mais recente não pode ser instalado. Você precisa instalar um patch anterior, reiniciar o servidor e, em seguida, instalar o patch mais recente.

----Fim

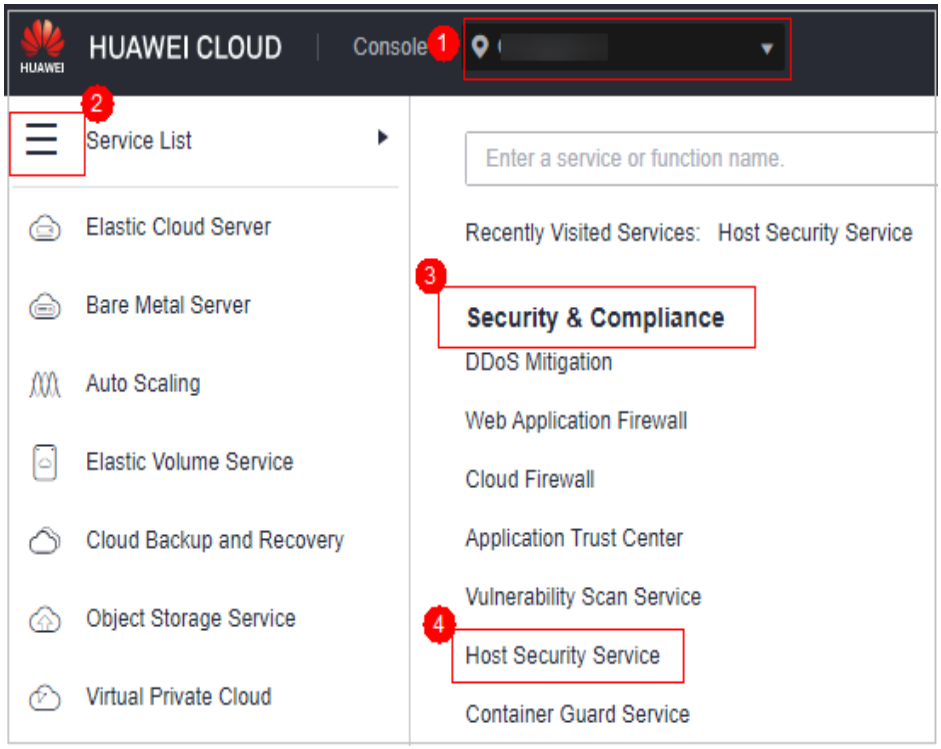
Correção automática de vulnerabilidades (visualização do servidor)

Você só pode corrigir vulnerabilidades do Linux e do Windows com um clique 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 4-8 Acessar o HSS



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

Passo 4 Corrija a vulnerabilidade de um servidor de destino.

- Corrigir todas as vulnerabilidades em um servidor
  a. Localize a linha que contém um servidor de destino e clique em **Fix** na coluna **Operation**.
  b. Na caixa de diálogo **Fix** exibida, selecione o tipo de vulnerabilidade a ser corrigida, selecione **I am aware that if I have not backed up my ECSs before fixing vulnerabilities, services may be interrupted and fail to be rolled back during maintenance.** e clique em **OK**.

     Somente as vulnerabilidades do Linux e do Windows podem ser corrigidas automaticamente com um clique. As vulnerabilidades de Web-CMS e aplicação precisam ser corrigidas manualmente fazendo logon no servidor.
  c. Clique no nome do servidor. No painel deslizante de detalhes do servidor exibido, visualize o status da correção de vulnerabilidade. **Tabela 4-9** descreve os status de correção de vulnerabilidade.
- Corrigir uma ou mais vulnerabilidades em um servidor

a. Clique no nome de um servidor de destino. O painel deslizante de detalhes do servidor é exibido.

b. Localize a linha que contém uma vulnerabilidade de destino e clique em **Fix** na coluna **Operation**.

   Como alternativa, você pode selecionar todas as vulnerabilidades de destino e clicar em **Fix** acima da lista de vulnerabilidades para corrigir vulnerabilidades em lotes.

c. Na caixa de diálogo **Fix** exibida, selecione **I am aware that if I have not backed up my ECSs before fixing vulnerabilities, services may be interrupted and fail to be rolled back during maintenance.** e clique em **Auto Fix**.

d. Na coluna **Status** da vulnerabilidade de destino, exiba o status de correção da vulnerabilidade. **Tabela 4-9** descreve os status de correção de vulnerabilidade.

Tabela 4-9 Status de correção de vulnerabilidade

Status	Descrição
Unhandled	A vulnerabilidade não é corrigida.
Ignored	A vulnerabilidade não afeta seus serviços. Você ignorou a vulnerabilidade.
Verifying	O HSS está verificando se uma vulnerabilidade corrigida foi corrigida com sucesso.
Fixing	O HSS está corrigindo a vulnerabilidade.
Fixed	A vulnerabilidade foi corrigida com sucesso.
Restart required	A vulnerabilidade foi corrigida com sucesso. Você precisa reiniciar o servidor o mais rápido possível.
Failed	A vulnerabilidade não pode ser corrigida. A possível causa é que a vulnerabilidade não existe ou foi alterada.
Restart the server and try again	Esse status é exibido apenas para vulnerabilidades que existem em servidores do Windows. A vulnerabilidade não foi corrigida no servidor do Windows por um longo tempo. Como resultado, o patch mais recente não pode ser instalado. Você precisa instalar um patch anterior, reiniciar o servidor e, em seguida, instalar o patch mais recente.

----Fim

Corrigir manualmente as vulnerabilidades

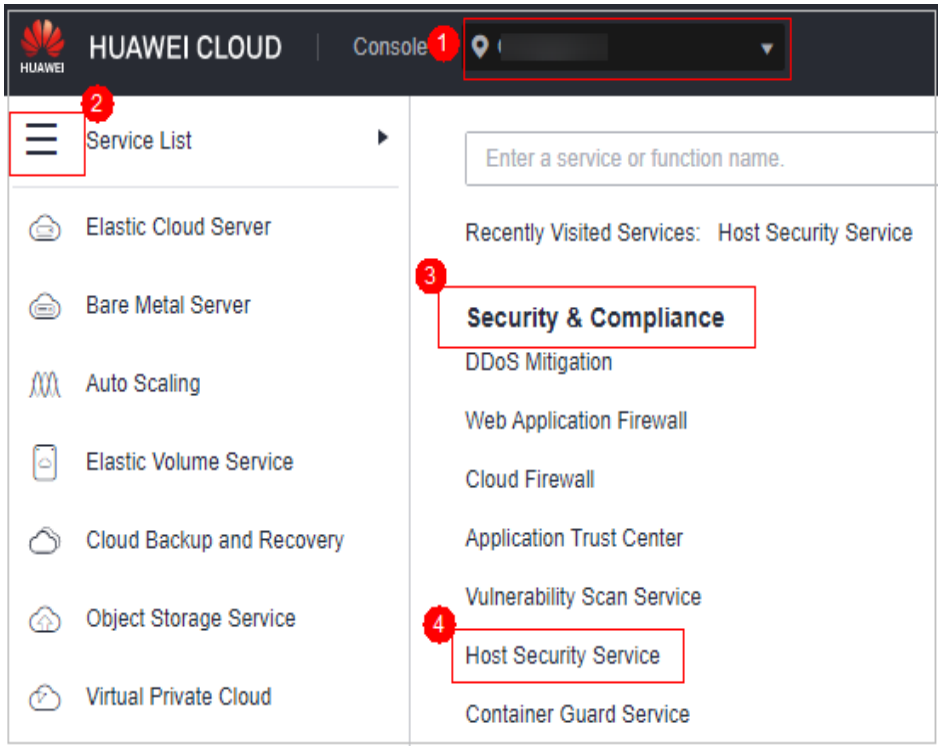
O HSS não corrige automaticamente as vulnerabilidades de Web-CMS ou aplicação com um clique. Você pode fazer logon no servidor para corrigi-las manualmente consultando as sugestões de correção no painel deslizante de detalhes da vulnerabilidade.

Visualização de sugestões de correção de vulnerabilidade

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 4-9 Acessar o HSS



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

Passo 4 Clique no nome de uma vulnerabilidade de destino para acessar o painel deslizante de detalhes da vulnerabilidade e visualizar as sugestões de correção.

----Fim

Corrigir vulnerabilidades referindo-se a sugestões de correção de vulnerabilidades

A correção de vulnerabilidade pode afetar a estabilidade do serviço. Você é aconselhado a usar um dos seguintes métodos para evitar esse impacto:

- Método 1: criar uma nova VM para corrigir a vulnerabilidade.
  a. Crie uma imagem para que o ECS seja corrigido. Para obter detalhes, consulte **Criação de uma imagem de ECS completa usando um ECS**.
  b. Use a imagem para criar um ECS. Para obter detalhes, consulte **Criação de ECSs usando uma imagem**.
  c. Corrija a vulnerabilidade no novo ECS e verifique o resultado.
  d. Mude os serviços para o novo ECS e verifique se eles estão funcionando de forma estável.
  e. Libere o ECS original. Se ocorrer uma falha após a alternância de serviço e não puder ser corrigida, você poderá alternar os serviços de volta para o ECS original.
- Método 2: corrigir a vulnerabilidade no servidor de destino.
  a. Crie um backup para o ECS cujas vulnerabilidades precisam ser corrigidas. Para obter detalhes, consulte **Criação de um backup do CSBS**.

b. Corrija vulnerabilidades no servidor atual.

c. Se os serviços ficarem indisponíveis depois que a vulnerabilidade for corrigida e não puder ser recuperada em tempo hábil, use o backup para restaurar o servidor. Para obter detalhes, consulte **Uso de backups para restaurar servidores**.

NOTA

- Use o método 1 se você estiver corrigindo uma vulnerabilidade pela primeira vez e não puder estimar o impacto nos serviços. É aconselhável escolher o modo de cobrança de pagamento por uso para o ECS recém-criado. Após a mudança de serviço, você pode alterar o modo de cobrança para anual/mensal. Dessa forma, você pode liberar o ECS a qualquer momento para economizar custos se a vulnerabilidade não for corrigida.
- Use o método 2 se você já tiver corrigido a vulnerabilidade em servidores semelhantes anteriormente.

Ignorar vulnerabilidades

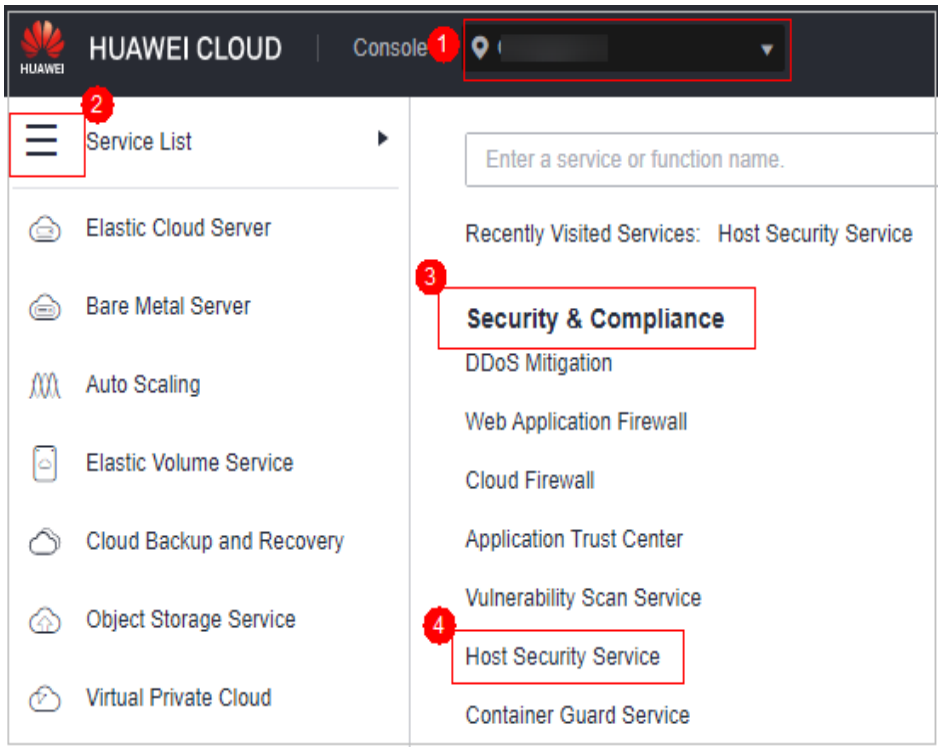
Algumas vulnerabilidades são arriscadas apenas em condições específicas. Por exemplo, se uma vulnerabilidade puder ser explorada apenas por meio de uma porta aberta, mas o servidor de destino não abrir nenhuma porta, a vulnerabilidade não prejudicará o servidor. Tais vulnerabilidades podem ser ignoradas.

Alarmes não serão gerados pelo HSS para vulnerabilidades ignoradas.

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 4-10 Acessar o HSS



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

Passo 4 Localize a linha que contém uma vulnerabilidade de destino e clique em **Ignore** na coluna **Operation**.

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

----Fim

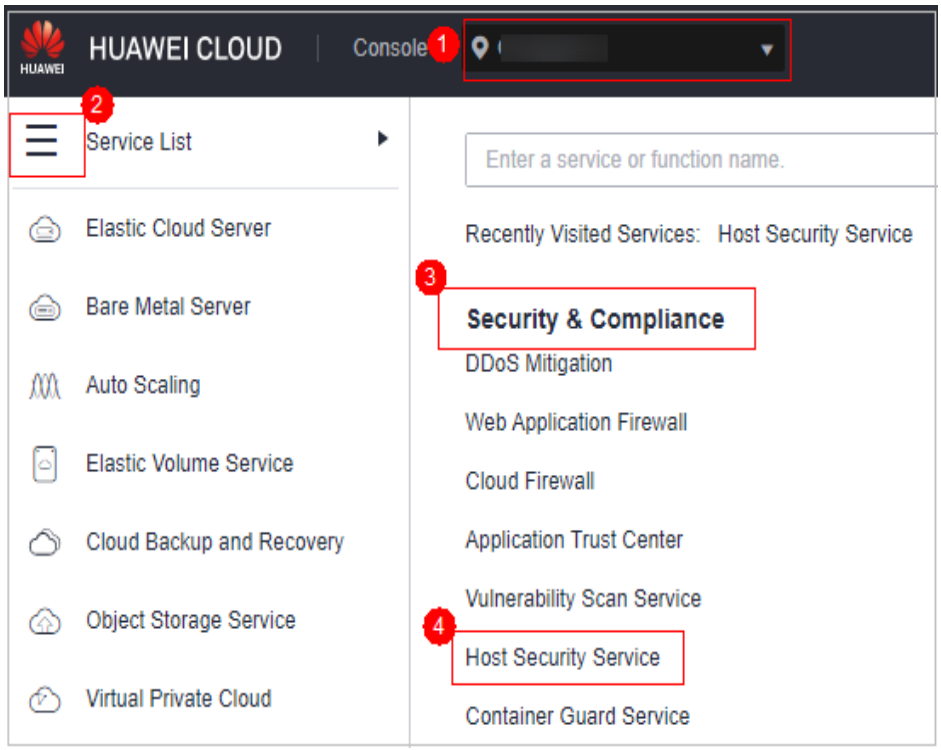
Colocar vulnerabilidades na lista branca

Se você avaliar que algumas vulnerabilidades não afetam seus serviços e não deseja visualizar as vulnerabilidades na lista de vulnerabilidades, poderá colocar as vulnerabilidades na lista branca. Depois que forem colocadas na lista branca, as vulnerabilidades serão ignoradas na lista de vulnerabilidades e nenhum alarme será relatado. As vulnerabilidades não serão verificadas e as informações de vulnerabilidade não serão exibidas quando a próxima tarefa de verificação de vulnerabilidade for executada.

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 4-11 Acessar o HSS



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

- Colocar na lista branca todos os servidores afetados por uma vulnerabilidade

  O HSS ignorará a vulnerabilidade ao fazer a verificação de vulnerabilidades em todos os servidores.

  a. Na coluna **Operation** da linha que contém a vulnerabilidade de destino, clique em **More** e selecione **Add to Whitelist**.

Você também pode selecionar várias vulnerabilidades e clicar em **Add to Whitelist** acima da lista de vulnerabilidades.

Figura 4-12 Colocar na lista branca todos os servidores afetados por uma vulnerabilidade

b. Na caixa de diálogo exibida, clique em **OK**.

- Colocar na lista branca um ou mais servidores afetados por uma vulnerabilidade

  O HSS ignorará a vulnerabilidade ao fazer a verificação de vulnerabilidades nesses servidores.

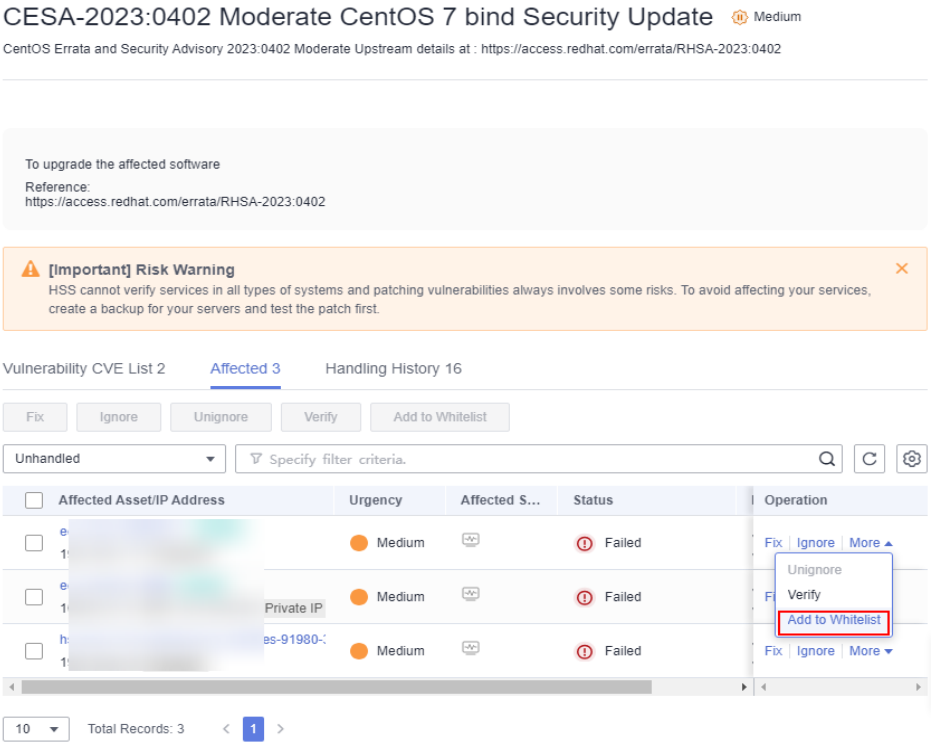
  a. Clique em um nome de vulnerabilidade de destino.

  b. No painel deslizante exibido, clique na guia **Affected**.

  c. Na coluna **Operation** da linha que contém o servidor de destino, clique em **More** e selecione **Add to Whitelist**.

  Você também pode selecionar vários servidores e clicar em **Add to Whitelist** acima da lista de servidores.

Figura 4-13 Colocar na lista branca um único servidor afetado por uma vulnerabilidade



d. Na caixa de diálogo exibida, clique em **OK**.

- Colocar vulnerabilidades na lista branca usando regras de lista branca

a. No canto superior direito da página **Vulnerabilities**, clique em **Configure Policy**. O painel deslizante **Configure Policy** é exibido.

b. Na área **Vulnerability Whitelist**, clique em **Add Rule**.

c. Configure uma regra de lista branca de acordo com **Tabela 4-10**.

Figura 4-14 Configuração de uma regra de lista branca

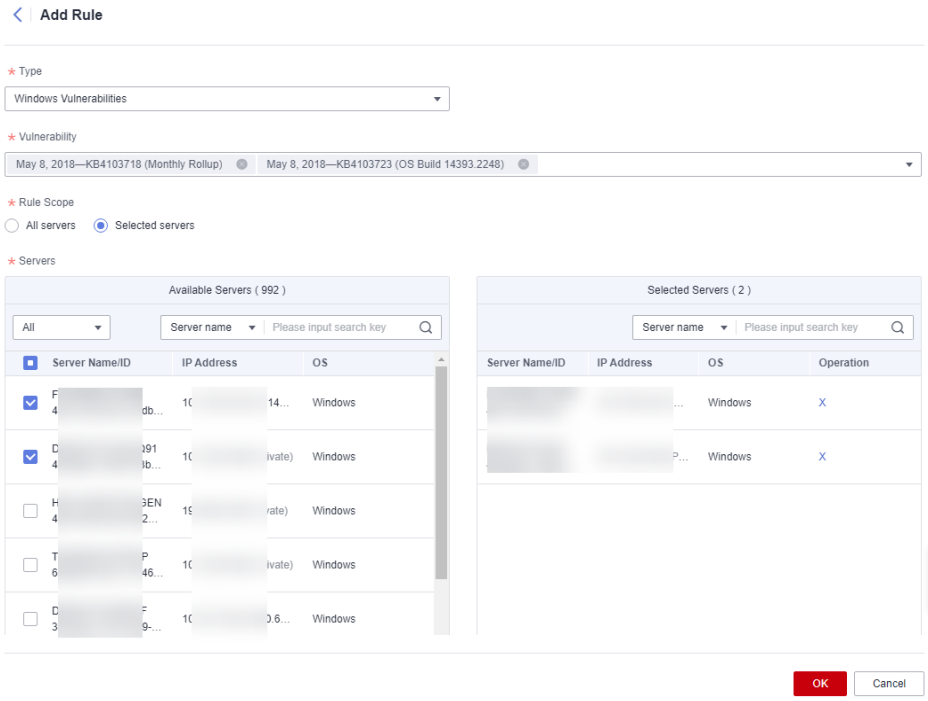


Tabela 4-10 Parâmetros de regra de lista branca de vulnerabilidade

Parâmetro	Descrição
Type	Selecione o tipo de vulnerabilidades a serem colocadas na lista branca. Os valores possíveis são os seguintes: ■ **Linux Vulnerabilities** ■ **Windows Vulnerabilities** ■ **Web-CMS Vulnerabilities** ■ **Application Vulnerabilities**
Vulnerability	Selecione uma ou mais vulnerabilidades a serem incluídas na lista branca.

Parâmetro	Descrição
Rule Scope	Selecione os servidores afetados pelas vulnerabilidades. Os valores possíveis são os seguintes: ■ **All servers** O HSS ignorará a vulnerabilidade ao fazer a verificação de vulnerabilidades em todos os servidores. ■ **Selected servers** Selecione um ou mais servidores de destino. O HSS ignorará as vulnerabilidades ao fazer a verificação de vulnerabilidades nesses servidores. Você pode procurar um servidor de destino por nome de servidor, ID, EIP ou endereço IP privado.
Remarks (Optional)	Digite as observações.

d. Clique em **OK**.

----Fim

Verificar a correção de vulnerabilidade

Depois que uma vulnerabilidade é corrigida, é aconselhável verificá-la imediatamente.

Verificação manual

- Clique em **Verify** na página de detalhes da vulnerabilidade.
- Certifique-se de que o software foi atualizado para a versão mais recente. A tabela a seguir fornece os comandos para verificar o resultado da atualização do software.

Tabela 4-11 Comandos de verificação

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

- **Verifique manualmente se há vulnerabilidades** e visualize os resultados da correção de vulnerabilidades.

Verificação automática

O HSS realiza uma verificação completa todas as manhãs. Se você não realizar uma verificação manual, poderá visualizar o resultado da verificação do sistema no dia seguinte após corrigir a vulnerabilidade.

4.1.5 Gerenciamento da lista branca de vulnerabilidades

Se você avaliar que algumas vulnerabilidades não afetam seus serviços e não deseja exibir as vulnerabilidades na lista de vulnerabilidades, poderá colocar as vulnerabilidades na lista branca. Depois que forem colocadas na lista branca, as vulnerabilidades serão ignoradas na lista de vulnerabilidades e nenhum alarme será relatado. As vulnerabilidades não serão verificadas e as informações de vulnerabilidade não serão exibidas quando a próxima tarefa de verificação de vulnerabilidade for executada.

Esta seção descreve como colocar uma vulnerabilidade na lista branca, modificar uma regra de lista branca de vulnerabilidades e remover uma regra de lista branca de vulnerabilidades da lista branca de vulnerabilidades.

Restrições

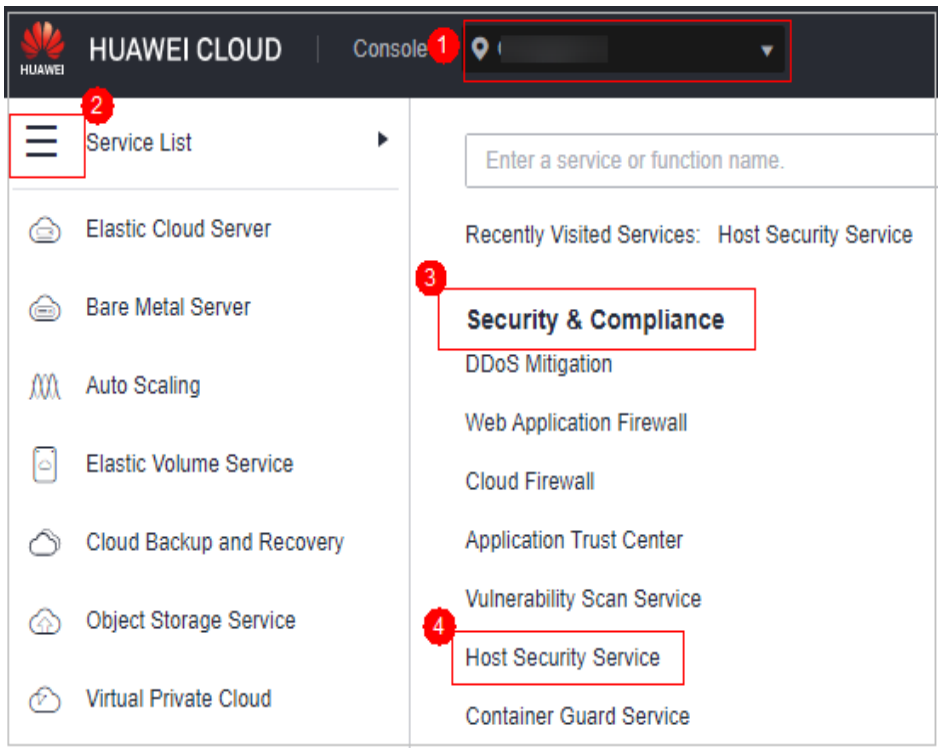
A edição básica não suporta esta função. Para obter detalhes sobre como comprar e atualizar o HSS, consulte **Compra de uma cota do HSS** e **Atualização de sua edição**.

Colocar vulnerabilidades na lista branca

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 4-15 Acessar o HSS



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

- Colocar na lista branca todos os servidores afetados por uma vulnerabilidade

O HSS ignorará a vulnerabilidade ao fazer a verificação de vulnerabilidades em todos os servidores.

a. Na coluna **Operation** da linha que contém a vulnerabilidade de destino, clique em **More** e selecione **Add to Whitelist**.

   Você também pode selecionar várias vulnerabilidades e clicar em **Add to Whitelist** acima da lista de vulnerabilidades.

   Figura 4-16 Colocar na lista branca todos os servidores afetados por uma vulnerabilidade

b. Na caixa de diálogo exibida, clique em **OK**.

- Colocar na lista branca um ou mais servidores afetados por uma vulnerabilidade

  O HSS ignorará a vulnerabilidade ao fazer a verificação de vulnerabilidades nesses servidores.

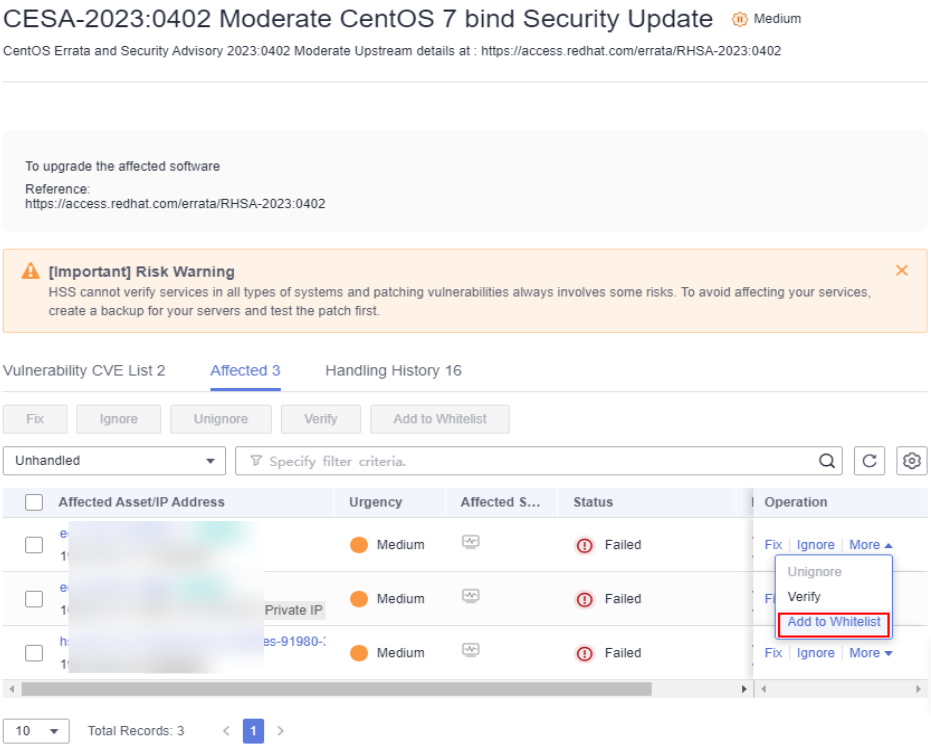
  a. Clique em um nome de vulnerabilidade de destino.

  b. No painel deslizante exibido, clique na guia **Affected**.

  c. Na coluna **Operation** da linha que contém o servidor de destino, clique em **More** e selecione **Add to Whitelist**.

     Você também pode selecionar vários servidores e clicar em **Add to Whitelist** acima da lista de servidores.

     Figura 4-17 Colocar na lista branca um único servidor afetado por uma vulnerabilidade



d. Na caixa de diálogo exibida, clique em **OK**.

- Colocar vulnerabilidades na lista branca usando regras de lista branca

a. No canto superior direito da página **Vulnerabilities**, clique em **Configure Policy**. O painel deslizante **Configure Policy** é exibido.

b. Na área **Vulnerability Whitelist**, clique em **Add Rule**.

c. Configure uma regra de lista branca de acordo com **Tabela 4-12**.

Figura 4-18 Configuração de uma regra de lista branca

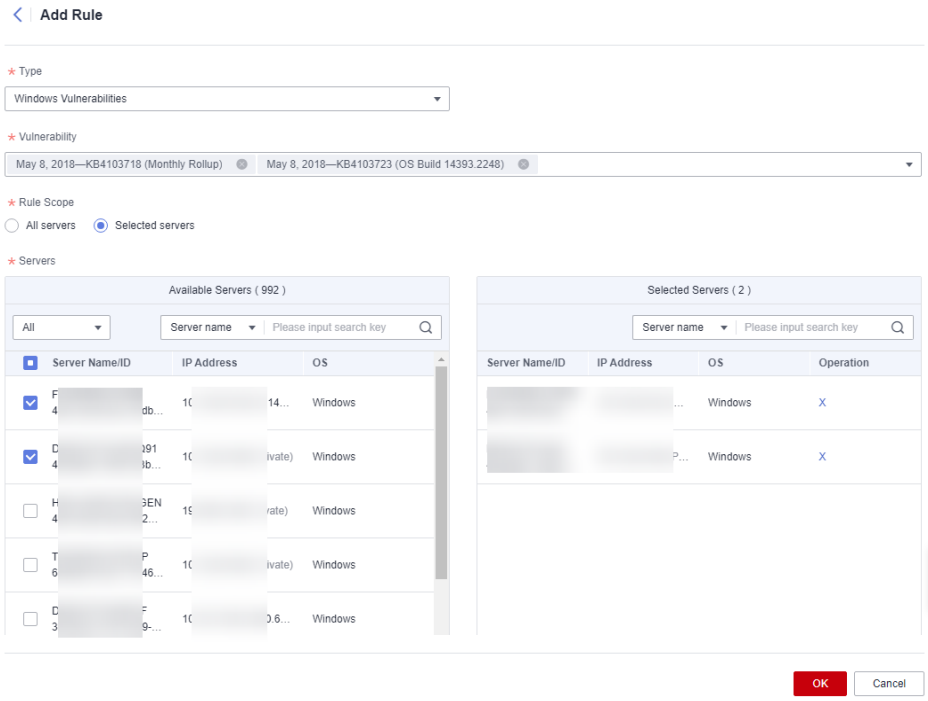


Tabela 4-12 Parâmetros de regra de lista branca de vulnerabilidade

Parâmetro	Descrição
Type	Selecione o tipo de vulnerabilidades a serem colocadas na lista branca. Os valores possíveis são os seguintes: ■ **Linux Vulnerabilities** ■ **Windows Vulnerabilities** ■ **Web-CMS Vulnerabilities** ■ **Application Vulnerabilities**
Vulnerability	Selecione uma ou mais vulnerabilidades a serem incluídas na lista branca.

Parâmetro	Descrição
Rule Scope	Selecione os servidores afetados pelas vulnerabilidades. Os valores possíveis são os seguintes: ■ **All servers** O HSS ignorará a vulnerabilidade ao fazer a verificação de vulnerabilidades em todos os servidores. ■ **Selected servers** Selecione um ou mais servidores de destino. O HSS ignorará as vulnerabilidades ao fazer a verificação de vulnerabilidades nesses servidores. Você pode procurar um servidor de destino por nome de servidor, ID, EIP ou endereço IP privado.
Remarks (Optional)	Digite as observações.

d. Clique em **OK**.

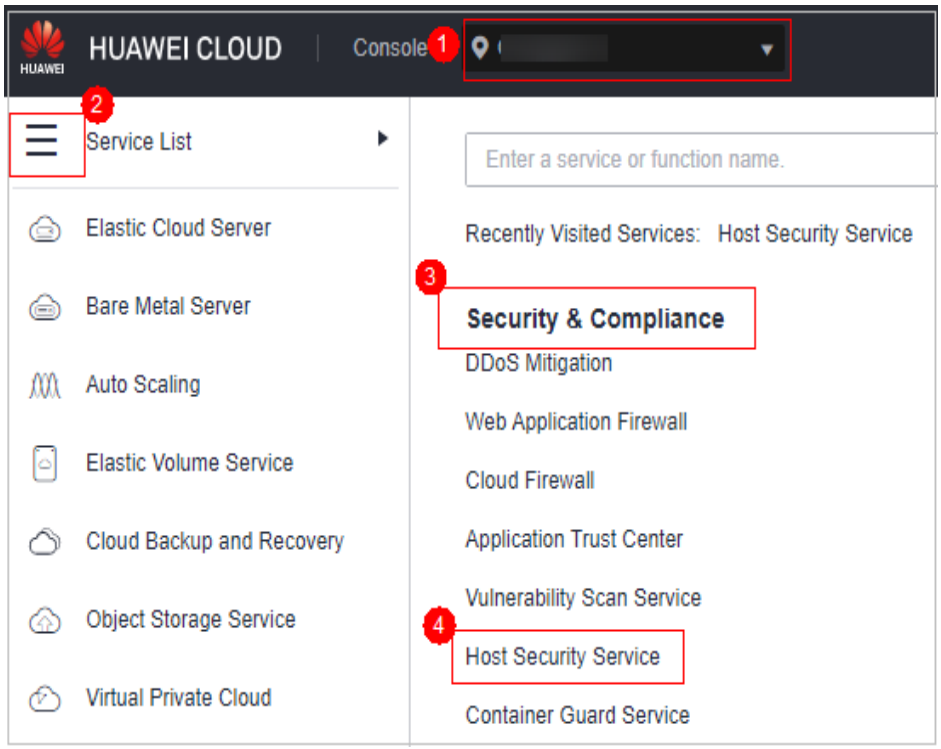
----Fim

Editar uma lista branca 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 4-19 Acessar o HSS



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

Passo 4 No canto superior direito da página **Vulnerabilities**, clique em **Configure Policy**. O painel deslizante **Configure Policy** é exibido.

Passo 5 Na linha que contém a regra da lista branca de vulnerabilidades desejada, clique em **Edit** na coluna **Operation**.

Passo 6 Na página de edição, modifique as informações e clique em **OK**.

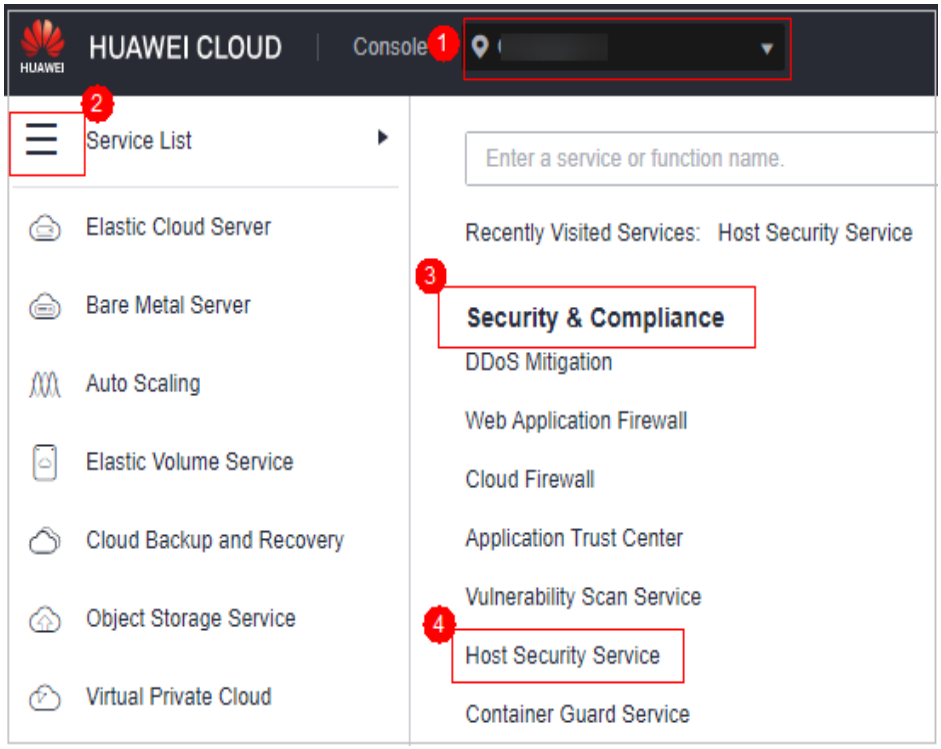
----Fim

Remover uma regra de lista branca de vulnerabilidades da lista branca 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 4-20 Acessar o HSS



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

Passo 4 No canto superior direito da página **Vulnerabilities**, clique em **Configure Policy**. O painel deslizante **Configure Policy** é exibido.

Passo 5 Na linha que contém a regra da lista branca de vulnerabilidades desejada, clique em **Delete** na coluna **Operation**.

Passo 6 Na caixa de diálogo exibida, confirme as informações e clique em **OK**.

----Fim

4.1.6 Visualização do histórico de tratamento de vulnerabilidades

Para vulnerabilidades que foram tratadas, você pode consultar esta seção para visualizar o histórico de tratamento de vulnerabilidades (manipulador e tempo de tratamento).

Restrições

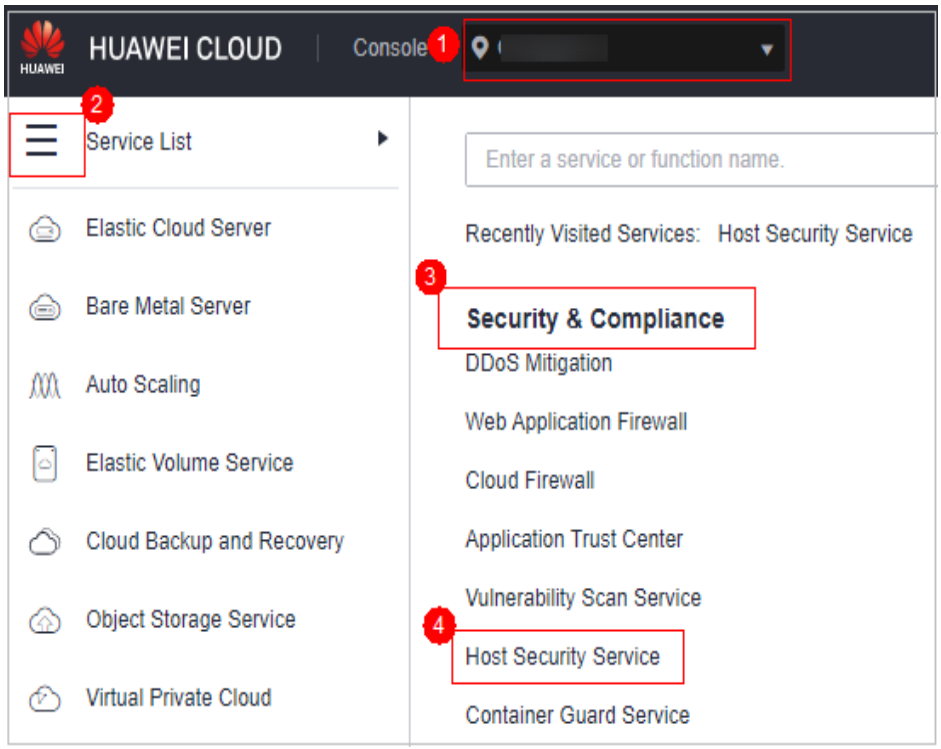
A edição básica não suporta esta função. Para obter detalhes sobre como comprar e atualizar o HSS, consulte **Compra de uma cota do HSS** e **Atualização de sua edição**.

Visualização do histórico de tratamento de uma vulnerabilidade

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**.

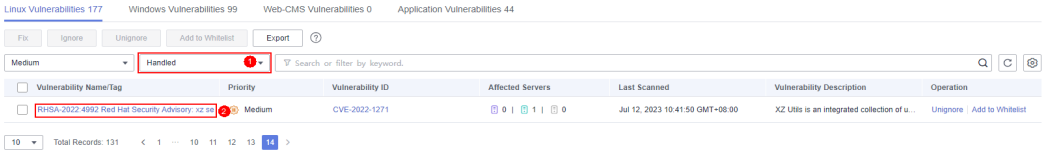
Figura 4-21 Acessar o HSS



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

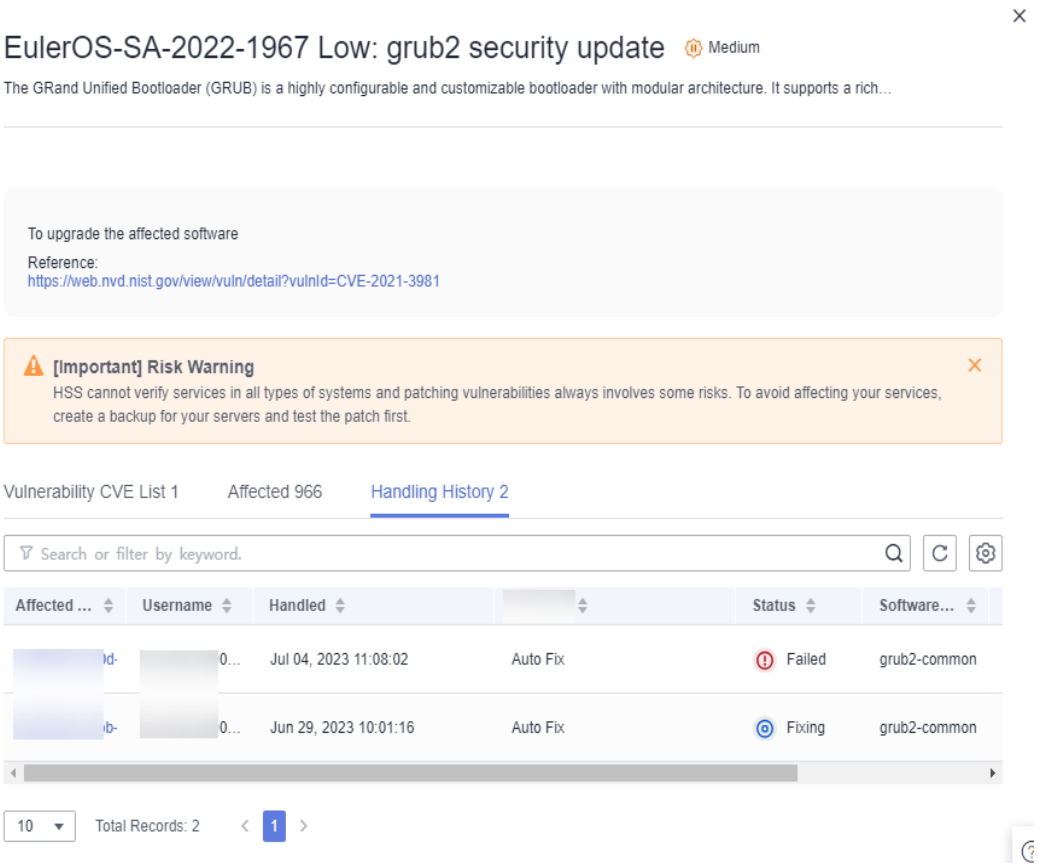
Passo 4 Na lista de vulnerabilidades tratadas, clique em um nome de vulnerabilidade. O painel deslizante de detalhes da vulnerabilidade é exibido.

Figura 4-22 Selecionar Handled na lista suspensa



Passo 5 Clique na guia **Handling History** para visualizar o histórico de tratamento da vulnerabilidade.

Figura 4-23 Histórico de tratamento



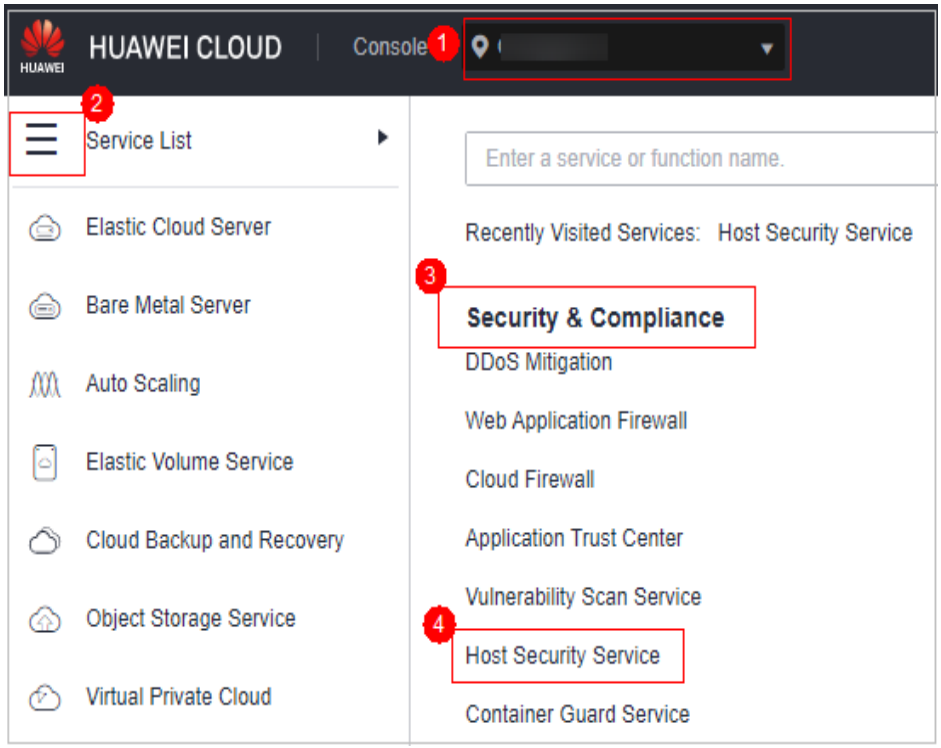
----Fim

Visualização do histórico de tratamento de todas as 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 4-24 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Security Operations** > **Handling History**. A página **Handling History** é exibida.

Passo 4 Na página de guia **Vulnerabilities** exibida, visualize o histórico de tratamento de todas as vulnerabilidades.

- Visualização do histórico de tratamento de vulnerabilidades de um projeto empresarial especificado

  No canto superior esquerdo da página **Handling History**, selecione um projeto empresarial para **Enterprise Project** para visualizar o histórico de tratamento de vulnerabilidades do servidor no projeto empresarial.

- Visualização do histórico de tratamento de vulnerabilidades de uma propriedade especificada

  Na caixa de pesquisa acima da lista de histórico de tratamento de vulnerabilidades, digite um tipo de vulnerabilidade, nome de vulnerabilidade ou endereço IP do servidor e clique em para visualizar o histórico de tratamento de vulnerabilidades de uma propriedade especificada.

----Fim

4.2 Inspeção de linha de base

4.2.1 Visão geral da verificação da linha de base

O HSS detecta políticas complexas, senhas fracas e detalhes de configuração, incluindo a taxa de configurações seguras, os 5 principais servidores com configurações inseguras, os servidores com senhas fracas e os 5 principais servidores com senhas fracas. O HSS verifica

proativamente políticas de complexidade de senha fraca e outras configurações inseguras e fornece **sugestões** para corrigir riscos detectados.

Restrições

Os servidores que não estão protegidos pelo HSS não suportam operações relacionadas com a linha de base.

Pré-requisito

Somente os servidores protegidos pela edição empresarial ou superior são verificados.

Métodos de verificação

- Verificação automática

  O HSS realiza automaticamente uma verificação abrangente às 04:00 todos os dias. Se você quiser personalizar o período e o tempo de verificação automática da linha de base, poderá ativar as edições premium, WTP e de container. Para mais detalhes, consulte **Verificação de configuração**.

- Verificação manual

  Para exibir os riscos de linha de base de um servidor especificado, você pode **criar uma política de verificação de linha de base** para esses servidores. No canto superior direito da página **Baseline Checks**, selecione uma política e clique em **Scan**. Depois que a verificação manual da linha de base for concluída, você poderá visualizar os riscos da linha de base dos servidores especificados.

Itens de verificação

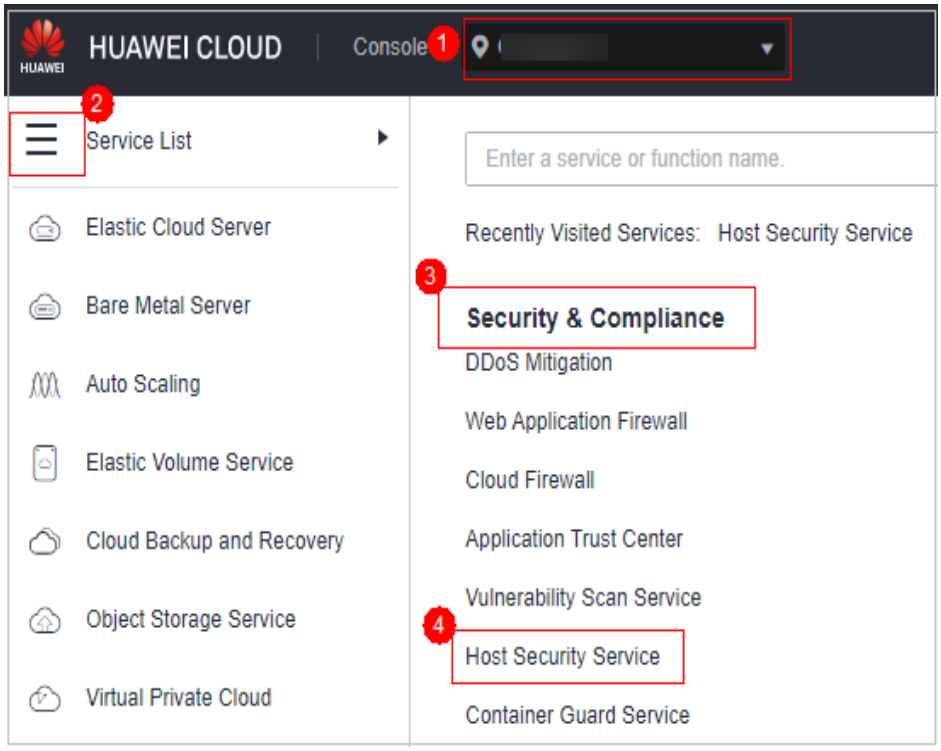
Item	Descrição
Password Complexity Policy Detection	Verificar as políticas de complexidade de senha e modificar-as com base nas sugestões fornecidas pelo HSS para melhorar a segurança da senha.
Common Weak Password Detection	Alterar senhas fracas para senhas mais fortes com base nos resultados e sugestões da verificação do HSS.
Unsafe Configurations	Verifique as configurações inseguras de logon do Tomcat, Nginx e SSH encontradas pelo HSS.

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 4-25 Acessar o HSS



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

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 Clique em diferentes guias na página exibida para verificar as configurações inseguras detectadas. **Tabela 4-13** lista os parâmetros correspondentes.

Para visualizar os resultados de verificação de servidores sob diferentes políticas de verificação de linha de base, você pode alternar entre as políticas de verificação de linha de base.

Figura 4-26 Visão geral da verificação da linha de base

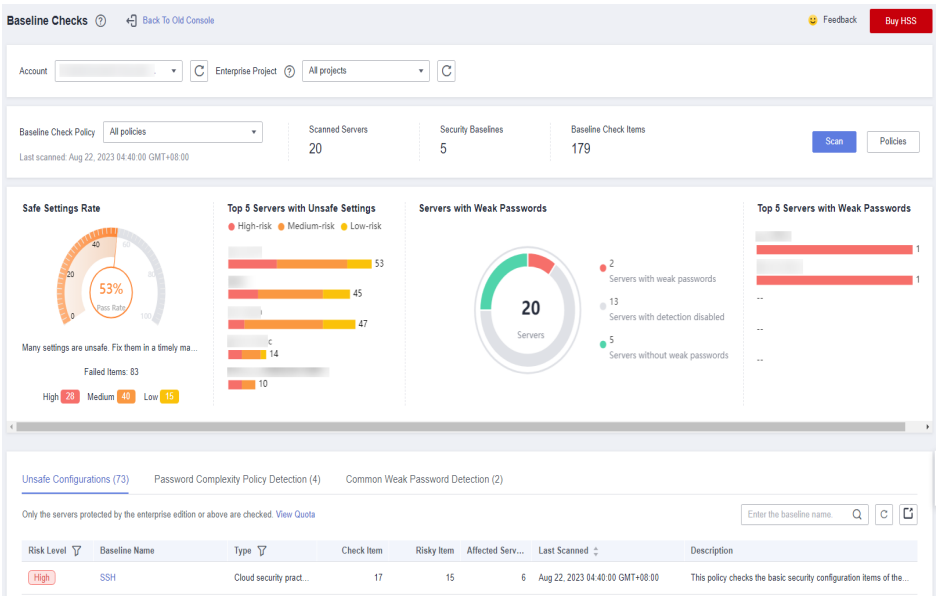


Tabela 4-13 Visão geral da verificação da linha de base

Parâmetro	Descrição
Baseline Check Policy	Políticas de verificação de linha de base disponíveis que foram adicionadas. Você pode selecionar, criar, editar e excluir essas políticas.
Scanned Servers	Número total de servidores detectados.
Security Baselines	Número de linhas de base executadas durante a detecção do servidor.
Baseline Check Items	Número total de itens de configuração do servidor verificados.
Safe Settings Rate	Porcentagem de itens de configuração que passaram pela verificação de linha de base para o número total de itens de verificação. Os itens com falha são exibidos por nível de risco.
Top 5 Servers with Unsafe Settings	Estatísticas em servidores com riscos de configuração de servidores. Os 5 principais servidores com os maiores riscos são classificados preferencialmente. Se não houver configurações de alto risco, os servidores são classificados em médio risco e baixo risco em sequência.
Servers with Weak Passwords	Número total de servidores detectados, bem como o número de servidores com senhas fracas, aqueles sem senhas fracas e aqueles com detecção de senha fraca desativada.
Top 5 Servers with Weak Passwords	Estatísticas sobre os 5 principais servidores com riscos de senha mais fracos.
Unsafe Configurations	Alarmes gerados para servidores com riscos de configuração e estatísticas de risco.

Parâmetro	Descrição
Password Complexity Policy Detection	Estatísticas em servidores com senhas fracas que não atendem aos requisitos da linha de base.
Common Weak Password Detection	Estatísticas em servidores com senhas e contas fracas.

----Fim

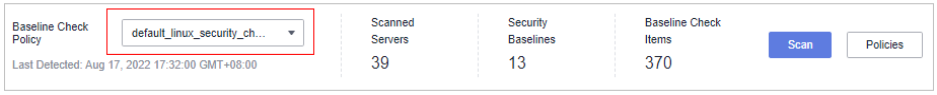
Execução manual de uma verificação de linha de base

AVISO

- Em uma verificação manual, somente os servidores vinculados à política de linha de base de destino são verificados. Se a política padrão for usada, **vincule servidores** e execute a verificação manual.
- Antes de executar uma verificação manual, verifique se a política de destino está disponível na lista suspensa **Baseline Check Policy**. Para obter detalhes sobre como criar uma política, consulte **Criação de uma política de verificação de linha de base**.

Passo 1 Escolha **Prediction** > **Baseline Checks**. Selecione a política de verificação da linha de base de destino.

Figura 4-27 Selecionar a política de linha de base de destino



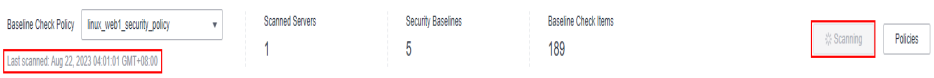
Passo 2 Clique em **Scan** no canto superior direito da página.

Passo 3 Se a hora exibida na área **Last scanned** sob **Baseline Check Policy** for a hora real da verificação, a verificação estará concluída.

NOTA

- Depois que uma verificação manual é executada, o botão exibirá **Scanning** e será desativado. Se o tempo de verificação exceder 30 minutos, o botão será ativado automaticamente novamente. Se a hora exibida na área **Last scanned** se tornar a hora de verificação atual, isso indica que a verificação foi concluída.
- Depois que a verificação for concluída, você pode visualizar os resultados da verificação e as sugestões de manipulação consultando a **Visualização de detalhes da verificação da linha de base**.

Figura 4-28 Verificar status



----Fim

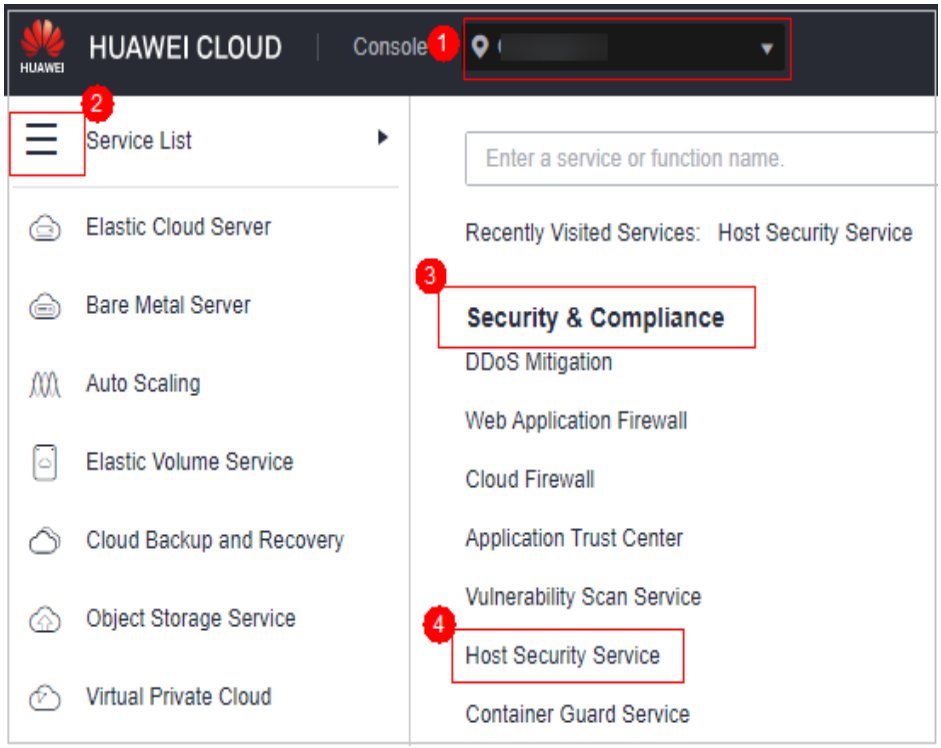
Exportação do relatório de verificação da linha de base

Você pode filtrar e exportar o relatório de verificação de linha de base conforme necessário.

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 4-29 Acessar o HSS



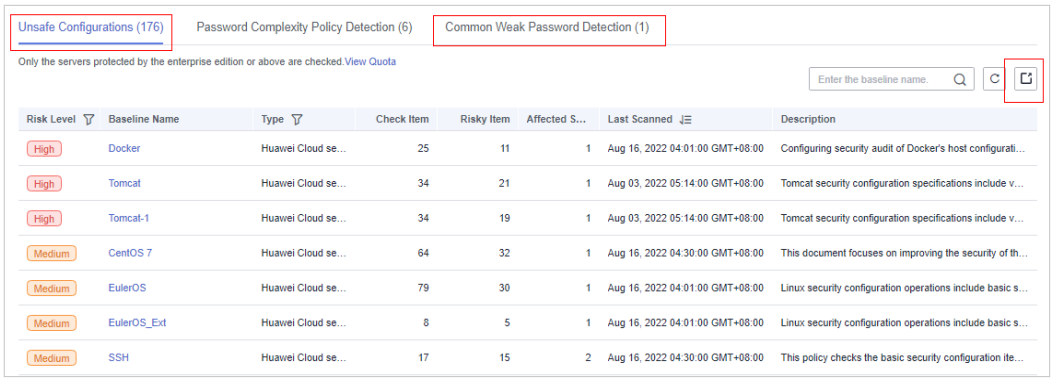
Passo 3 No painel de navegação à esquerda, escolha **Prediction** > **Baseline Checks**.

Passo 4 Clique em diferentes guias na página exibida para verificar os riscos detectados.

NOTA

Atualmente, apenas os relatórios das páginas **Unsafe Configurations** e **Common Weak Password Detection** podem ser exportados.

Figura 4-30 Visualizar a lista de riscos



Passo 5 Clique na guia **Unsafe Configurations** ou **Common Weak Password Detection** e clique em  no canto superior direito da lista para baixar os alarmes de risco filtrados.

NOTA

- Na página **Unsafe Configurations**, você pode clicar na imagem na coluna correspondente para procurar alarmes com base no nível e tipo de risco.
- Na guia **Common Weak Password Detection**, você pode pesquisar alarmes por nome de servidor, endereço IP e nome de conta e fazer download dos alarmes.
- Um máximo de 5.000 relatórios de verificação de risco podem ser baixados por vez nas páginas **Unsafe Configurations** e **Common Weak Password Detection**.

----Fim

4.2.2 Visualização de detalhes da verificação da linha de base

O HSS verifica seu software em busca de políticas de complexidade de senhas fracas e outras configurações inseguras e fornece sugestões para corrigir riscos detectados. Para obter detalhes sobre configurações inseguras, consulte **Inspeção de linha de base**.

Restrições

Os servidores que não estão protegidos pelo HSS não suportam operações relacionadas com a linha de base.

Pré-requisito

Somente os servidores protegidos pela edição empresarial ou superior são verificados.

Descrição da detecção

A detecção da linha de base do MySQL do SO Linux é baseada nas especificações de configuração de segurança do MySQL 5. Se o MySQL 8 estiver instalado em seu servidor, os seguintes itens de verificação não serão exibidos nos resultados da detecção, pois serão descartados nessa versão. Os resultados da detecção são exibidos apenas no servidor cuja versão do MySQL é 5.

- Regra: não definir **old_passwords** como **1**.
- Regra: definir secure_auth como **1** ou **ON**.
- Regra: não definir **skip_secure_auth**.
- Regra: definir **log_warnings** como **2**.
- Regra: configurar a política de limpeza do binlog do MySQL.
- Regra: o parâmetro **sql_mode** contém **NO_AUTO_CREATE_USER**.
- Regra: usar o plug-in de auditoria do MySQL.

Itens de verificação

Tabela 4-14 Itens de verificação

Item	Descrição
Configurações inseguras	Atualmente, os seguintes padrões e tipos de verificação são suportados: ● Para Linux: – Práticas de segurança da Huawei Cloud: Apache 2, Docker, MongoDB, Redis, MySQL 5, Nginx, Tomcat, SSH, vsftp, CentOS 7, EulerOS, EulerOS_ext, Kubernetes-Node e Kubernetes-Master. – Conformidade de DJCP MLPS: Apache 2, MongoDB, MySQL 5, Nginx, Tomcat, CentOS 6, CentOS 7, CentOS 8, Debian 9, Debian 10, Debian 11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu 12, Ubuntu 14, Ubuntu 16, Ubuntu 18, Alma, SUSE 12 e SUSE 15. ● Para Windows: – A linha de base da prática de segurança na nuvem pode verificar MongoDB, Apache2, MySQL, Nginx, Redis, Tomcat, Windows_2008, Windows_2012, Windows_2016 e Windows_2019.
Políticas de complexidade de senha	Políticas de complexidade de senha em contas do sistema.
Senhas fracas comuns	Senhas fracas definidas na biblioteca de senhas fracas comuns. Senhas fracas comuns de MySQL, FTP e contas do sistema.

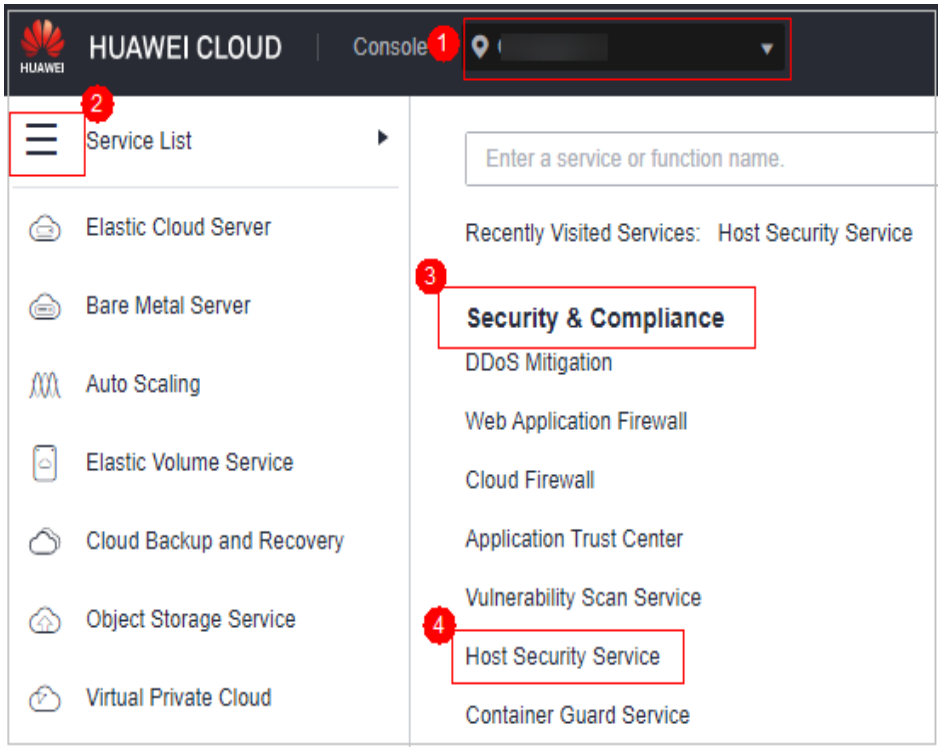
Visualização de configurações inseguras

Veja as estatísticas de risco de configurações inseguras e as sugestões correspondentes.

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 4-31 Acessar o HSS



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

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 Clique na guia **Unsafe Configurations** para exibir os itens de risco. Para obter mais informações, consulte **Tabela 4-15**.

Para exibir os resultados da verificação de configuração do servidor em uma política de verificação de linha de base especificada, selecione uma política na lista suspensa **Baseline Check Policy**.

Figura 4-32 Visualizar detalhes de configuração insegura

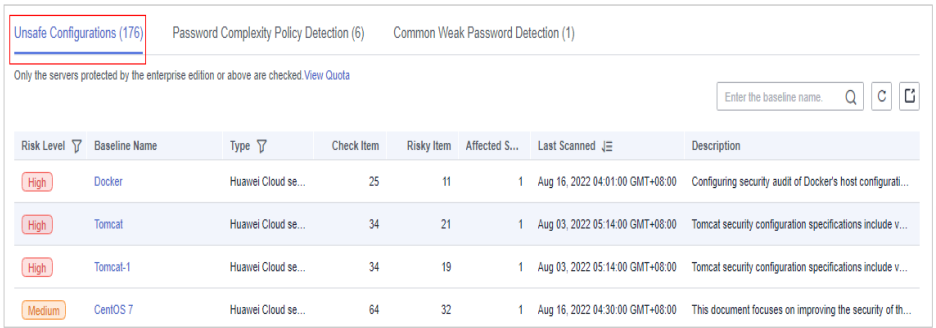
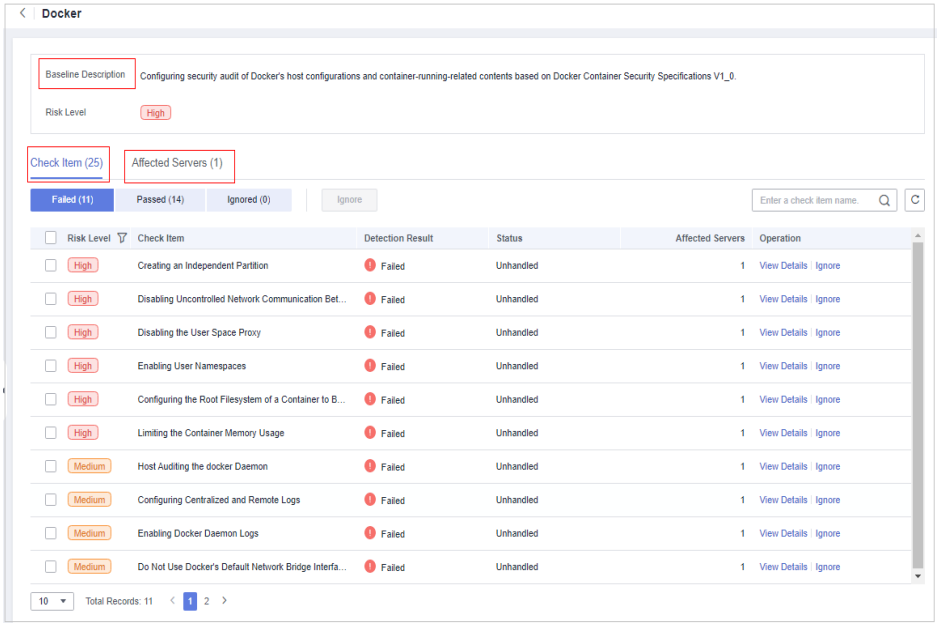


Tabela 4-15 Descrição do parâmetro

Parâmetro	Descrição
Risk Level	Nível de um resultado de detecção. ● High ● Low ● Medium ● Safe
Baseline Name	Nome da linha de base que é verificada.
Type	Tipo de política da linha de base que foi verificada. ● Práticas de segurança na nuvem ● DJCP MLPS
Check Item	Número total de itens de configuração verificados.
Risky Item	Número total de configurações arriscadas.
Affected Servers	Número total de servidores afetados pelos riscos detectados em uma linha de base.
Last Scanned	Hora em que a última detecção foi realizada.
Description	Descrição de uma linha de base.

Passo 5 Clique no nome da linha de base de destino na lista para exibir a descrição da linha de base, os servidores afetados e os detalhes sobre todos os itens de verificação.

Figura 4-33 Exibição de detalhes da verificação da linha de base

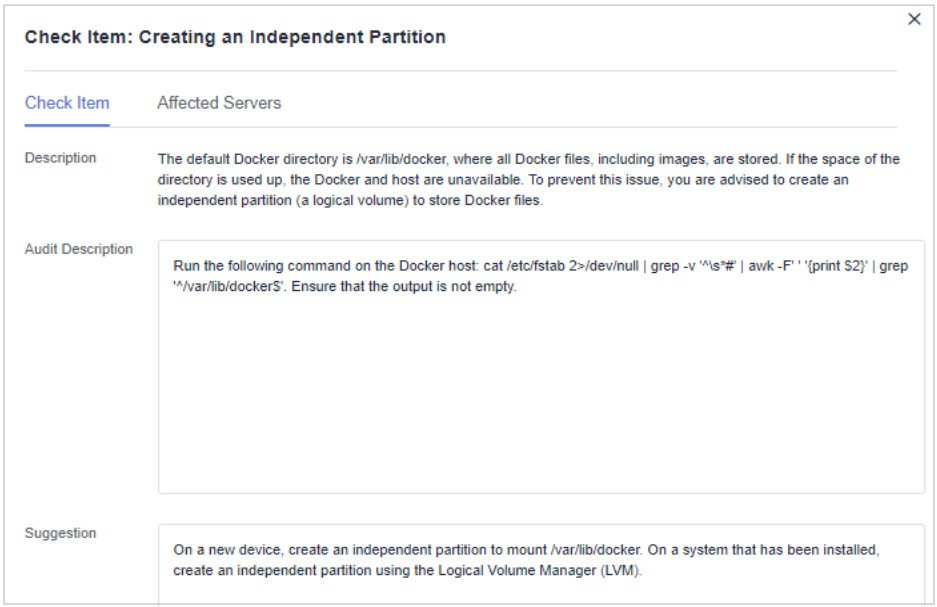


Passo 6 Clique em **View Details** na coluna **Operation** do item de verificação de destino para exibir a descrição, a descrição da auditoria e as sugestões de manipulação.

Você precisa verificar se um item de risco é crítico ou precisa ser tratado.

Se sim, modifique o item de verificação de acordo com as sugestões de manipulação. Se não, clique em **Ignore** na coluna **Operation** do item de verificação.

Figura 4-34 Exibição de detalhes do item de verificação



----Fim

Visualização da detecção de política de complexidade de senha

Visualize as estatísticas de risco e sugestões de tratamento de detecção de política de complexidade de senha.

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação à esquerda, escolha **Prediction** > **Baseline Checks**.

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 3 Clique na guia **Password Complexity Policy Detection** para exibir os itens estatísticos de risco e as sugestões de tratamento. Para obter mais informações, consulte **Tabela 4-16**.

Figura 4-35 Exibição dos detalhes da detecção da política de complexidade de senhas

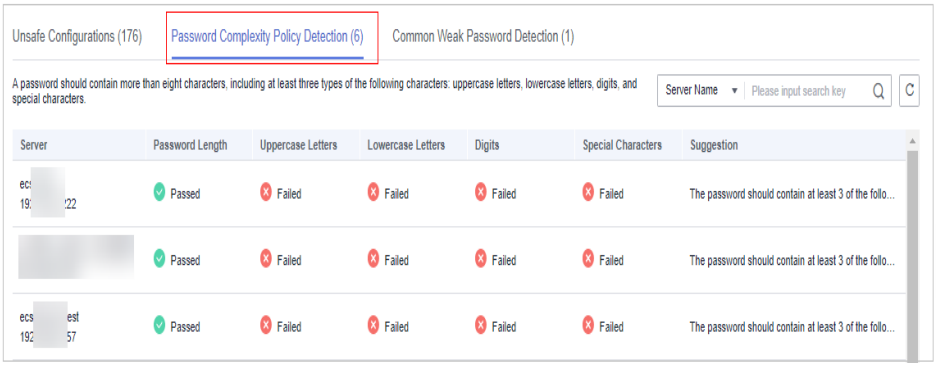


Tabela 4-16 Descrição do parâmetro

Parâmetro	Descrição
Server	Nome e endereço IP do servidor detectado.
Password Length	Se o comprimento da senha do servidor de destino atende aos requisitos. ● Passed ● Failed
Uppercase Letters	Se as letras maiúsculas usadas na senha do servidor de destino atendem aos requisitos. ● Passed ● Failed
Lowercase Letters	Se as letras minúsculas usadas na senha do servidor de destino atendem aos requisitos. ● Passed ● Failed
Digits	Se os dígitos usados na senha do servidor de destino atendem aos requisitos. ● Passed ● Failed
Special characters	Se os caracteres especiais usados na senha do servidor de destino atendem aos requisitos. ● Passed ● Failed
Suggestion	Sugestão para corrigir senhas inseguras

----Fim

Visualização da detecção de senha fraca comum

Visualize as estatísticas de risco de detecção de senha fraca e as sugestões de manipulação correspondentes.

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação à esquerda, escolha **Prediction** > **Baseline Checks**.

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 3 Clique na guia **Common Weak Password Detection** para exibir as estatísticas de contas com senhas fracas arriscadas no servidor. Para obter mais informações, consulte **Tabela 4-17**.

Figura 4-36 Visualização da detecção de senha fraca comum

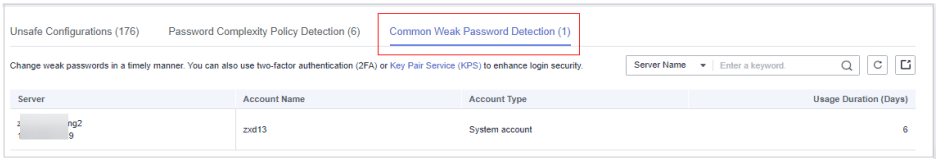


Tabela 4-17 Descrição do parâmetro

Parâmetro	Descrição
Server	Nome e endereço IP do servidor detectado.
Account Name	Contas com senhas fracas que são detectadas no servidor de destino.
Account Type	Tipo de uma conta.
Usage Duration (Days)	Período para usar uma senha fraca.

NOTA

- Para melhorar a segurança do servidor, é aconselhável modificar as contas com senhas fracas para fazer logon no sistema em tempo hábil, como contas SSH.
- Para proteger os dados internos do seu servidor, é aconselhável modificar contas de software que usam senhas fracas, como contas MySQL e contas FTP.

Depois de modificar senhas fracas, é aconselhável executar a detecção manual imediatamente para verificar o resultado. Se você não realizar a verificação manual, o HSS verificará automaticamente as configurações no dia seguinte no início da manhã.

- Uma senha deve conter mais de oito caracteres, incluindo letras maiúsculas, minúsculas, dígitos e caracteres especiais.

----Fim

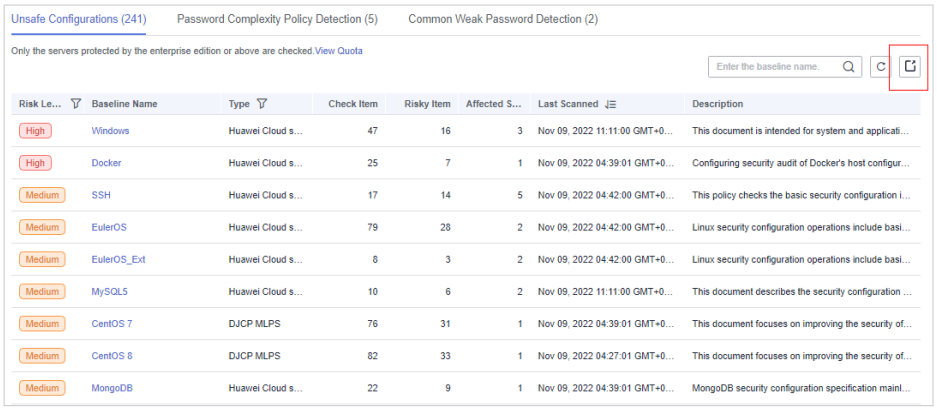
Exportação do relatório de verificação da linha de base

Na página **Baseline Checks**, você pode clicar em  no canto superior direito de uma guia para exportar o relatório de verificação.

NOTA

- O resultado da verificação de um único servidor de nuvem não pode ser exportado separadamente.
- Até 5000 registros de alarme podem ser exportados por vez.

Figura 4-37 Exportação do relatório de verificação da linha de base



4.2.3 Correção de configurações inseguras

Este tópico fornece sugestões sobre como corrigir configurações inseguras encontradas pelo HSS.

Restrições

Os servidores que não estão protegidos pelo HSS não suportam operações relacionadas com a linha de base.

Modificar a política de complexidade de senha

- Para monitorar a política de complexidade de senha em um servidor de Linux, instale os Módulos de autenticação plugáveis (PAM) no servidor. Para obter detalhes, consulte **Como instalar um PAM em um SO Linux?**
- Para obter detalhes sobre como modificar a política de complexidade de senha em um servidor de Linux, consulte **Como instalar um PAM e definir uma política de complexidade de senha adequada em um SO Linux?**
- Para obter detalhes sobre como modificar a política de complexidade de senha em um servidor de Windows, consulte **Como definir uma política de complexidade de senha segura em um SO Windows?**

Depois de modificar a política de complexidade de senha, execute uma verificação manual na parte superior da página **Baseline Checks** para verificar o resultado. Se você não realizar uma verificação manual, o HSS verificará automaticamente as configurações às 00:00:00 do dia seguinte.

Melhorar a força da senha

- Para melhorar a segurança do servidor, é aconselhável modificar as contas com senhas fracas para fazer logon no sistema em tempo hábil, como contas 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 verificar manualmente o resultado imediatamente. Se você não realizar uma verificação manual, o HSS verificará automaticamente as configurações às 00:00:00 do dia seguinte.

Corrigir configurações inseguras em um servidor

Configurações inseguras nas principais aplicações do sistema host podem ser exploradas por hackers para invadir o sistema. Tais configurações incluem algoritmos de criptografia inseguros usados pela inicialização SSH e Tomcat com permissões de raiz.

O HSS pode detectar configurações inseguras fornecer sugestões detalhadas.

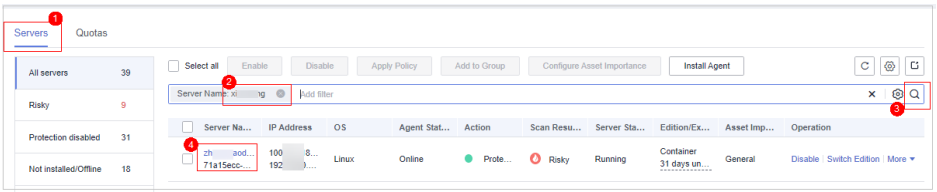
Passo 1 No console do HSS, escolha **Asset Management** > **Servers & Quota** e clique na guia **Servers**.

NOTA

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

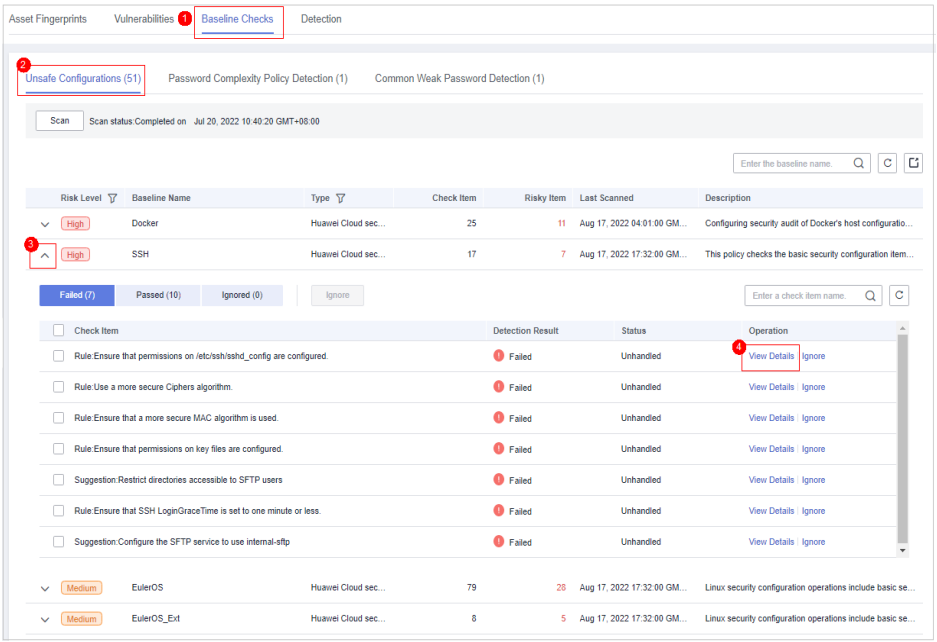
Passo 2 Procure o servidor de destino e clique no nome do servidor para ir para a página de detalhes do servidor.

Figura 4-38 Localizar o servidor de destino



Passo 3 Clique em **Baseline Checks** e clique na guia **Unsafe Configurations**. Clique no ícone antes de um item de risco para expandir e visualizar todos os detalhes do item de verificação.

Figura 4-39 Visualizar detalhes do item de verificação para um servidor



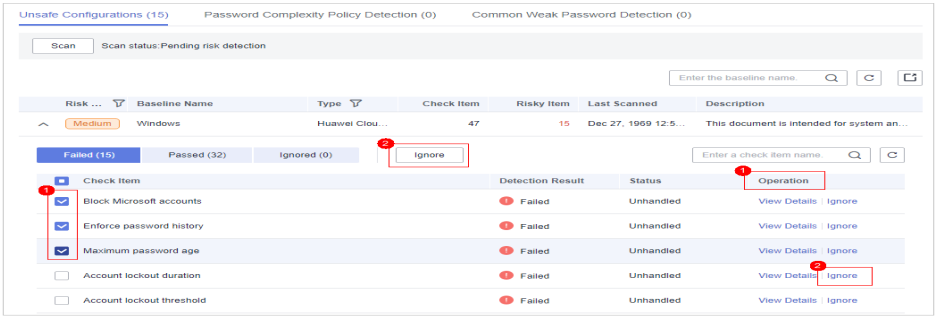
Passo 4 Lide com itens de risco.

- Ignorar os riscos

  Clique em **Ignore** na coluna **Operation** do item de verificação de destino para ignorar um item de verificação.

  Selecione vários itens de verificação e clique em **Ignore** para ignorá-los em lotes.

  Figura 4-40 Ignorar riscos em um servidor



- Correção de riscos

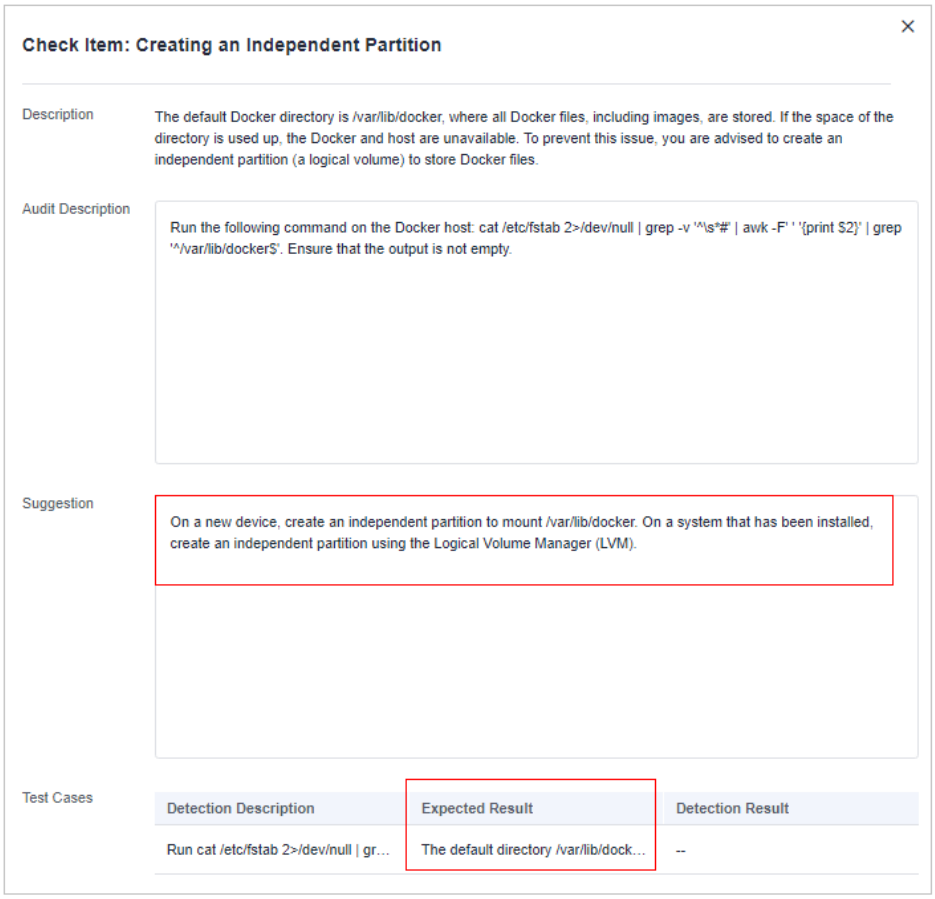
  a. Clique em **View Details** na coluna **Operation** do item de risco de destino para visualizar os detalhes do item de verificação.

  b. Visualize o conteúdo na **Audit Description** e **Suggestion** e corrija as configurações não seguras.

  NOTA

  - Atualmente, a correção de um clique é suportada para algumas configurações de linha de base do EulerOS e configurações de linha de base do CentOS 8. Você pode simplesmente clicar em **Fix** na coluna **Operation** do item de verificação de EulerOS ou CentOS de destino para corrigir as configurações inseguras. Se alguns parâmetros precisarem ser configurados durante a restauração, mantenha os valores padrão.
  - Você é aconselhado a corrigir as configurações com alta gravidade imediatamente e corrigir aquelas com média ou baixa gravidade.

Figura 4-41 Visualizar sugestões sobre como corrigir riscos em um servidor



- Verificação

  Se um item de verificação com falha tiver sido corrigido, você poderá atualizar seu status por meio da verificação.

  Se um item de verificação não for corrigido, clique em **View Cause** para visualizar a causa. Em seguida, corrigi-lo novamente.

  NOTA

  – Atualmente, as verificações de linha de base não são suportadas para SOs Windows.
  – As verificações de linha de base são suportadas para os seguintes SOs Linux: Apache 2, Docker, MongoDB, Redis, MySQL 5, Nginx, Tomcat, SSH, vsftp, CentOS 6, CentOS 7, CentOS 8, EulerOS, Debian 9, Debian 10, Debian 11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu 12, Ubuntu 14, Ubuntu 16 e Ubuntu 18.

  a. Clique em **Verify** na coluna **Operation** da linha que contém o item de risco de destino.
  b. Na caixa de diálogo exibida, clique em **OK**. O status muda para **Verifying**. O sistema inicia a verificação automática. Após a conclusão da verificação, verifique o status.

----Fim

Corrigir configurações arriscadas em todos os servidores

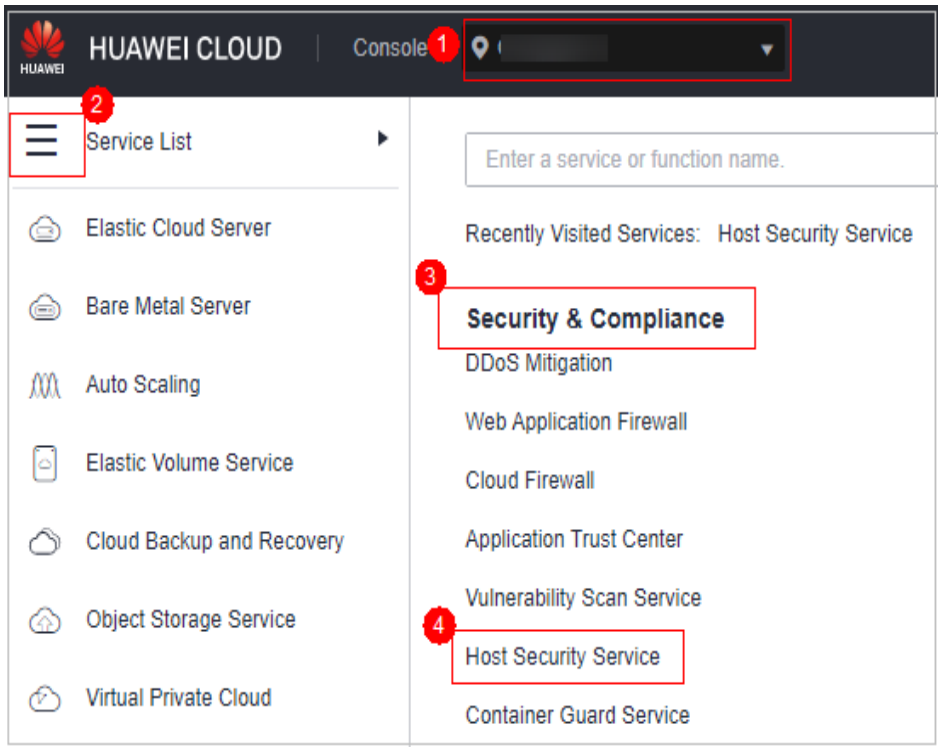
Configurações arriscadas nas principais aplicações do sistema host podem ser exploradas por hackers para invadir o sistema. Tais configurações incluem algoritmos de criptografia inseguros usados pela inicialização SSH e Tomcat com permissões de raiz.

O HSS pode detectar configurações inseguras fornecer sugestões detalhadas.

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 4-42 Acessar o HSS



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

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 Clique na guia **Unsafe Configurations** para exibir os itens de risco. Para obter mais informações, consulte **Tabela 4-18**.

Para exibir os resultados da verificação de configuração do servidor em uma política de verificação de linha de base especificada, selecione uma política na lista suspensa **Baseline Check Policy**.

Figura 4-43 Visualizar detalhes de configuração insegura

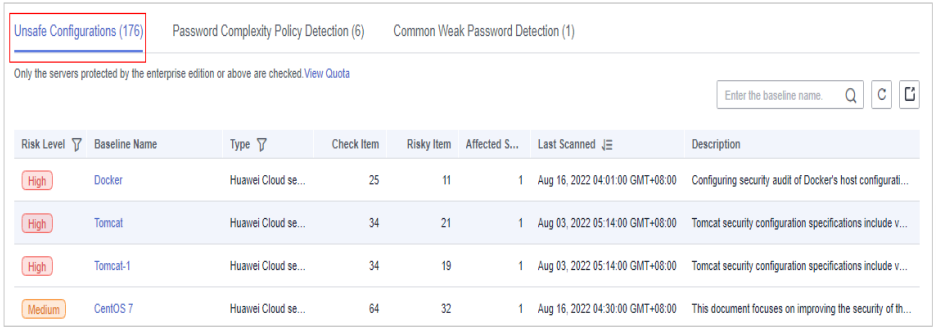
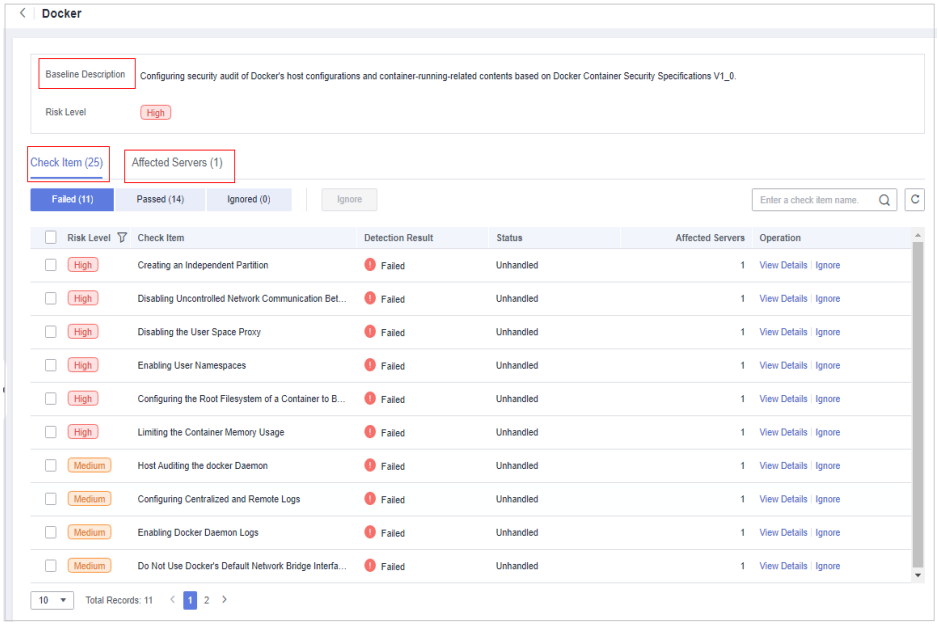


Tabela 4-18 Descrição do parâmetro

Parâmetro	Descrição
Risk Level	Nível de um resultado de detecção. ● High ● Low ● Medium ● Safe
Baseline Name	Nome da linha de base que é verificada.
Type	Tipo de política da linha de base que foi verificada. ● Práticas de segurança na nuvem ● DJCP MLPS
Check Item	Número total de itens de configuração verificados.
Risky Item	Número total de configurações arriscadas.
Affected Servers	Número total de servidores afetados pelos riscos detectados em uma linha de base.
Last Scanned	Hora em que a última detecção foi realizada.
Description	Descrição de uma linha de base.

Passo 5 Clique no nome da linha de base de destino na lista para exibir a descrição da linha de base, os servidores afetados e os detalhes sobre todos os itens de verificação.

Figura 4-44 Exibição de detalhes da verificação da linha de base



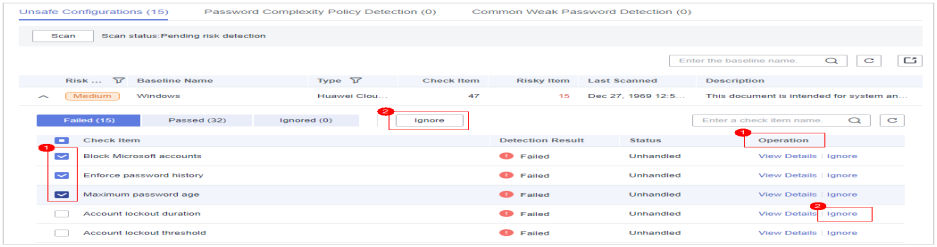
Passo 6 Lide com itens de risco.

- Ignorar os riscos

  Clique em **Ignore** na coluna **Operation** do item de verificação de destino para ignorar um item de verificação.

  Selecione vários itens de verificação e clique em **Ignore** para ignorá-los em lotes.

  Figura 4-45 Ignorar os riscos

- Correção de riscos

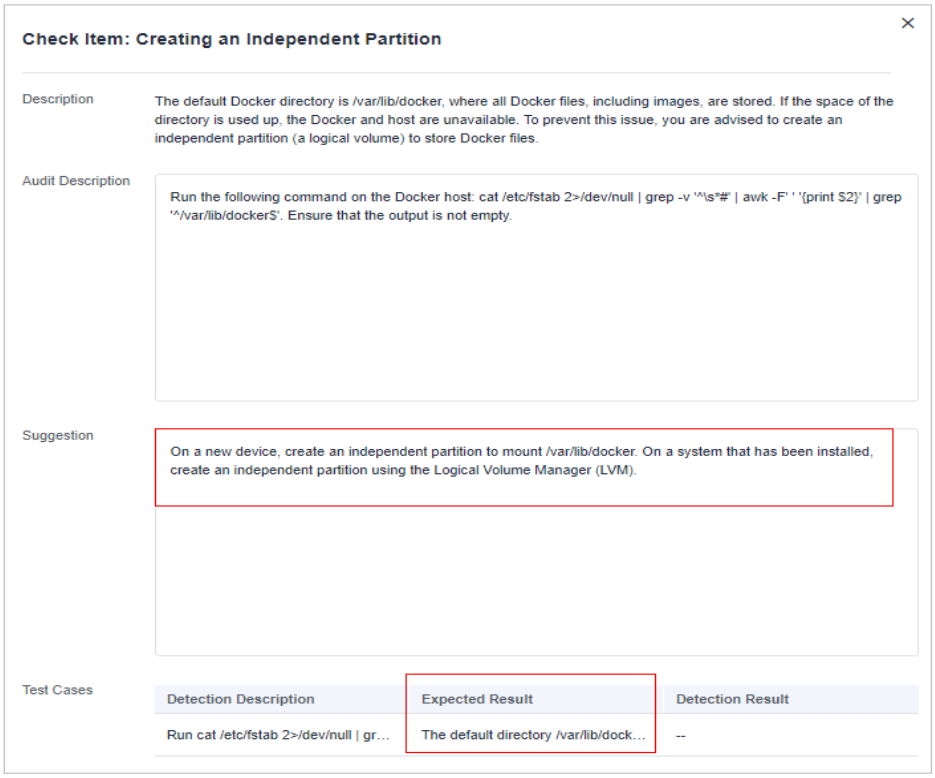
  a. Clique em **View Details** na coluna **Operation** do item de risco de destino para visualizar os detalhes do item de verificação.

  b. Visualize o conteúdo nas caixas de texto **Audit Description** e **Suggestion** e lide com os riscos com base nas sugestões ou no **Expected Result** descrito na área **Test Cases**.

  NOTA

  - Atualmente, a correção de um clique é suportada para algumas configurações de linha de base do EulerOS e configurações de linha de base do CentOS 8. Você pode simplesmente clicar em **Fix** na coluna **Operation** do item de verificação de EulerOS ou CentOS de destino para corrigir as configurações inseguras. Se alguns parâmetros precisarem ser configurados durante a restauração, mantenha os valores padrão.
  - Você é aconselhado a corrigir as configurações com alta gravidade imediatamente e corrigir aquelas com média ou baixa gravidade.

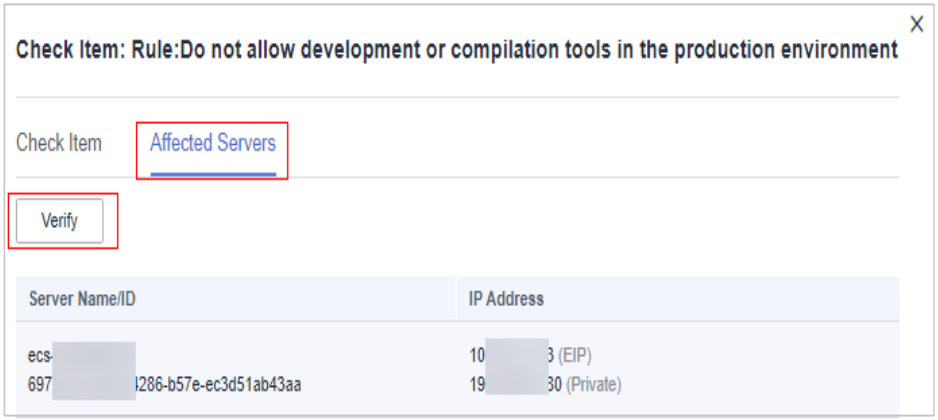
Figura 4-46 Visualizar as sugestões de manuseio



c. Clique em **Affected Servers** para exibir os servidores afetados pelo item de verificação.

Clique em **Verify** para atualizar a lista de servidores afetados.

Figura 4-47 Visualizar servidores afetados



- Verificação

  Se um item de verificação com falha tiver sido corrigido, você poderá atualizar seu status por meio da verificação.

  Se um item de verificação não for corrigido, clique em **View Cause** para visualizar a causa. Em seguida, corrigi-lo novamente.

NOTA

- Atualmente, as verificações de linha de base não são suportadas para SOs Windows.
- As verificações de linha de base são suportadas para os seguintes SOs Linux: Apache 2, Docker, MongoDB, Redis, MySQL 5, Nginx, Tomcat, SSH, vsftp, CentOS 6, CentOS 7, CentOS 8, EulerOS, Debian 9, Debian 10, Debian 11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu 12, Ubuntu 14, Ubuntu 16 e Ubuntu 18.

a. Clique em **Verify** na coluna **Operation** da linha que contém o item de risco de destino.

b. Na caixa de diálogo exibida, clique em **OK**. O status muda para **Verifying**. O sistema inicia a verificação automática. Após a conclusão da verificação, verifique o status.

----Fim

4.2.4 Gerenciamento de políticas de verificação de linha de base

Você pode criar, editar e excluir políticas de verificação para verificações manuais de linha de base e pode personalizar o item de verificação conforme necessário.

Restrições

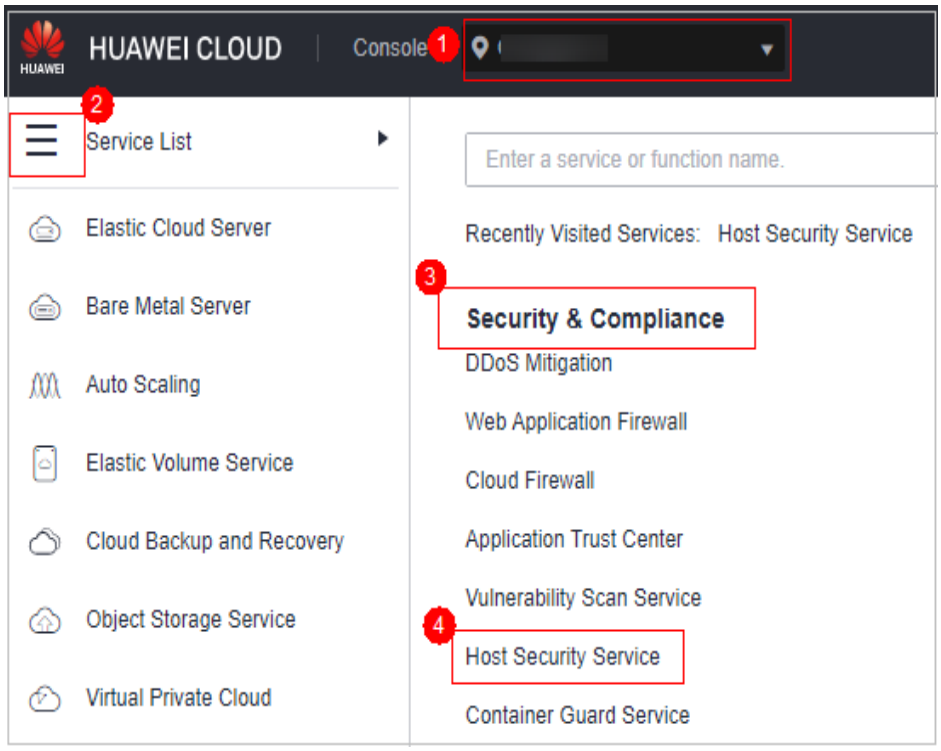
- As políticas na página **Prediction** > **Baseline Checks** só entram em vigor em verificações manuais da linha de base. Para obter detalhes sobre como configurar as políticas, consulte "Verificação de configuração" e "Verificação de senha fraca" em **Modificação de uma política**.
- Os servidores que não estão protegidos pelo HSS não suportam operações relacionadas à linha de base.

Criação de uma política de verificação de linha de base

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 4-48 Acessar o HSS

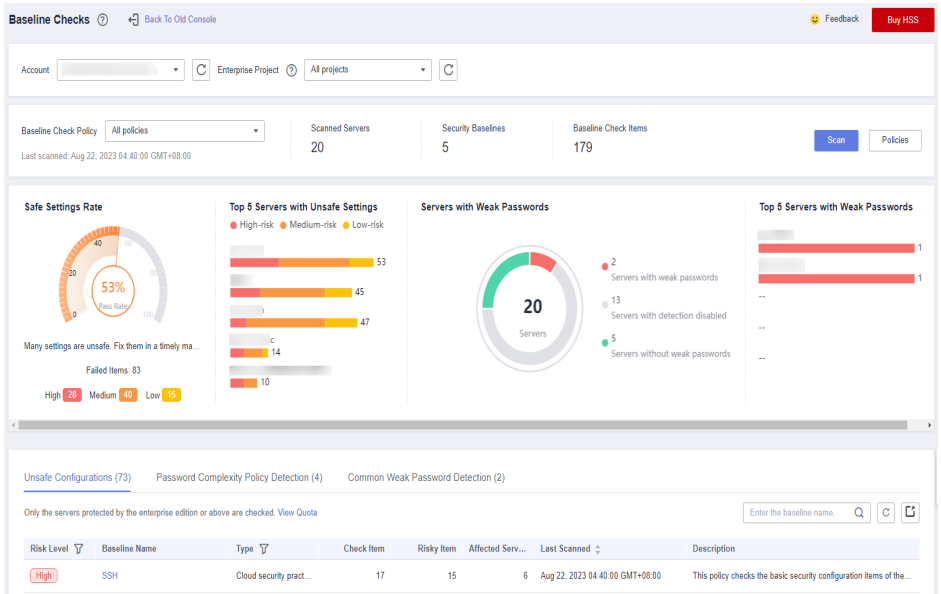


Passo 3 No painel de navegação à esquerda, escolha **Prediction** > **Baseline Checks**.

NOTA

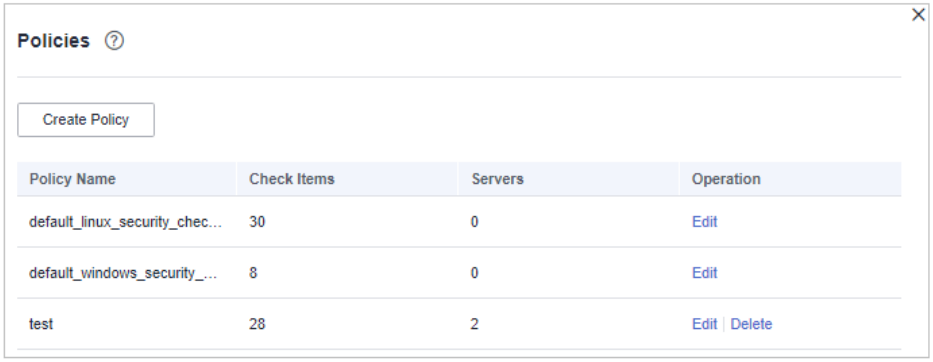
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figura 4-49 Visão geral da verificação da linha de base



Passo 4 Clique em **Policies** no canto superior direito da página.

Figura 4-50 Políticas



Passo 5 Clique em **Create Policy** e configure as informações de política consultando **Tabela 4-19**.

Para verificar os detalhes da linha de base, clique em **Rule Details** à direita de um nome de linha de base.

NOTA

Se você selecionar **Linux** para **OS**, poderá selecionar quaisquer verificações incluídas em **Baseline** e editar regras. Esta função não é suportada para servidores do Windows.

Figura 4-51 Criação de uma política

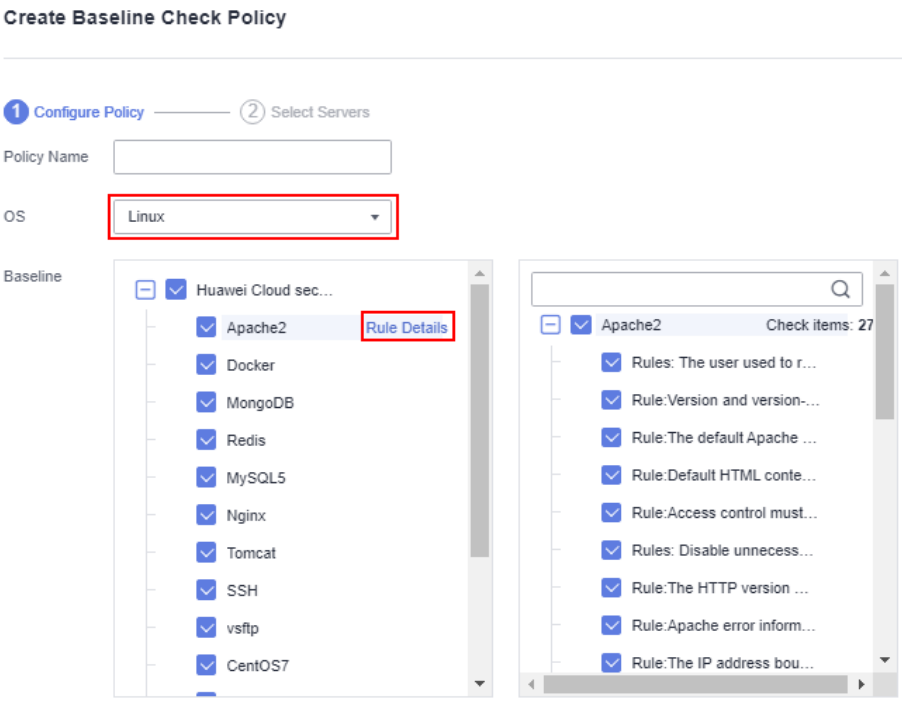
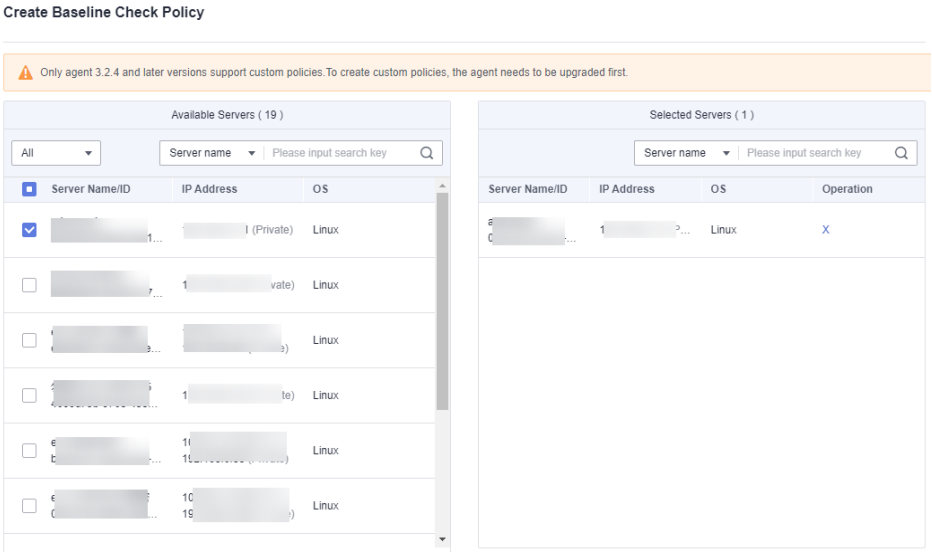


Tabela 4-19 Parâmetros da política de linha de base

Parâmetro	Descrição	Exemplo de valor
Policy Name	Nome da política	linux_web1_security_policy
OS	SO que será verificado. ● Linux ● Windows	Linux
Baseline	Linha de base usada para uma verificação. Os itens de verificação são os seguintes: ● Para Linux: – Práticas de segurança da Huawei Cloud: Apache 2, Docker, MongoDB, Redis, MySQL 5, Nginx, Tomcat, SSH, vsftp, CentOS 7, EulerOS, EulerOS_ext, Kubernetes-Node e Kubernetes-Master. – Conformidade de DJCP MLPS: Apache 2, MongoDB, MySQL 5, Nginx, Tomcat, CentOS 6, CentOS 7, CentOS 8, Debian 9, Debian 10, Debian 11, Red Hat 6, Red Hat 7, Red Hat 8, Ubuntu 12, Ubuntu 14, Ubuntu 16, Ubuntu 18, Alma, SUSE 12 e SUSE 15. ● Para Windows: – A linha de base da prática de segurança na nuvem pode verificar MongoDB, Apache2, MySQL, Nginx, Redis, Tomcat, Windows_2008, Windows_2012, Windows_2016 e Windows_2019.	**Cloud security practices**: selecionar tudo **DJCP MLPS**: selecionar tudo

Passo 6 Confirme as informações, clique em **Next** e selecione o servidor a ser vinculado à aplicação com base no nome do servidor, ID do servidor, EIP ou endereço IP privado.

Figura 4-52 Selecionar servidores



Passo 7 Confirme as informações e clique em **OK**. A política de linha de base será exibida na lista de políticas.

----Fim

Edição de uma política de verificação de linha de base

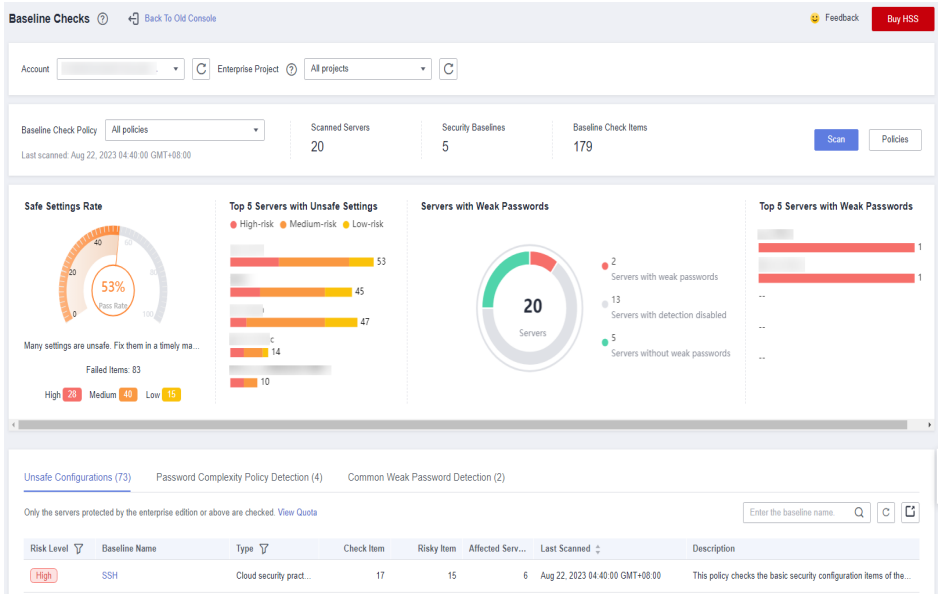
Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação à esquerda, escolha **Prediction** > **Baseline Checks**.

NOTA

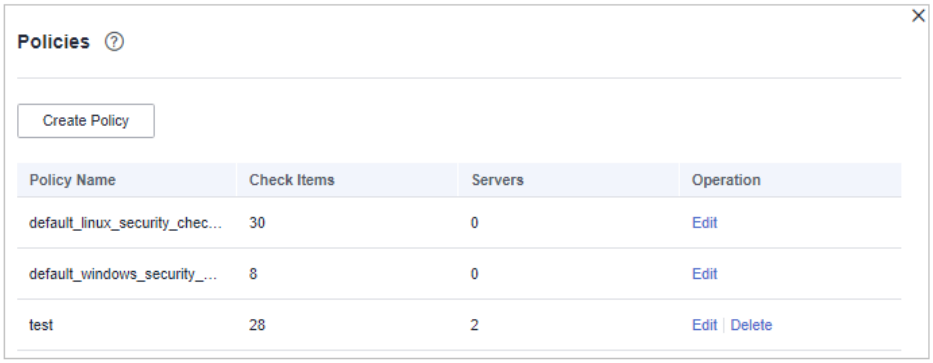
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figura 4-53 Visão geral da verificação da linha de base



Passo 3 Clique em **Policies** no canto superior direito da página.

Figura 4-54 Políticas

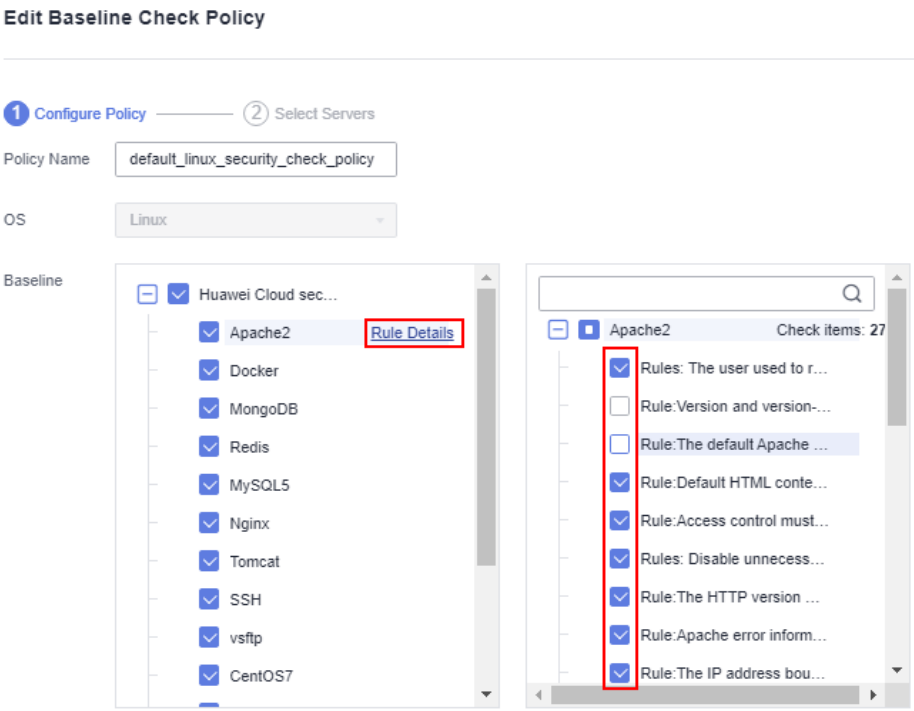


Passo 4 Clique em **Edit** na coluna **Operation** de uma política. Na página de detalhes da política exibida, configure o nome da política e verifique os itens.

NOTA

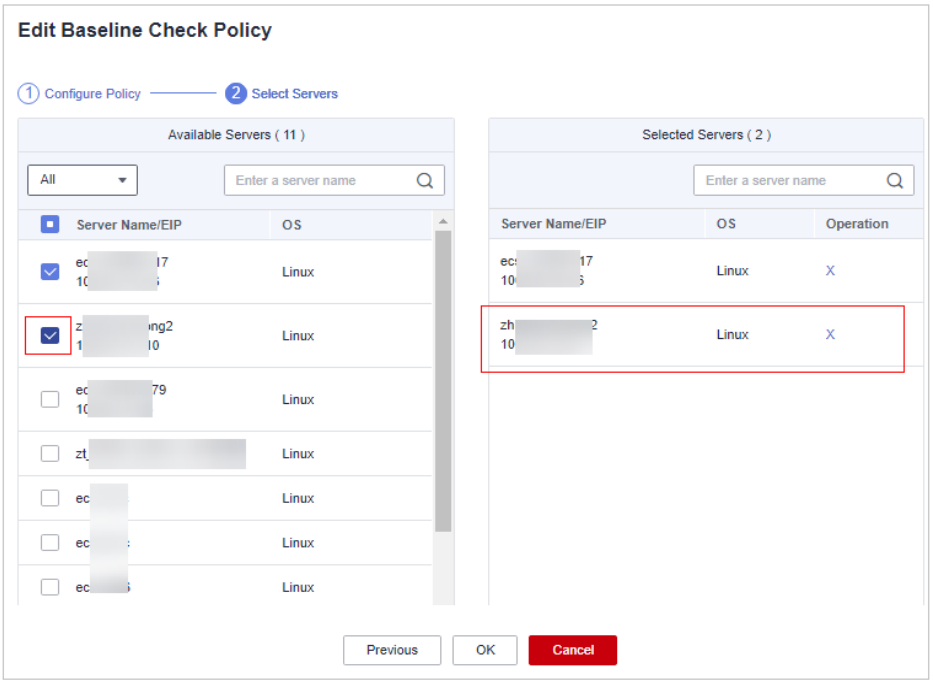
Se você selecionar **Linux** para **OS**, poderá selecionar quaisquer verificações incluídas em **Baseline** e editar regras. Esta função não é suportada para servidores do Windows.

Figura 4-55 Editar uma política de verificação de linha de base



Passo 5 Confirme a configuração, clique em **Next** e selecione servidores.

Figura 4-56 Selecionar servidores



Passo 6 Confirme as informações e clique em **OK**. Você pode visualizar a política atualizada na lista de políticas.

----Fim

Exclusão de uma política de verificação de linha de base

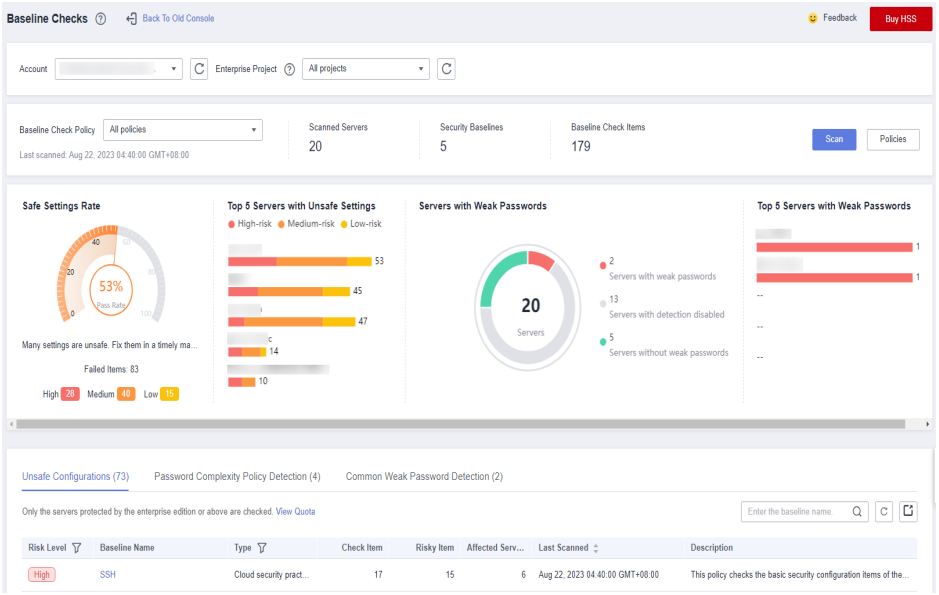
Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação à esquerda, escolha **Prediction** > **Baseline Checks**.

NOTA

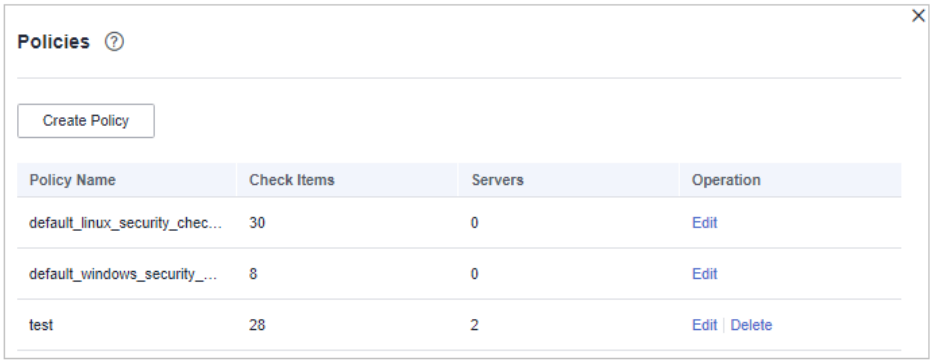
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figura 4-57 Visão geral da verificação da linha de base



Passo 3 Clique em **Policies** no canto superior direito da página.

Figura 4-58 Políticas



Passo 4 Clique em **Delete** na coluna **Operation** de uma política. Na caixa de diálogo exibida, confirme as informações e clique em **OK**.

----Fim

4.3 Segurança de imagens de containers

4.3.1 Vulnerabilidades de imagem

Esta seção descreve como verificar as vulnerabilidades na imagem privada e determinar se deve ignorar as vulnerabilidades.

Pré-requisito

A proteção de container foi ativada.

Método de detecção

Depois de ativar a proteção de nó, suas imagens do Linux serão verificadas automaticamente.

Restrições

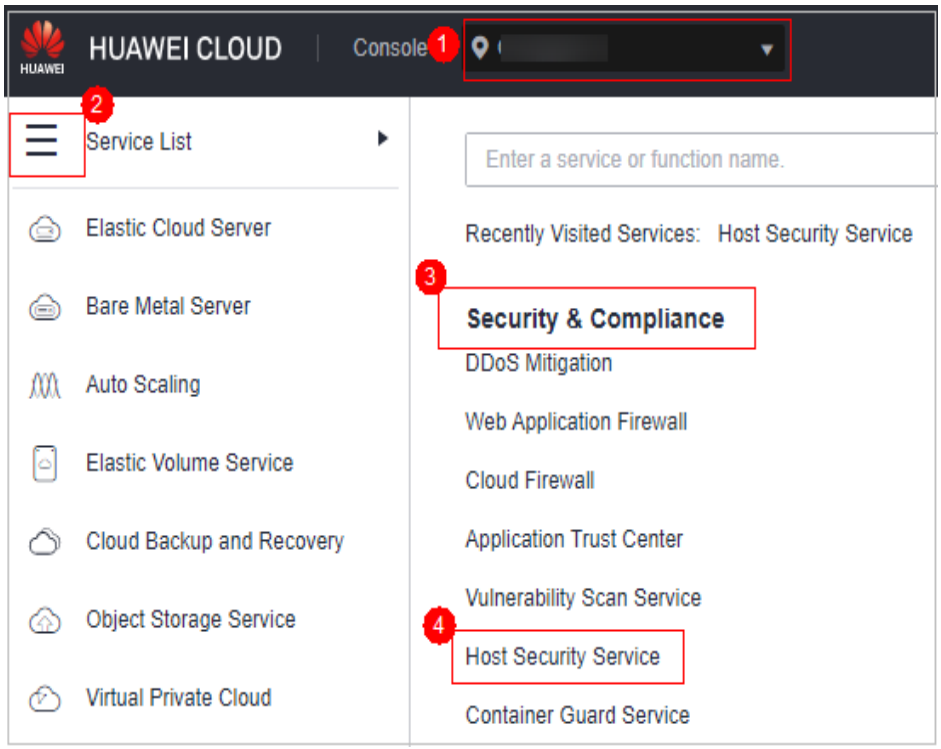
Somente vulnerabilidades em imagens do Linux podem ser verificadas.

Visualizar vulnerabilidades em imagens locais

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 4-59 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Prediction** > **Container Images**. Na página exibida, clique em **Image Vulnerabilities** e clique em **Local Image Vulnerabilities** para exibir vulnerabilidades de imagem local.

Tabela 4-20 Descrição do parâmetro

Parâmetro	Descrição	Operação
Vulnerability Name	-	• Clique em para visualizar os detalhes de uma vulnerabilidade, incluindo **CVE ID**, **CVSS Score**, **Disclosed** e **Vulnerability Details**. • Clique no nome de uma vulnerabilidade para visualizar as imagens afetadas pela vulnerabilidade. Para obter detalhes, consulte **Passo 6**
Repair Urgency	Mostra se a vulnerabilidade deve ser reparada imediatamente.	-
Unprocessed Images	Mostra o número de imagens em que a vulnerabilidade foi detectada, mas ainda não corrigida.	-
Historically Affected Images	Mostra o número de imagens que foram afetadas.	-
Solution	Fornece uma solução para corrigir a vulnerabilidade.	Clique no link na coluna **Solution** para exibir a solução.

Passo 4 Clique no nome da vulnerabilidade para ver as informações básicas e as imagens afetadas.

----Fim

Visualizar vulnerabilidades em imagens privadas

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação à esquerda, escolha **Prediction** > **Container Images**. Na página exibida, clique em **Image Vulnerabilities** e clique em **Private Image Vulnerabilities** para exibir as vulnerabilidades de imagem privada.

NOTA

Clique em uma imagem de risco para verificar a visão geral da vulnerabilidade, incluindo o nome da vulnerabilidade, a urgência, o status, o número de imagens afetadas e a descrição da vulnerabilidade.

Figura 4-60 Visualizar vulnerabilidades em imagens privadas

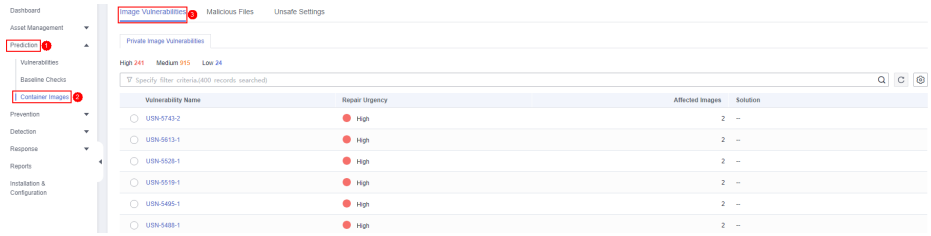


Tabela 4-21 Descrição do parâmetro

Parâmetro	Descrição	Operação
Vulnerability Name	-	● Clique em ⌄ para visualizar os detalhes de uma vulnerabilidade, incluindo **CVE ID**, **CVSS Score**, **Disclosed** e **Vulnerability Details**. ● Clique no nome de uma vulnerabilidade para visualizar as imagens afetadas pela vulnerabilidade. Para mais detalhes, consulte **Passo 3**.
Repair Urgency	Mostra se a vulnerabilidade deve ser reparada imediatamente.	-
Unprocessed Images	Mostra o número de imagens em que a vulnerabilidade foi detectada, mas ainda não corrigida.	-
Historically Affected Images	Mostra o número de imagens que foram afetadas.	-
Solution	Fornece uma solução para corrigir a vulnerabilidade.	Clique no link na coluna **Solution** para exibir a solução.

Passo 3 Clique no nome da vulnerabilidade para ver as informações básicas e as imagens afetadas.

Figura 4-61 Detalhes das vulnerabilidades

----Fim

4.3.2 Visualização de resultados de detecção de arquivos maliciosos

Arquivos maliciosos nas imagens privadas podem ser detectados automaticamente, ajudando você a descobrir e eliminar as ameaças de segurança em seus ativos.

Frequência de verificação

Uma verificação abrangente é realizada automaticamente no início da manhã todos os dias.

Pré-requisitos

A proteção de container foi ativada.

Restrições

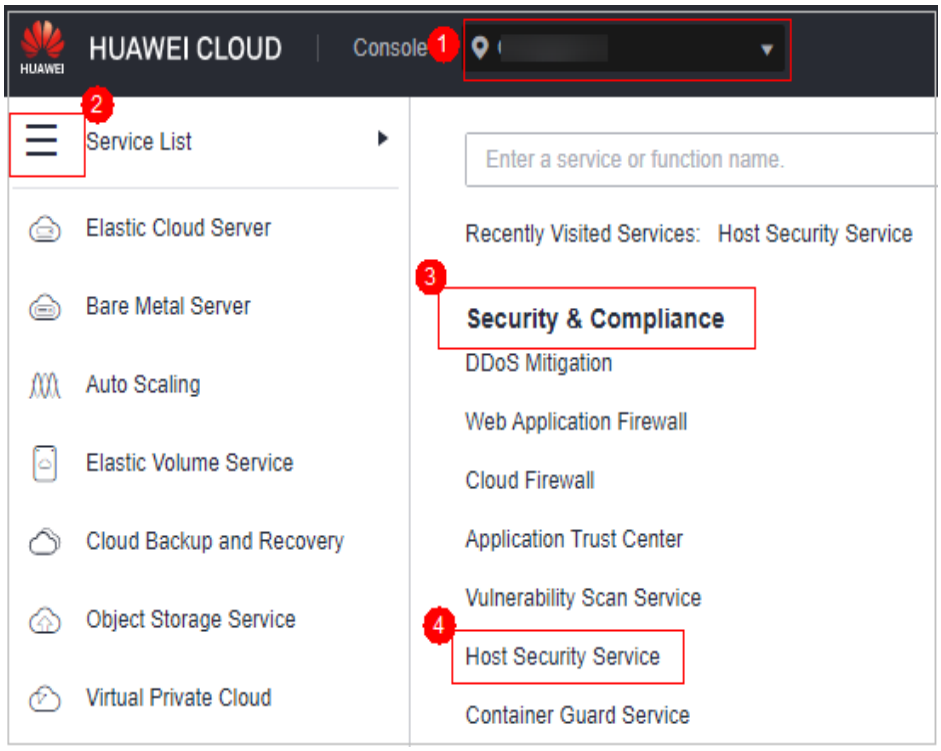
Somente arquivos maliciosos em imagens do Linux podem ser detectados.

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 4-62 Acessar o HSS

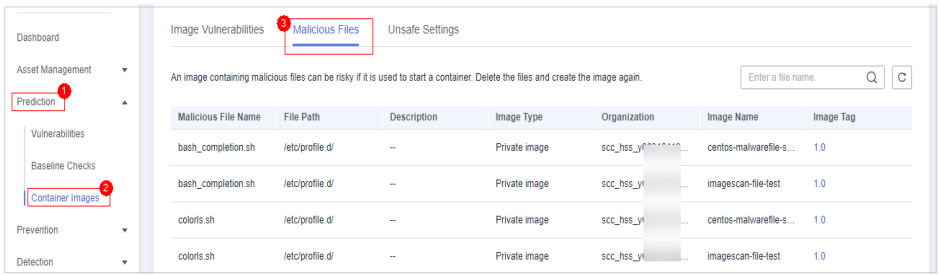


Passo 3 Na árvore de navegação à esquerda, escolha **Prediction** > **Container Images**.

Passo 4 Clique na guia **Malicious Files** para exibir detalhes sobre os arquivos maliciosos em imagens privadas. Exclua os arquivos maliciosos ou crie imagens novamente, conforme necessário, com base no resultado da verificação.

- Arquivos maliciosos incluem cavalos de Troia, worms, vírus e Adware.
- Na coluna **Image Tag**, clique em uma versão de imagem para exibir seu relatório de vulnerabilidades.

Figura 4-63 Resultados de detecção de arquivos maliciosos



----Fim

4.3.3 Verificação da linha de base da imagem

Seu repositório de imagens privadas é verificado em busca de configurações inseguras e fornece sugestões para modificar as configurações, ajudando-o a combater intrusões e a atender aos requisitos de conformidade.

Frequência de verificação

Uma verificação abrangente é realizada automaticamente pelo HSS no início da manhã todos os dias.

Pré-requisitos

A proteção de container foi ativada.

Restrições

Somente riscos de configuração em imagens do Linux podem ser detectados.

Itens de verificação

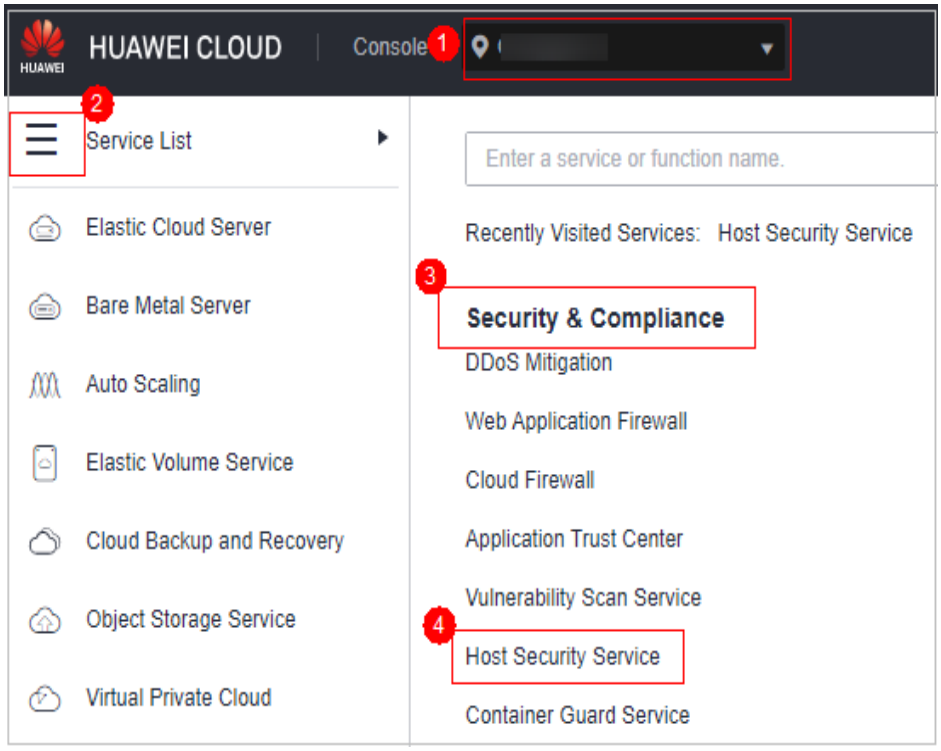
- Contas com nomes ou UIDs duplicados
- Contas não raiz cujos UIDs são 0
- Código de verificação de senha
- Contas com valores de hash de senha duplicados
- Algoritmos de hash de senha fraca
- Garantir que a senha da conta não esteja vazia.
- Nomes de grupos ou GIDs duplicados
- Conta não privilegiada incorretamente incluída no grupo de privilégios
- Entradas "+" anteriores no arquivo /etc/passwd
- Entradas "+" anteriores no arquivo /etc/shadow
- Entradas "+" anteriores no arquivo /etc/group
- Garantir que todos os grupos no arquivo /etc/passwd estejam no arquivo /etc/group
- Período de validade da senha não configurado
- Garantir que as datas de alteração de senha de todos os usuários sejam datas passadas.
- Relação de confiança do host
- Estabelecimento de relação de confiança em nível de raiz predefinido
- Usuário **root** não está no grupo com GID 0
- Membros no grupo sombra

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**.

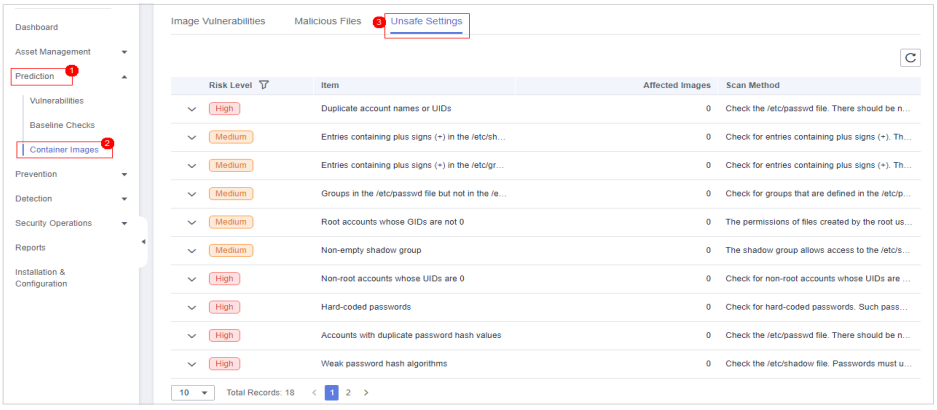
Figura 4-64 Acessar o HSS



Passo 3 Na árvore de navegação à esquerda, escolha **Prediction** > **Container Images**.

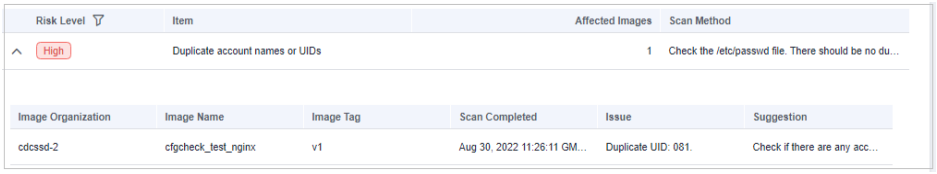
Passo 4 Clique na guia **Unsafe Settings** para exibir as configurações inseguras na imagem.

Figura 4-65 Visualizar configurações inseguras



Passo 5 Clique em ⌄ ao lado de um item de verificação para exibir seus detalhes e sugestões e modifique suas configurações inseguras de acordo.

Figura 4-66 Verificar detalhes do item



----Fim

5 Prevenção

5.1 Proteção da aplicação

5.1.1 Visualização da proteção de aplicações

Para proteger suas aplicações com RASP, você simplesmente precisa adicionar sondas a elas, sem ter que modificar arquivos de aplicações.

Princípios técnicos

Sondas (código de monitoramento e proteção) são adicionadas aos pontos de verificação (funções principais) das aplicações por meio de injeção de código dinâmico. As sondas identificam ataques com base em regras predefinidas, dados que passam pelos pontos de verificação e contextos (lógica de aplicações, configurações, dados e fluxos de eventos).

Pré-requisito

Você ativou a edição premium, WTP ou de container do HSS.

Restrições

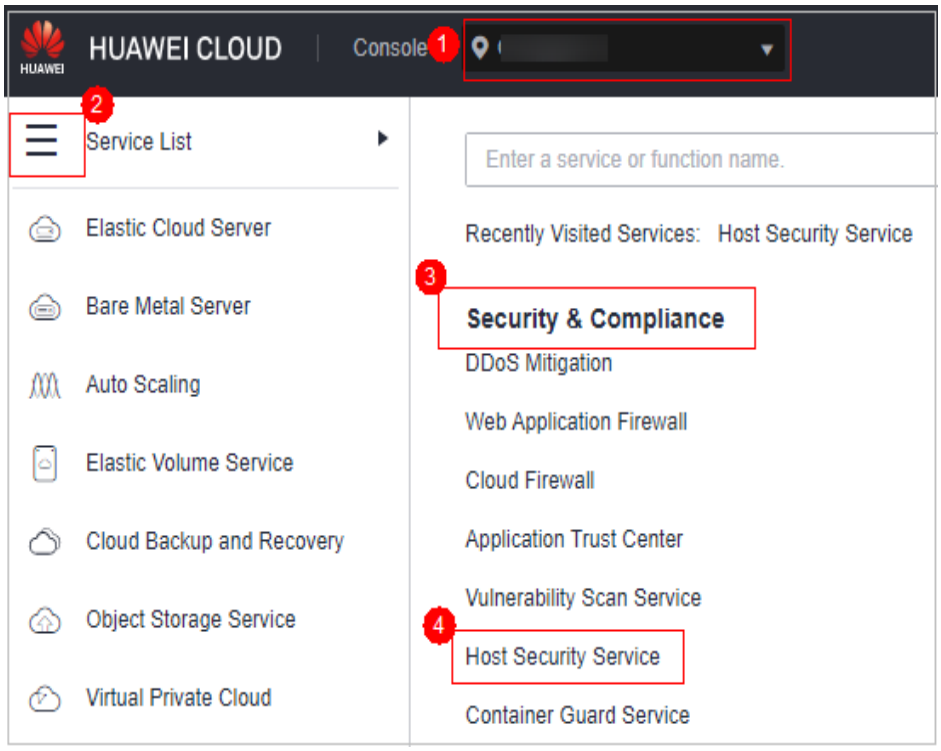
- Atualmente, apenas servidores do Linux são suportados.
- Até agora, apenas aplicações de Java podem ser protegidas.
- As edições premium e superiores suportam operações relacionadas à proteção de aplicações.

Visualização de configurações de 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 5-1 Acessar o HSS

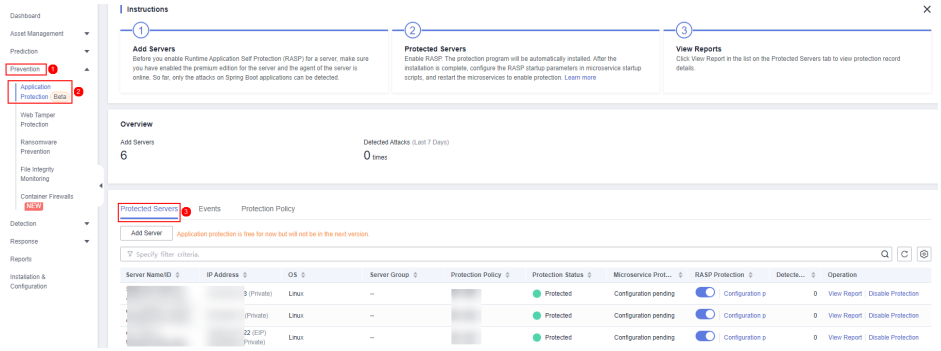


Passo 3 Escolha **Prevention** > **Application Protection**. Clique na guia **Protected Servers**.

NOTA

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

Figura 5-2 Visualização de configurações de proteção



Passo 4 Clique na guia **Protection Servers** e verifique a lista de servidores. Os parâmetros do servidor são os seguintes.

Tabela 5-1 Descrição do parâmetro

Parâmetro	Descrição
Server Name/ID	Nome e ID do servidor
IP Address	Endereço IP privado e EIP do servidor

Parâmetro	Descrição
OS	SO do servidor
Server Group	Grupo ao qual o servidor pertence
Policy	Políticas de detecção vinculadas ao servidor de destino.
Protection Status	Status de proteção de um servidor ● **Protected** ● **Unprotected**
Microservice Protection	Status de proteção de microsserviços. Seu valor pode ser: ● **Active** ● **Installing** ● **Configuration pending** ● **Installation failed**
RASP Protection.	Status de proteção RASP. Seu valor pode ser: ● **Installing** ● **Configuration pending** ● **Installation failed**
Detected Attacks	Número de ataques detectados por RASP.

----Fim

Visualização de eventos

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 Escolha **Prevention** > **Application Protection** e clique na guia **Events**. Para obter detalhes sobre os parâmetros, consulte **Tabela 5-2**.

NOTA

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

Figura 5-3 Eventos de proteção

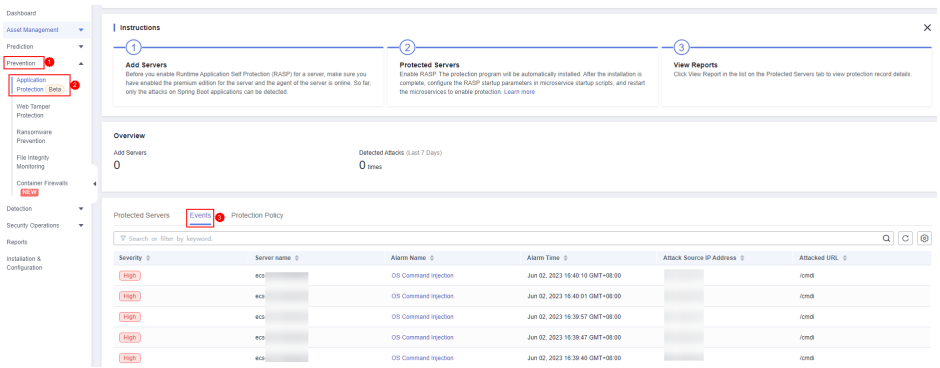
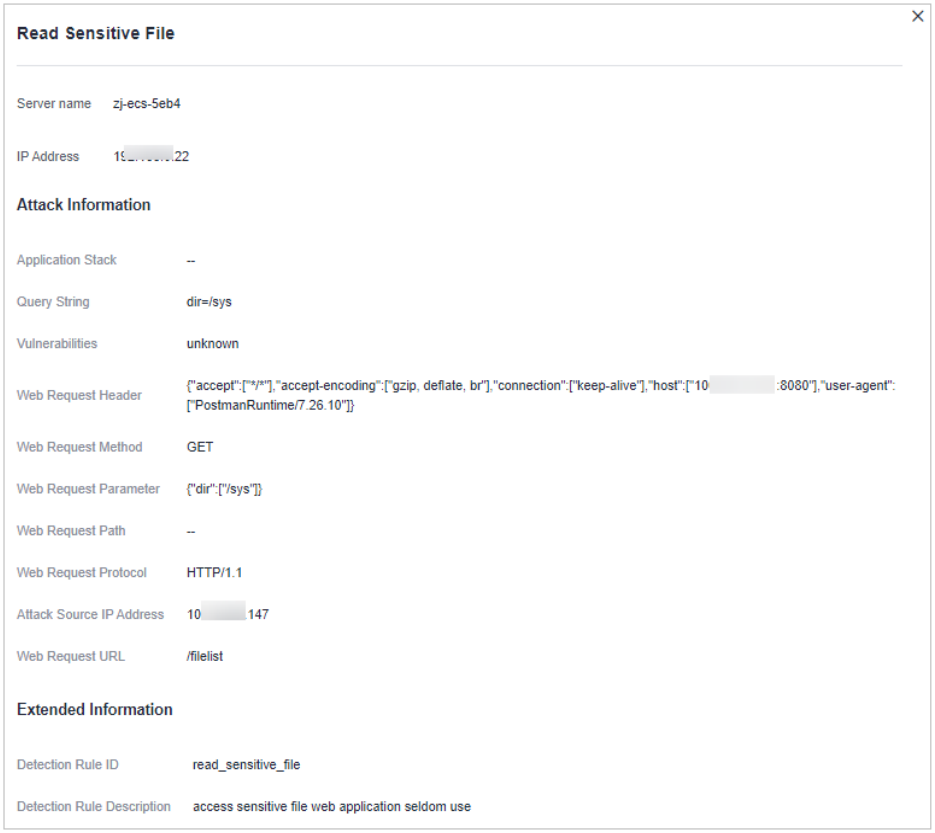


Tabela 5-2 Parâmetros do evento

Parâmetro	Descrição
Severity	Gravidade do alarme
Server Name	Servidor que aciona um alarme
Alarm Name	Nome do alarme
Alarm Time	Hora em que um alarme é informado
Attack Source IP Address	Endereço IP do servidor que aciona o alarme
Attack Source URL	URL do servidor que aciona o alarme

Passo 3 Você pode clicar em um nome de alarme para visualizar as informações do ataque (como as informações de solicitação e o endereço IP da origem do ataque) e informações estendidas (como ID e descrição da regra de detecção) e solucionar o problema adequadamente.

Figura 5-4 Visualização de eventos



----Fim

5.1.2 Habilitação da proteção de aplicações

Pré-requisito

Você ativou a edição premium, WTP ou de container do HSS.

Restrições

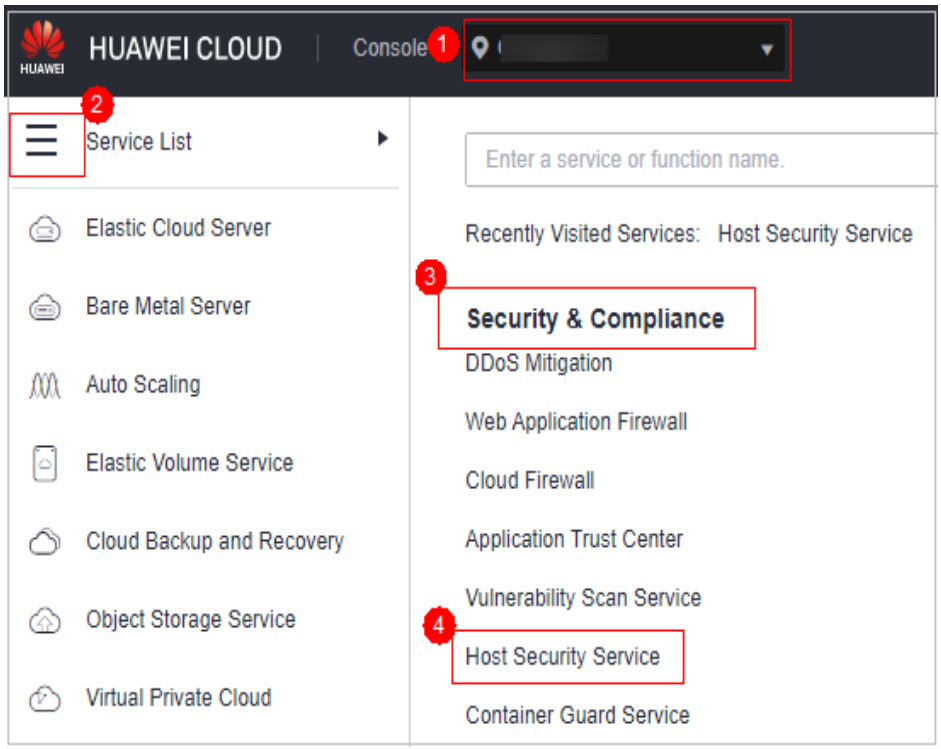
- Atualmente, apenas servidores do Linux são suportados.
- Até agora, apenas aplicações de Java podem ser protegidas.
- As edições premium e superiores suportam operações relacionadas à proteção de aplicações.

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 5-5 Acessar o HSS

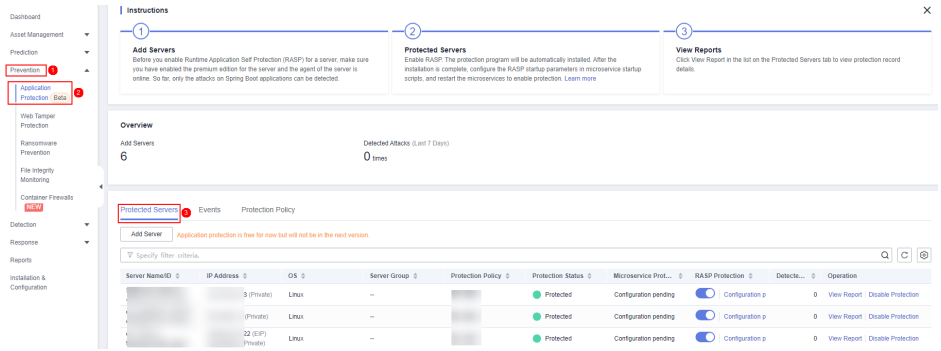


Passo 3 Escolha **Prevention** > **Application Protection**. Clique na guia **Protected Servers**.

NOTA

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

Figura 5-6 Visualização de configurações de proteção

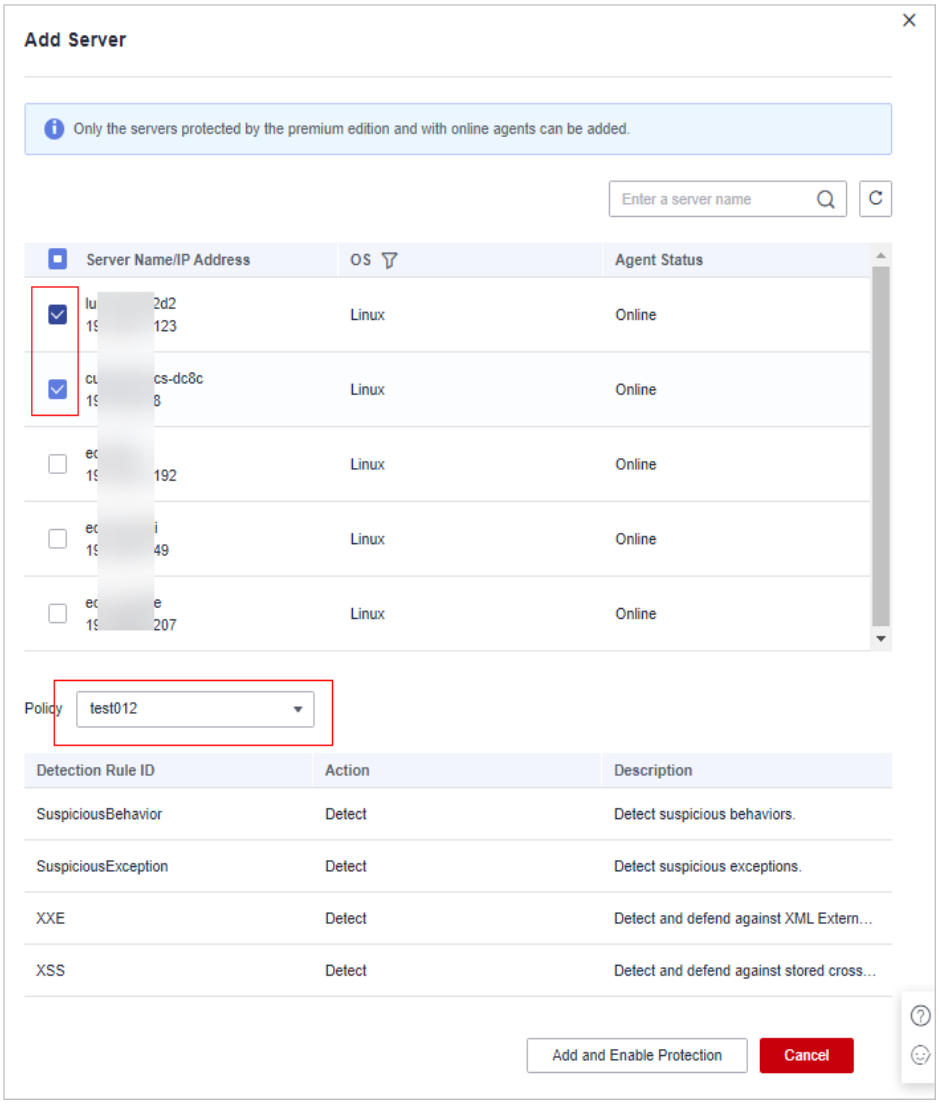


Passo 4 Clique em **Add Server**. Selecione servidores na caixa de diálogo exibida.

NOTA

Você pode selecionar uma política de segurança padrão ou criar uma política de segurança.

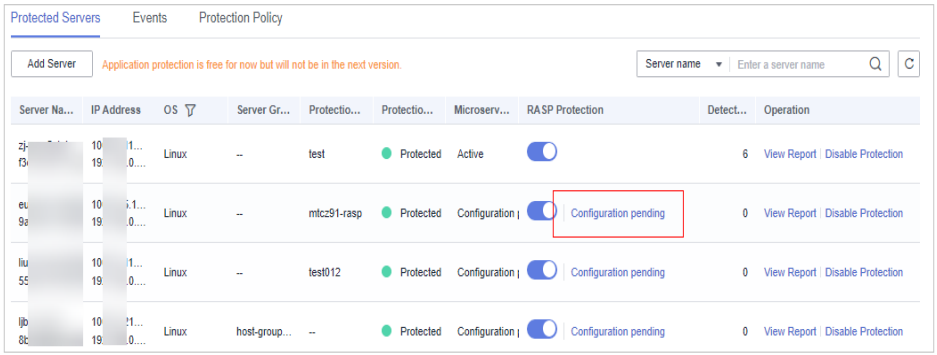
Figura 5-7 Selecionar o servidor de destino e a política



Passo 5 Clique em **Add and Enable Protection**.

Passo 6 Na guia **Protected Servers**, clique no status na coluna **RASP Protection**.

Figura 5-8 Visualizar o progresso da ativação da proteção

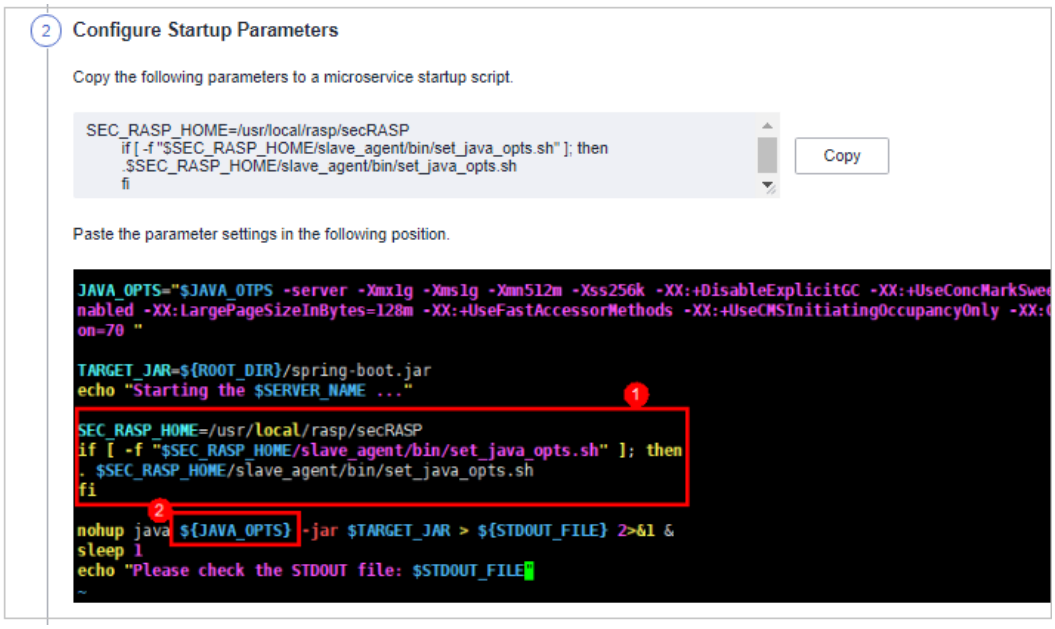


Passo 7 Verifique o progresso da instalação do software RASP. Aguarde até que a mensagem "Installation completed." seja exibida.

Figura 5-9 Instalação concluída

Passo 8 Efetue logon no servidor, vá para o caminho de inicialização do Spring Boot e copie os parâmetros da etapa **Configure Startup Parameters** para a caixa de comando.

Figura 5-10 Configurar parâmetros de inicialização



Passo 9 Reinicie o microsserviço para aplicar as configurações de proteção.

Passo 10 Na guia **Protected Servers**, verifique o status da proteção na coluna **Microservice Protection**. Se o status for **Active**, a proteção foi ativada.

----Fim

5.1.3 Gerenciamento da proteção de aplicações

Pré-requisito

Você ativou a edição premium, WTP ou de container do HSS.

Restrições

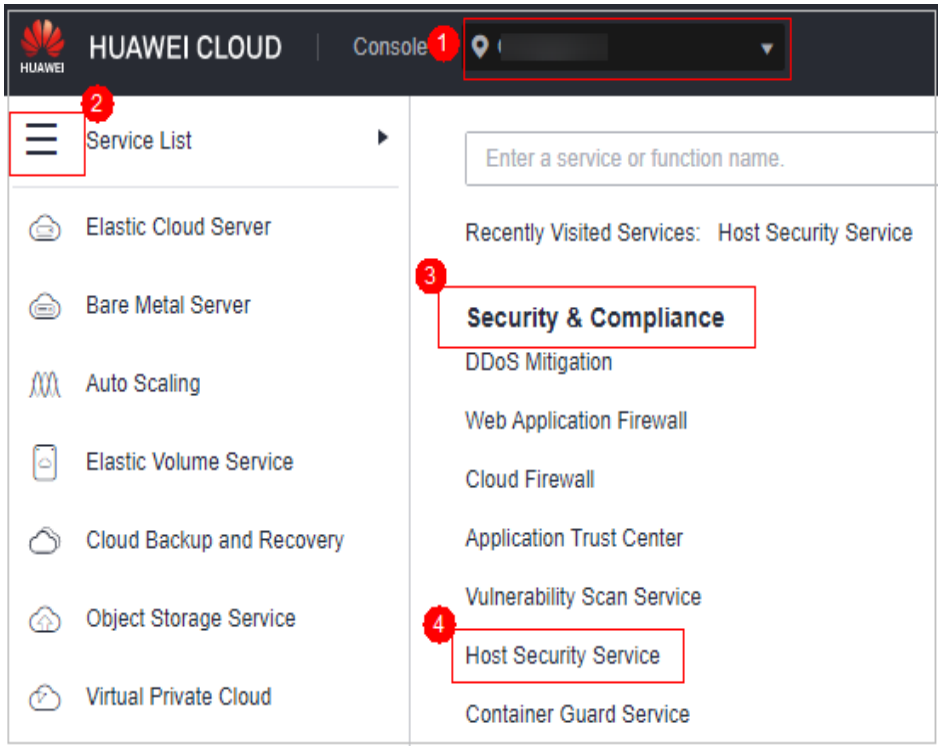
- Atualmente, apenas servidores do Linux são suportados.
- Até agora, apenas aplicações de Java podem ser protegidas.
- As edições premium e superiores suportam operações relacionadas à proteção de aplicações.

Visualizar o relatório

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**.

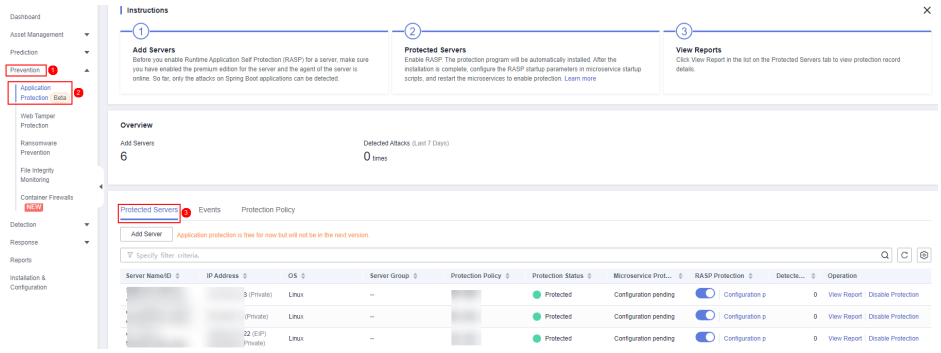
Figura 5-11 Acessar o HSS



Passo 3 Escolha **Prevention** > **Application Protection**. Clique na guia **Protected Servers**.

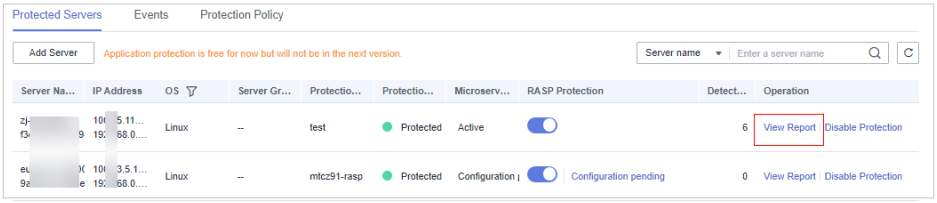
> **NOTA**
>
> If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figura 5-12 Visualização de configurações de proteção



Passo 4 Clique em **View Report** na coluna **Operation** de um servidor para exibir os detalhes da detecção.

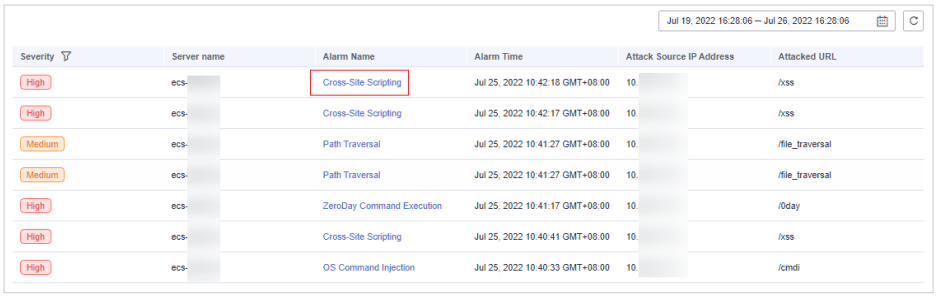
Figura 5-13 Visualizar um relatório



Passo 5 Clique em um nome de alarme para exibir seus detalhes.

Você pode visualizar as informações de ataque (como informações de solicitação e endereço IP de origem do ataque) e informações estendidas (como regras de detecção e investigações) e solucionar o problema de acordo.

Figura 5-14 Visualizar detalhes do alarme



----Fim

5.1.4 Desativação da proteção de aplicações

Pré-requisito

Você ativou a edição premium, WTP ou de container do HSS.

Restrições

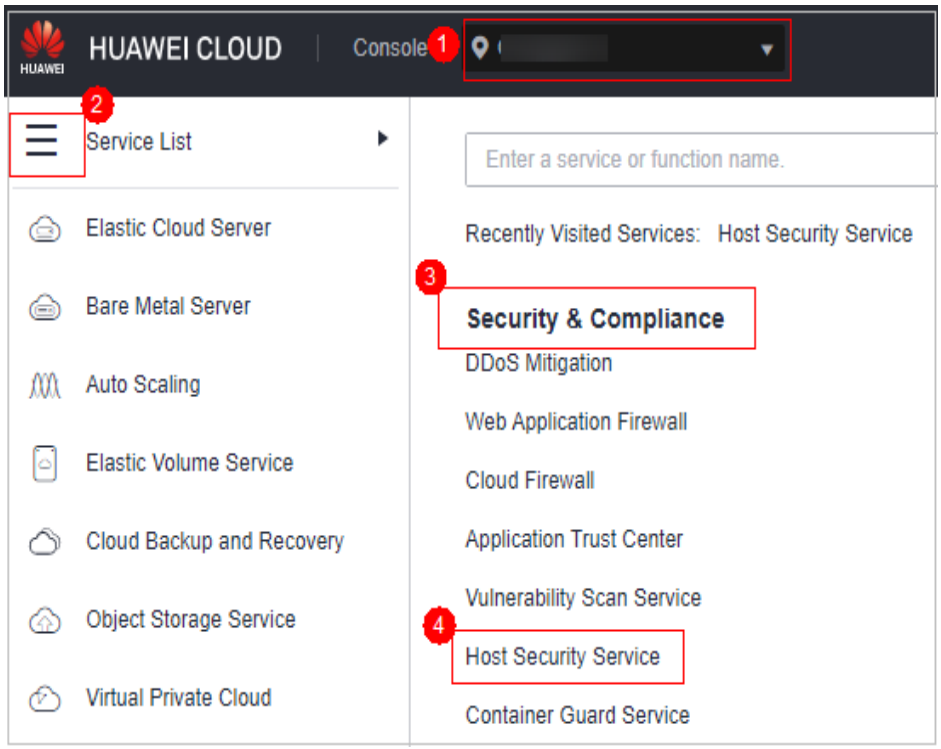
- Atualmente, apenas servidores do Linux são suportados.
- Até agora, apenas aplicações de Java podem ser protegidas.
- As edições premium e superiores suportam operações relacionadas à proteção de aplicações.

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 5-15 Acessar o HSS

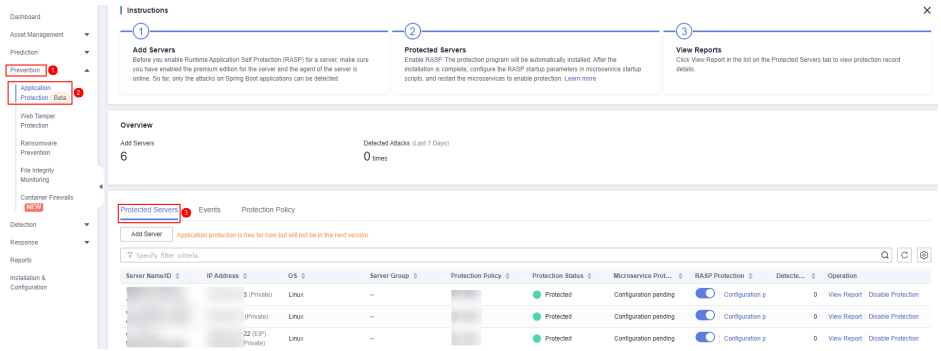


Passo 3 Escolha **Prevention** > **Application Protection**. Clique na guia **Protected Servers**.

NOTA

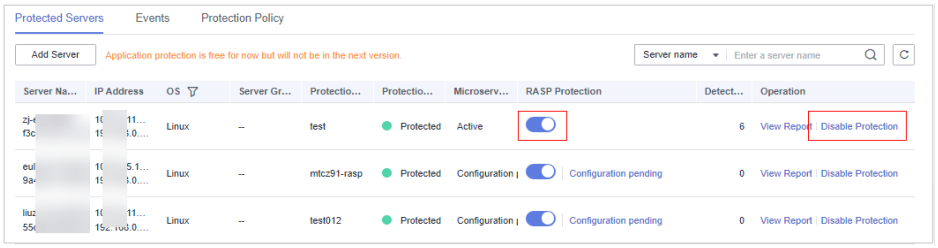
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figura 5-16 Visualização de configurações de proteção



Passo 4 Desative a opção de  na coluna **RASP Protection** ou clique em **Disable Protection** na coluna **Operation**.

Figura 5-17 Desativar a proteção



Passo 5 Na caixa de diálogo exibida, confirme as informações do servidor e clique em **OK**.

NOTA

Depois que RASP for desativada para um servidor, o servidor será removido da guia **Protected Servers**. Para obter detalhes sobre como ativar a proteção, consulte **Habilitação da proteção de aplicações**.

----Fim

5.1.5 Gerenciamento de políticas

Você pode adicionar, editar e excluir políticas de proteção de aplicações e selecionar e configurar regras de detecção para as políticas.

Restrições

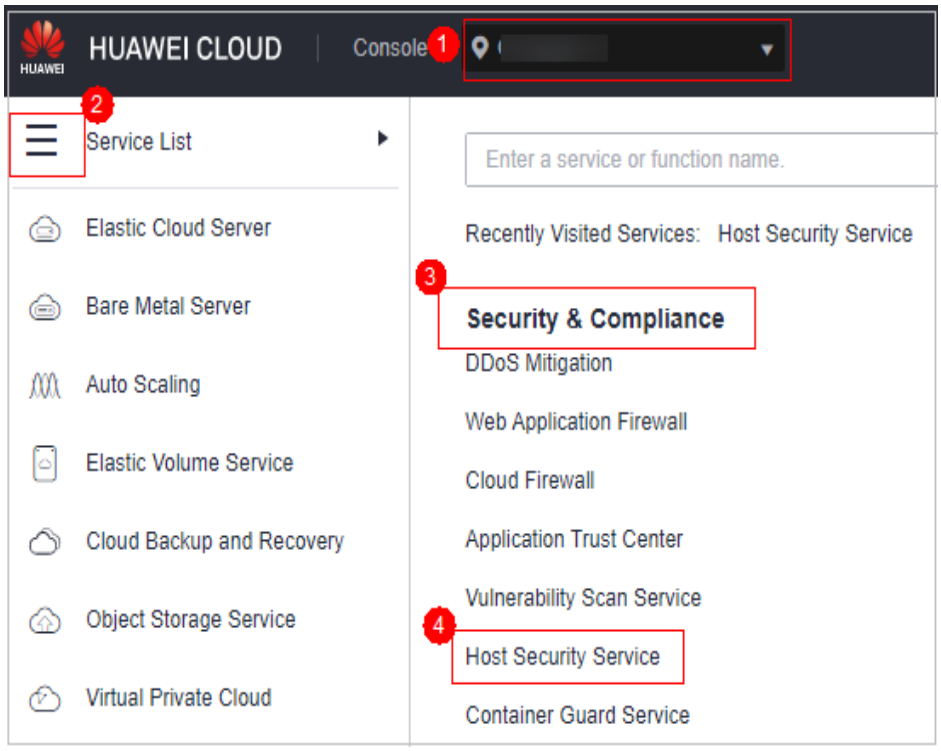
- Atualmente, apenas servidores do Linux são suportados.
- Até agora, apenas aplicações de Java podem ser protegidas.
- Você ativou a edição premium, WTP ou de container do HSS.

Adicionar uma política de 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 5-18 Acessar o HSS



Passo 3 Escolha **Prevention** > **Application Protection** e clique em **Protection Policies**. Para obter detalhes sobre os parâmetros, consulte **Tabela 5-3**.

NOTA

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

Figura 5-19 Políticas de proteção

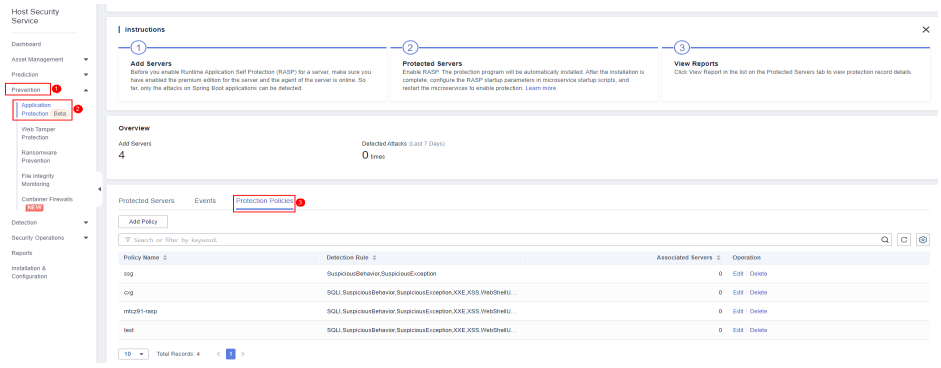


Tabela 5-3 Parâmetros da política de proteção

Parâmetro	Descrição
Policy Name	Nome da política de proteção
Detection Rule	Regras de detecção suportadas por uma política.

Parâmetro	Descrição
Associated Servers	Número de servidores vinculados a uma política.

Passo 4 Clique em **Add Policy**. Na caixa de diálogo exibida, insira o nome da política, selecione as regras a serem detectadas e configure detalhes sobre algumas regras de detecção. Para obter detalhes sobre os parâmetros, consulte **Tabela 5-4**.

Figura 5-20 Adicionar uma política de proteção

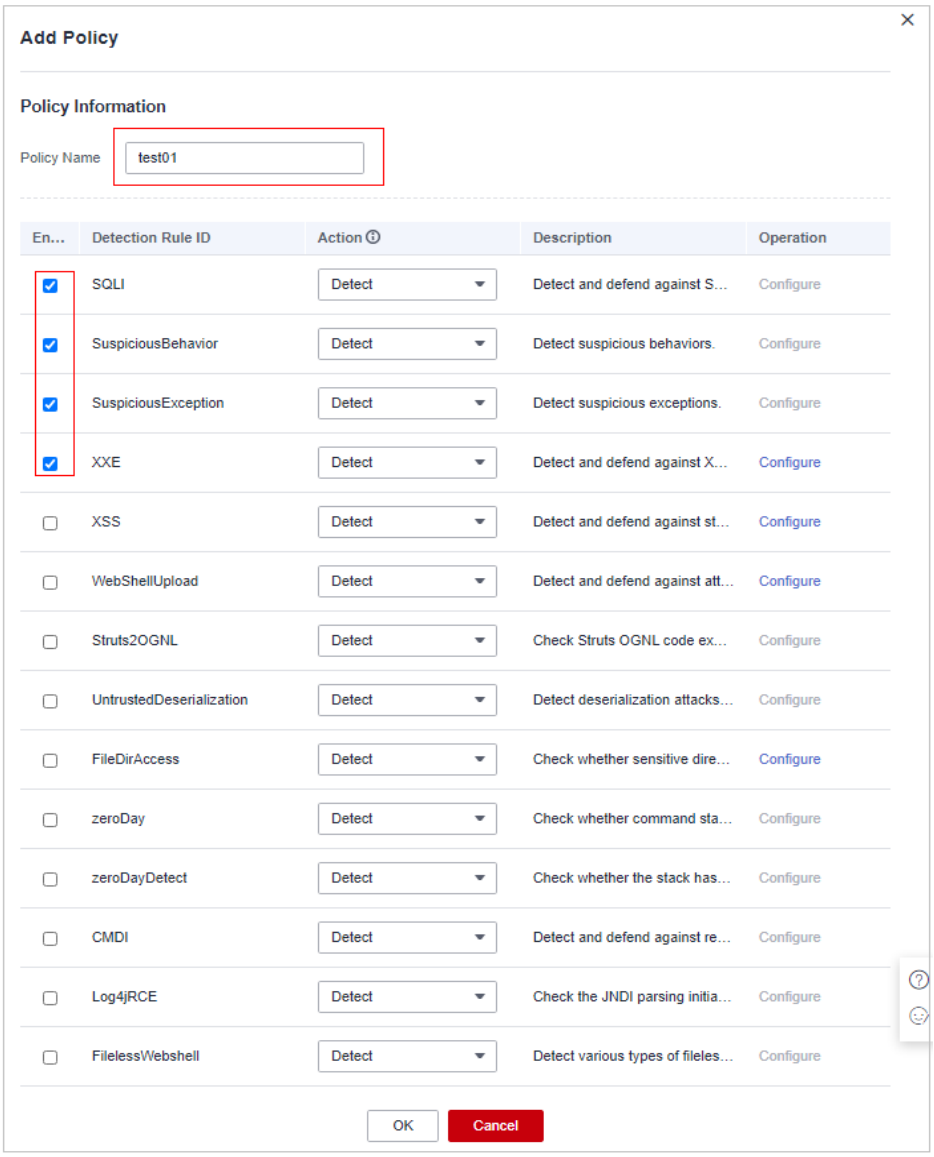


Tabela 5-4 Parâmetros da política de proteção de aplicações

Parâmetro	Descrição
Policy Name	Nome da política definida pelo usuário

Parâmetro	Descrição
Enabled	Se deve ativar uma regra de detecção para a política atual. Você pode selecionar regras de detecção para ativá-las conforme necessário.
Detection Rule ID	ID de uma regra de detecção
Action	Ação de proteção de uma regra de detecção. ● **Detect**: detecta objetos com base na regra de destino e relata alarmes para eventos de risco detectados. ● **Detect and block**: detecta objetos com base na regra de destino, relata alarmes para eventos de risco detectados e bloqueia ou intercepta diretamente itens de risco detectados. **AVISO** Bloqueio ou interceptação pode interromper os serviços. Tenha cuidado ao ativar esta função
Description	Descrição sobre o objeto detectado e o comportamento da política de proteção de destino.

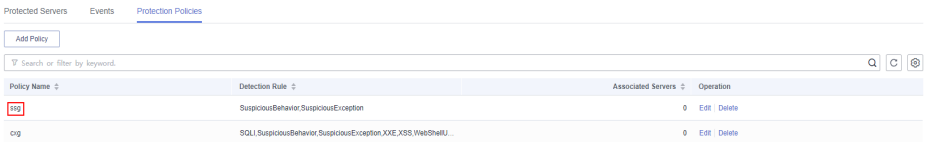
Passo 5 Clique em **Configure** na coluna **Operation** de uma regra de detecção para modificar o conteúdo da regra. **Tabela 5-5** descreve as regras de detecção suportadas.

Tabela 5-5 Regras de detecção que podem ser configuradas

Regra	Descrição	Exemplo
XXE	Protocolo de lista negra de XXE definido pelo usuário	.xml;.dtd;
XSS	Regras de blindagem de XSS definidas pelo usuário	xml;doctype;xmlns;import;entity
WebShellUpload	Sufixo definido pelo usuário de arquivos na lista negra.	.jspx;.jsp;.jar;.phtml;.asp;.php;.ascx;.ashx;.cer
FileDirAccess	Caminho definido pelo usuário dos arquivos na lista negra.	/etc/passwd;/etc/shadow;/etc/gshadow;

Passo 6 Confirme a política configurada e as regras de detecção selecionadas e clique em **OK**. Você pode verificar se a regra é adicionada na página de guia **Protection Policy**.

Figura 5-21 Exibição da política de proteção adicionada



----Fim

Editar uma política de proteção

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 Escolha **Prevention** > **Application Protection** e clique em **Protection Policies**. Para obter detalhes sobre os parâmetros, consulte **Tabela 5-6**.

NOTA

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

Figura 5-22 Políticas de proteção

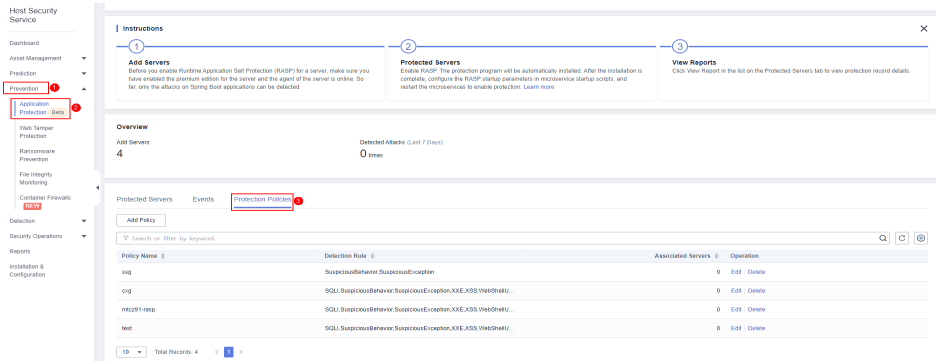


Tabela 5-6 Parâmetros da política de proteção

Parâmetro	Descrição
Policy Name	Nome da política de proteção
Detection Rule	Regras de detecção suportadas por uma política.
Associated Servers	Número de servidores vinculados a uma política.

Passo 3 Clique em **Edit** na coluna **Operation** de uma política para configurar o nome da política, as regras de detecção suportadas e o conteúdo da regra.

Figura 5-23 Edição de uma política de proteção

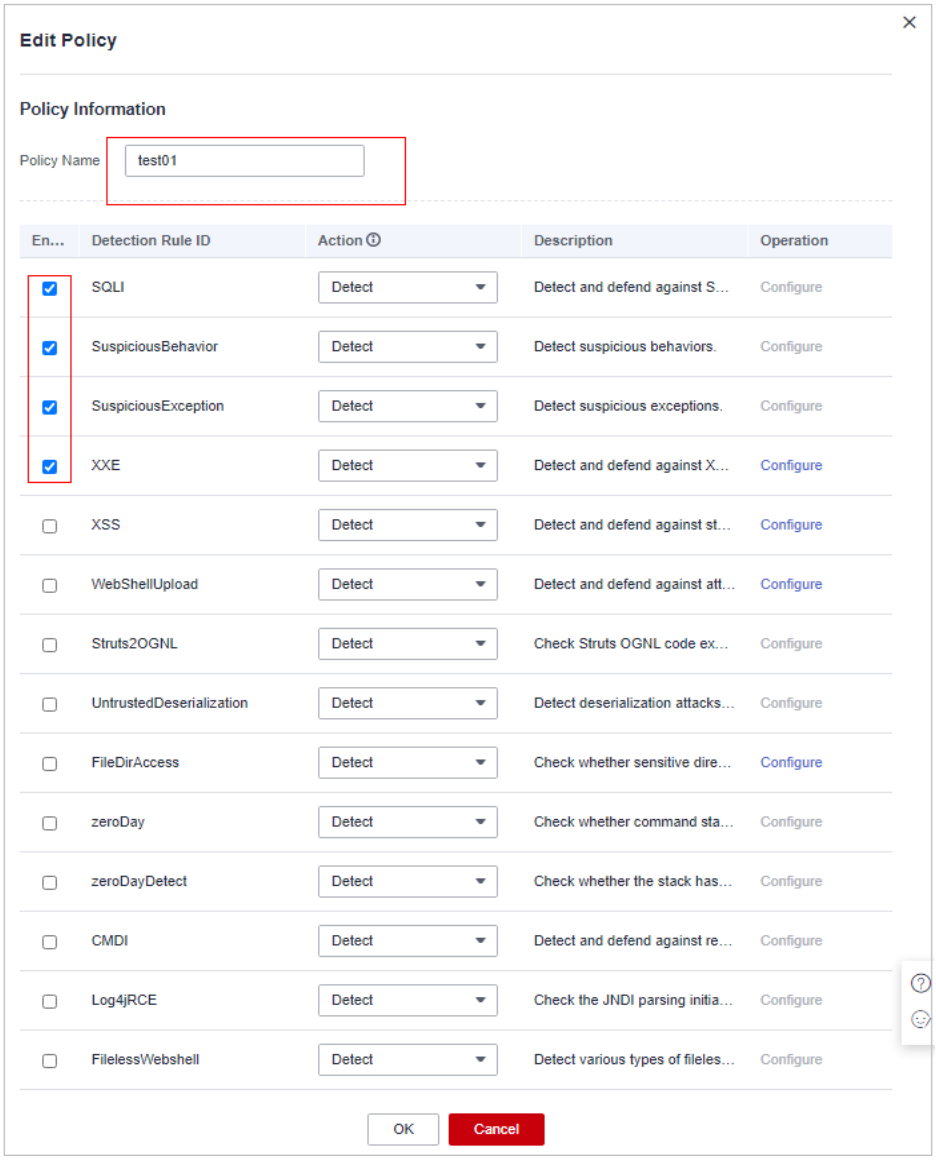


Tabela 5-7 Parâmetros da política de proteção de aplicações

Parâmetro	Descrição
Policy Name	Nome da política definida pelo usuário
Enabled	Se deve ativar uma regra de detecção para a política atual. Você pode selecionar regras de detecção para ativá-las conforme necessário.
Detection Rule ID	ID de uma regra de detecção

Parâmetro	Descrição
Action	Ação de proteção de uma regra de detecção. ● **Detect**: detecta objetos com base na regra de destino e relata alarmes para eventos de risco detectados. ● **Detect and block**: detecta objetos com base na regra de destino, relata alarmes para eventos de risco detectados e bloqueia ou intercepta diretamente itens de risco detectados. **AVISO** Bloqueio ou interceptação pode interromper os serviços. Tenha cuidado ao ativar esta função
Description	Descrição sobre o objeto detectado e o comportamento da política de proteção de destino.

Passo 4 Confirme a regra configurada e os itens de detecção selecionados e clique em **OK**. Você pode verificar se a política de destino foi modificada na página de guia **Protection Policy**.

----Fim

Excluir uma política

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 Escolha **Prevention** > **Application Protection** e clique em **Protection Policies**. Para obter detalhes sobre os parâmetros, consulte **Tabela 5-8**.

NOTA

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

Figura 5-24 Políticas de proteção

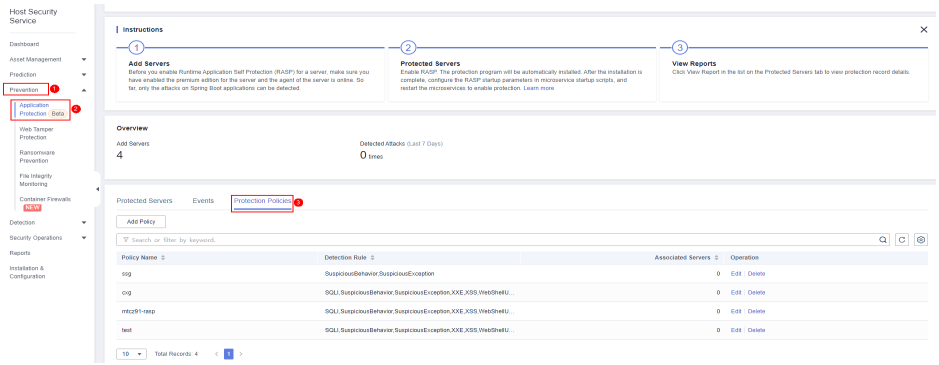


Tabela 5-8 Parâmetros da política de proteção

Parâmetro	Descrição
Policy Name	Nome da política de proteção
Detection Rule	Regras de detecção suportadas por uma política.

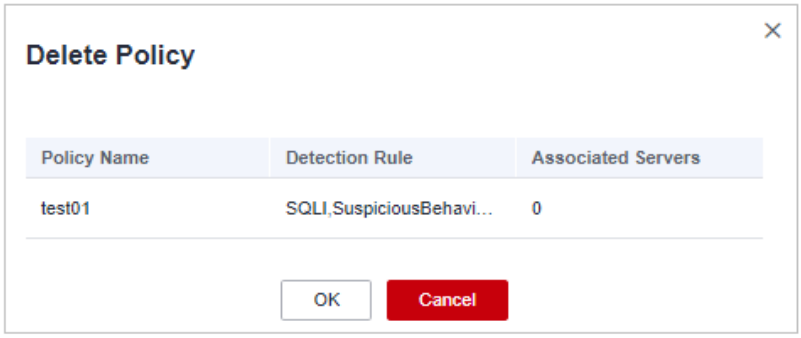
Parâmetro	Descrição
Associated Servers	Número de servidores vinculados a uma política.

Passo 3 Clique em **Delete** na coluna **Operation** da política de destino. Na caixa de diálogo exibida, confirme as informações da política e clique em **OK**.

AVISO

Se a política a ser excluída estiver vinculada a um servidor, vincule o servidor a outra política de proteção primeiro. Caso contrário, o botão **Delete** da política de destino ficará oculto.

Figura 5-25 Exclusão de uma política



----Fim

5.2 WTP

5.2.1 Adição de um diretório protegido

A WTP monitora diretórios de sites em tempo real, faz backup de arquivos e restaura arquivos adulterados usando o backup, protegendo sites de cavalos de Troia, links ilegais e adulteração.

Pré-requisitos

Você ativou a edição WTP.

Restrições

- Apenas os servidores protegidos pela edição WTP do HSS suportam as operações descritas nesta seção.
- As restrições nos diretórios protegidos são as seguintes:
  - Para o Linux,
    - Um servidor pode ter até 50 diretórios protegidos.
    - O caminho completo de um diretório protegido não pode exceder 256 caracteres.

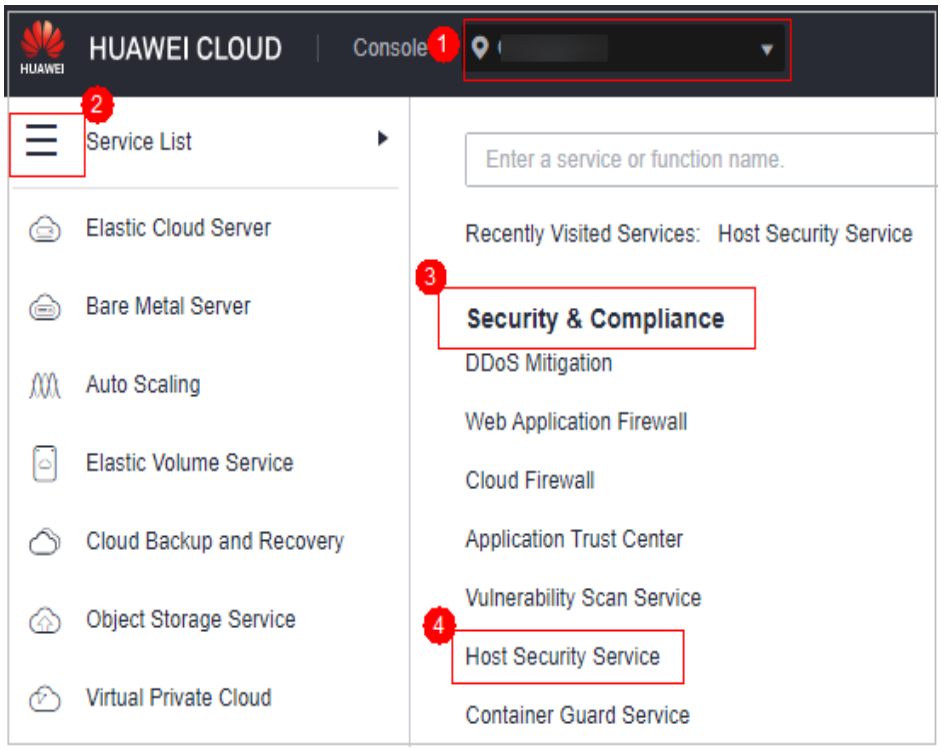
    - Os níveis de pasta de um diretório protegido não podem exceder 100.
    - O total de pastas em diretórios protegidos não pode exceder 900.000.
  - Para o Windows,
    - Um servidor pode ter até 50 diretórios protegidos.
    - O caminho completo de um diretório protegido não pode exceder 256 caracteres.
- As restrições nos caminhos de backup local são as seguintes:
  - O backup local é suportado apenas no Linux.
  - O caminho de backup local deve ser válido, ou a proteção contra adulteração da Web não terá efeito.
  - O caminho de backup local não pode se sobrepor ao diretório protegido adicionado.
  - A capacidade disponível do disco onde o caminho de backup local está localizado é maior do que o tamanho de todos os diretórios protegidos.

Adição de 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 5-26 Acessar o HSS

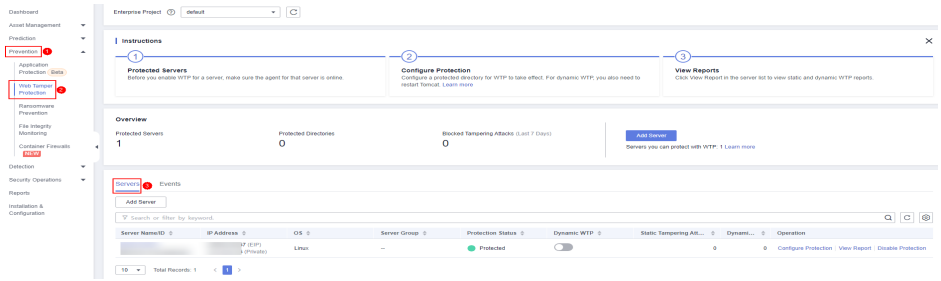


Passo 3 Escolha **Prevention** > **Web Tamper Protection**, clique em **Configure Protection**.

NOTA

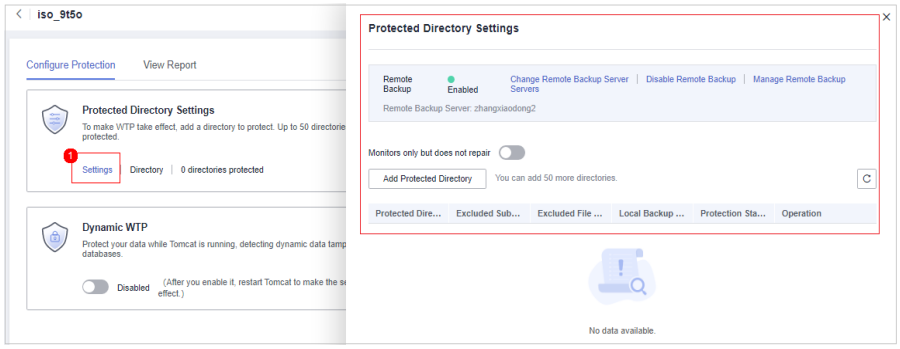
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figura 5-27 Entrar na página para configurações de diretório protegido



Passo 4 Clique em **Settings** em **Protected Directory Settings**.

Figura 5-28 Página para definir um diretório protegido



Passo 5 Você pode adicionar um máximo de 50 diretórios protegidos.

1. Clique em **Add**. Na caixa de diálogo **Add Protected Directory**, defina os parâmetros necessários. Para mais detalhes, consulte **Tabela 5-9**.

Figura 5-29 Adicionar um diretório protegido

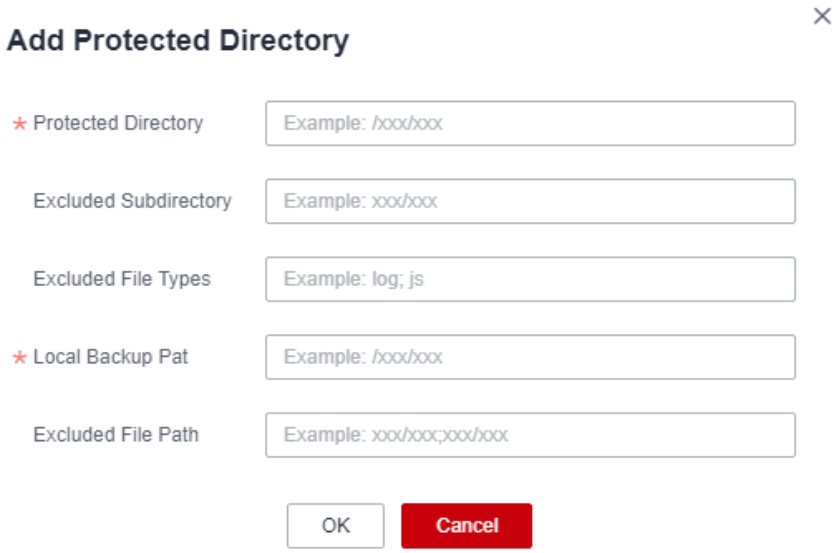


Tabela 5-9 Parâmetros para um diretório protegido

Parâmetro	Descrição	Restrição
Protected Directory	Arquivos e pastas neste diretório são somente leitura.	Não configurá-lo para nenhum diretório do SO.
Excluded Subdirectory	– Subdiretórios que não precisam ser protegidos no diretório protegido, como diretórios de arquivos temporários. – Separe os subdiretórios com ponto e vírgula (;). Um máximo de 10 subdiretórios podem ser adicionados.	O subdiretório é um diretório relativo no diretório protegido.
Excluded File Types	– Tipos de arquivos que não precisam ser protegidos no diretório protegido, como arquivos de log. – Separe os tipos de arquivos com ponto e vírgula (;). – Para registrar o status de execução do servidor em tempo real, exclua os arquivos de log no diretório protegido. Você pode conceder altas permissões de leitura e gravação para arquivos de log para impedir que invasores visualizem ou adulterem os arquivos de log.	-

Parâmetro	Descrição	Restrição
Local Backup Path	– Somente Linux é suportado. – Depois que a WTP é ativada, o backup dos arquivos no diretório protegido é feito automaticamente no caminho de backup local. – Geralmente, o backup é concluído em 10 minutos. A duração real depende do tamanho dos arquivos no diretório protegido. A proteção entra em vigor imediatamente quando o backup é concluído. – Não é feito o backup de subdiretórios e tipos de arquivos excluídos. – Se a WTP detectar que um arquivo em um diretório protegido foi adulterado, ela usará imediatamente o arquivo de backup no servidor local para restaurar o arquivo.	O caminho de backup local não pode se sobrepor ao diretório protegido adicionado.
Excluded File Path	– Caminhos que não precisam ser protegidos no diretório protegido. – Separe vários caminhos com ponto e vírgula (;). Um máximo de 50 caminhos podem ser adicionados. O comprimento máximo de um caminho é de 256 caracteres. – Um único caminho não pode começar com um espaço ou terminar com uma barra (/).	O caminho de arquivo excluído é o caminho de arquivo relativo do diretório protegido.

2. Clique em **OK**.

   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.

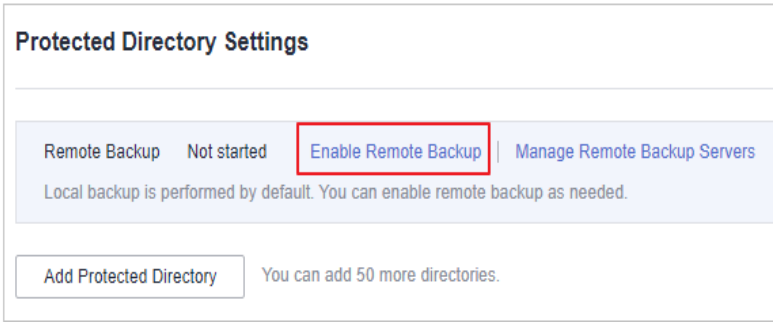
Passo 6 Habilite o backup remoto.

Por padrão, o HSS faz backup dos arquivos dos diretórios protegidos (excluindo subdiretórios e tipos de arquivos especificados) para o diretório de backup local especificado ao adicionar diretórios protegidos. Para proteger os arquivos de backup locais contra adulteração, você deve habilitar a função de backup remoto.

Para obter detalhes sobre como adicionar um servidor de backup remoto, consulte **Gerenciamento de servidores de backup remotos**.

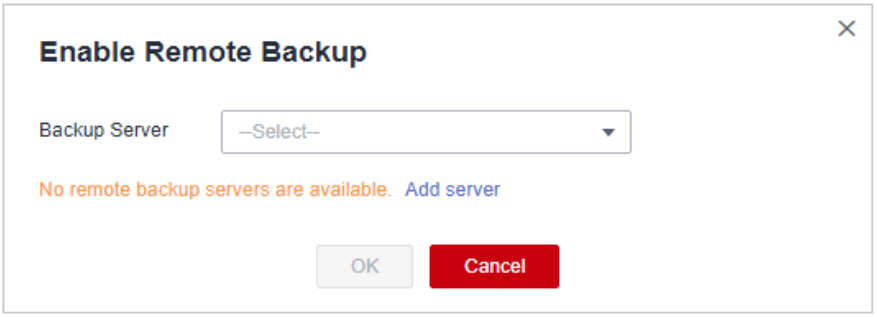
1. Na página **Protected Directory Settings**, clique em **Enable Remote Backup**.

   Figura 5-30 Habilitar o backup remoto

2. Selecione um servidor de backup na caixa de listagem suspensa.

   Figura 5-31 Configurar o backup remoto

3. Clique em **OK**.

----Fim

Procedimento de acompanhamento

- Exportar um diretório protegido: se você tiver configurado um grande número de diretórios protegidos, poderá clicar em  na página de configuração do diretório protegido para exportar as configurações de todos os diretórios protegidos para o seu PC local.
- Suspender a proteção: você pode suspender a WTP para um diretório, se necessário. Recomenda-se que você retome a WTP em tempo hábil para evitar que os arquivos no diretório sejam adulterados.
- Editar um diretório protegido: você pode modificar o diretório protegido adicionado conforme necessário.
- Excluir um diretório protegido: você pode excluir os diretórios que não precisam ser protegidos.

AVISO

- Depois que você suspender a proteção de um diretório protegido, excluí-lo ou modificar seu caminho, os arquivos no diretório não estarão mais protegidos. Antes de executar essas operações, verifique se você tomou outras medidas para proteger os arquivos.
- Depois de suspender a proteção de um diretório protegido, excluí-lo ou modificar seu caminho, se você encontrar os arquivos ausentes no diretório, pesquise-os no caminho de backup local ou remoto.

5.2.2 Gerenciamento de servidores de backup remotos

Por padrão, o HSS faz backup dos arquivos dos diretórios protegidos (excluindo subdiretórios e tipos de arquivos especificados) para o diretório de backup local especificado ao adicionar diretórios protegidos. Para proteger os arquivos de backup locais contra adulteração, você deve ativar a função de backup remoto.

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.

Restrições

Apenas os servidores protegidos pela edição WTP do HSS suportam as operações descritas nesta seção.

Pré-requisitos

Os seguintes servidores podem ser usados como servidores de backup remoto:

Servidores do Linux da Huawei Cloud cujo **Server Status** está **Running** e o **Agent Status** está **Online**

AVISO

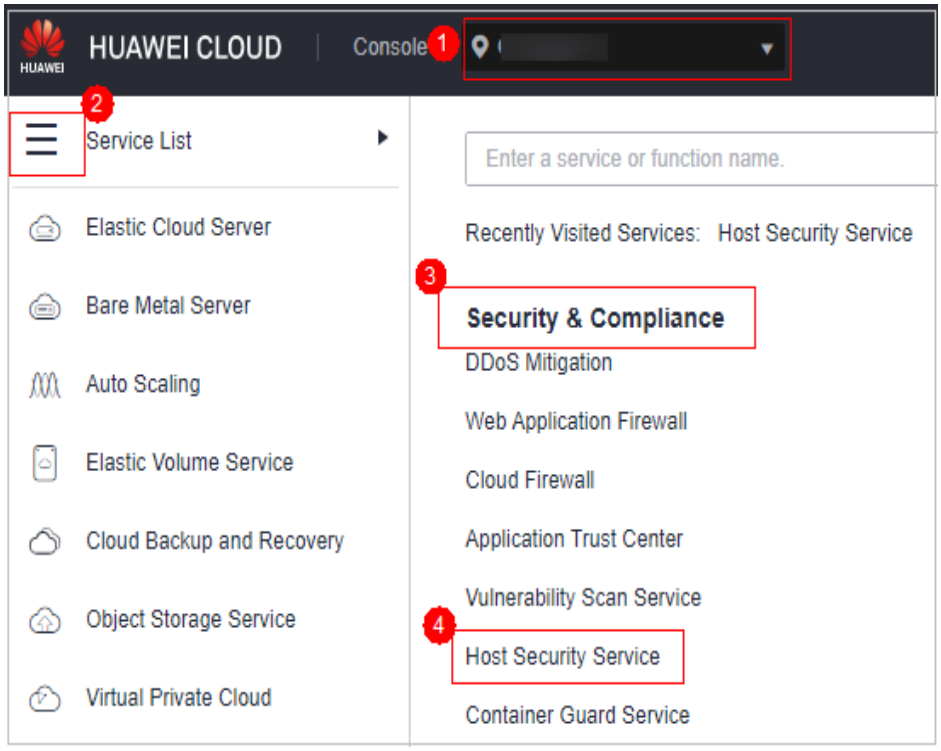
- A função de backup remoto pode ser usada quando o servidor de backup do Linux está conectado ao seu servidor de nuvem. Para garantir um backup adequado, é aconselhável selecionar um servidor de backup na mesma intranet que o seu servidor de nuvem.
- É aconselhável usar os servidores de intranet menos expostos a ataques como os servidores de backup remoto.

Adição de um servidor de backup remoto

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 5-32 Acessar o HSS

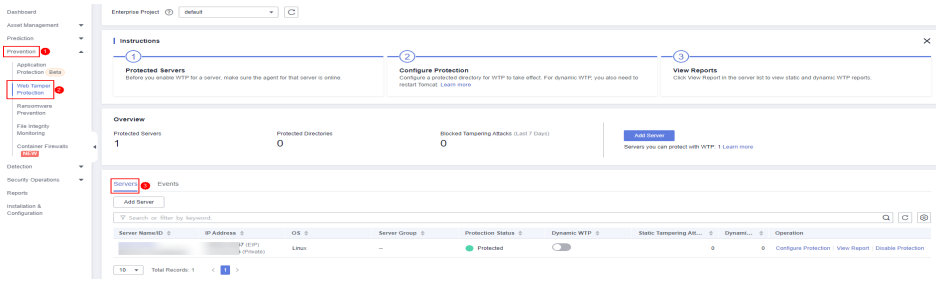


Passo 3 Escolha **Prevention** > **Web Tamper Protection**, clique em **Configure Protection**.

NOTA

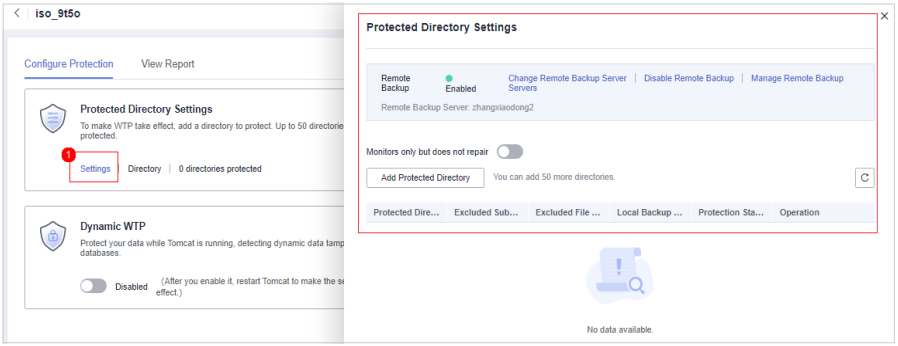
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figura 5-33 Entrar na página para configurações de diretório protegido



Passo 4 Clique em **Settings** em **Protected Directory Settings**.

Figura 5-34 Página para definir um diretório protegido



Passo 5 Clique em **Manage Remote Backup**. Na caixa de diálogo exibida, clique em **Add Backup Server**. Para mais detalhes, consulte **Tabela 5-10**.

Figura 5-35 Adição de um servidor de backup remoto

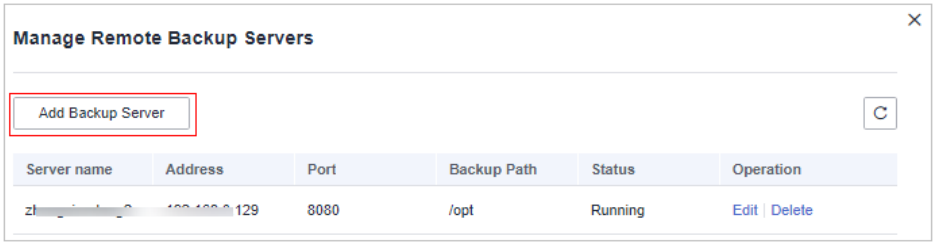


Figura 5-36 Configuração do servidor de backup

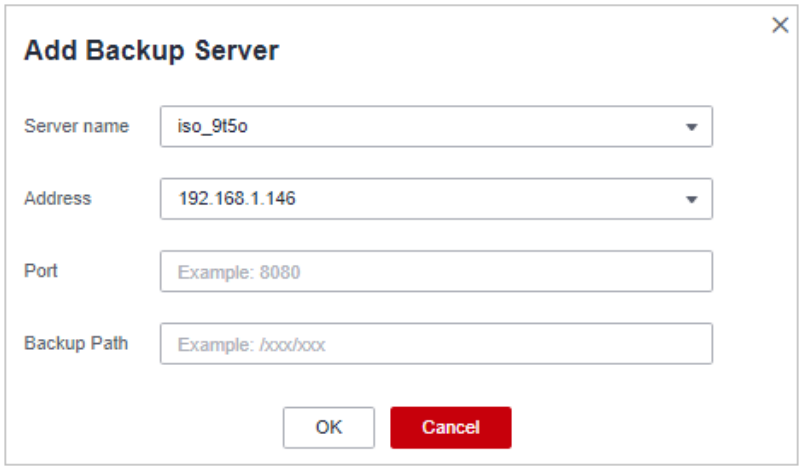


Tabela 5-10 Parâmetros do servidor de backup

Parâmetro	Descrição
Address	Este endereço é o endereço de rede privada do servidor da Huawei Cloud.
Port	Certifique-se de que a porta não esteja bloqueada por nenhum grupo de segurança ou firewall ou ocupada.

Parâmetro	Descrição
Backup Path	Caminho dos arquivos de backup remoto. ● Se o backup dos diretórios protegidos de vários servidores for feito no mesmo servidor de backup remoto, os dados serão armazenados em pastas separadas, nomeadas de acordo com os IDs de agente. Suponha que os diretórios protegidos dos dois servidores sejam **/hss01** e **hss02**, e os IDs de agente dos dois servidores são **f1fdbabc-6cdc-43af-acab-e4e6f086625f** e **f2ddbabc-6cdc-43af-abcd-e4e6f086626f**, e o caminho de backup remoto é **/hss01**. Os caminhos de backup correspondentes são **/hss01/f1fdbabc-6cdc-43af-acab-e4e6f086625f** e **/hss01/f2ddbabc-6cdc-43af-abcd-e4e6f086626f**. ● Se a WTP estiver ativada para o servidor de backup remoto, não defina o caminho de backup remoto para nenhum diretório protegido pela WTP. Caso contrário, o backup remoto falhará.

Passo 6 Clique em **OK**.

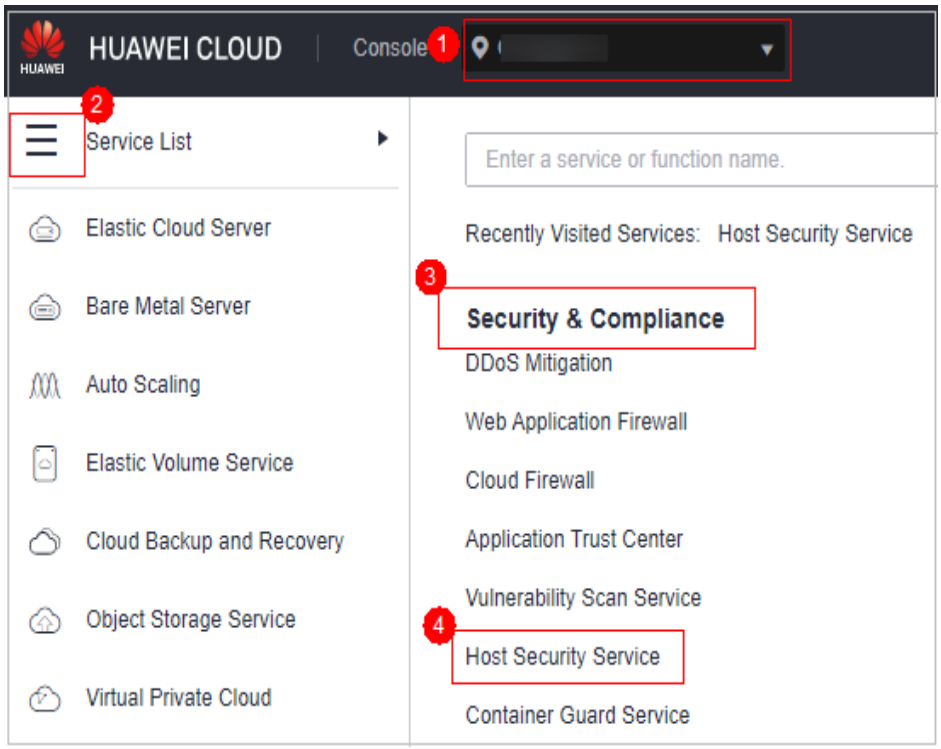
----Fim

Ativação do backup remoto

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 5-37 Acessar o HSS

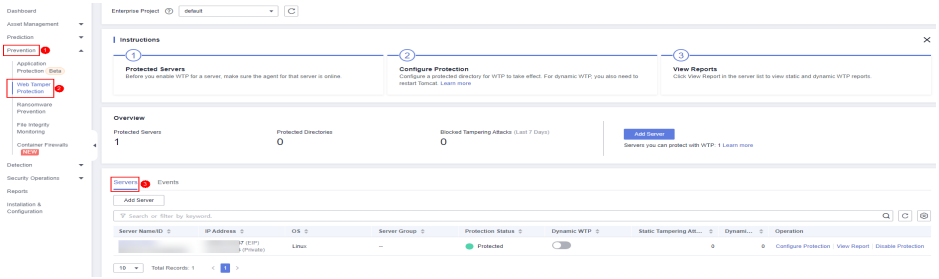


Passo 3 Escolha **Prevention** > **Web Tamper Protection**, clique em **Configure Protection**.

NOTA

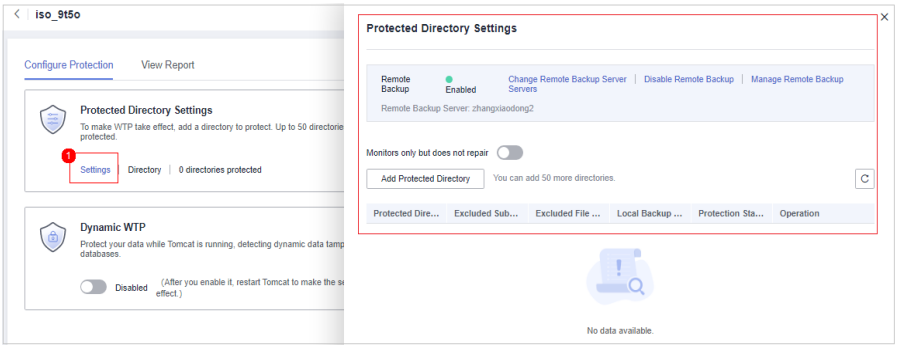
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figura 5-38 Entrar na página para configurações de diretório protegido



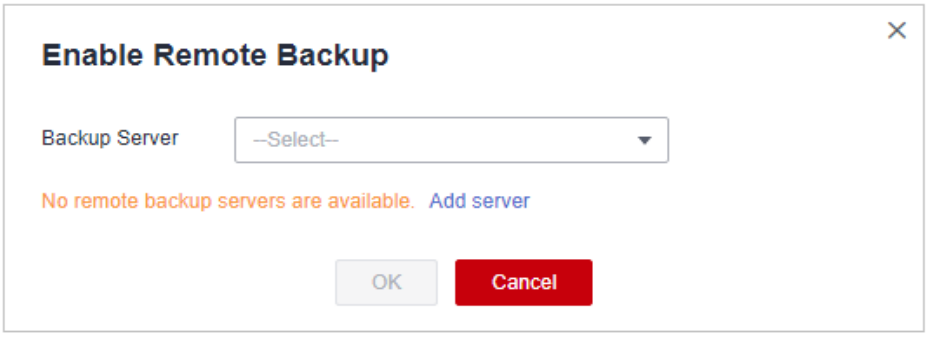
Passo 4 Clique em **Settings** em **Protected Directory Settings**.

Figura 5-39 Página para definir um diretório protegido



Passo 5 Clique em **Enable Remote Backup** e selecione um servidor de backup remoto.

Figura 5-40 Ativação do backup remoto



Passo 6 Clique em **OK** para iniciar o backup remoto.

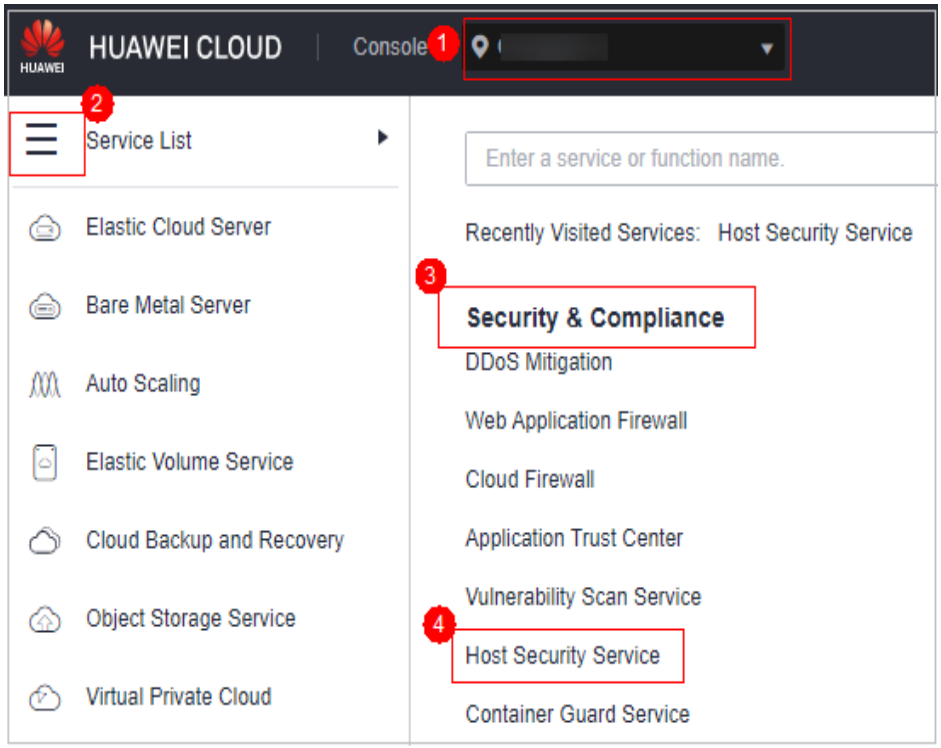
----Fim

Alteração de um servidor de backup remoto

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 5-41 Acessar o HSS

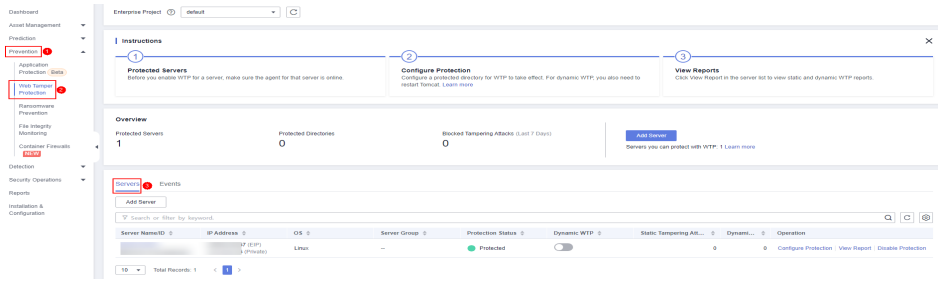


Passo 3 Escolha **Prevention** > **Web Tamper Protection**, clique em **Configure Protection**.

NOTA

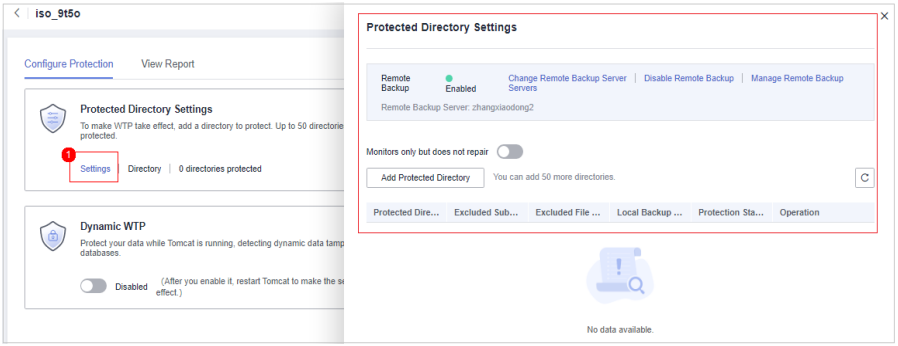
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figura 5-42 Entrar na página para configurações de diretório protegido



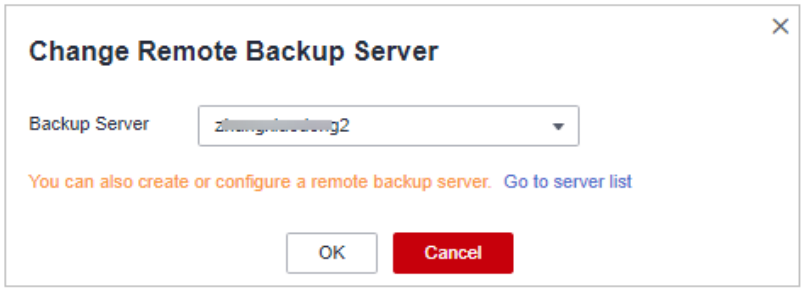
Passo 4 Clique em **Settings** em **Protected Directory Settings**.

Figura 5-43 Página para definir um diretório protegido



Passo 5 Clique em **Change Remote Backup Server**. Selecione um servidor de backup remoto na lista suspensa.

Figura 5-44 Alterar um servidor de backup remoto



Passo 6 Clique em **OK**.

----Fim

Procedimento de acompanhamento

Desativação do backup remoto

Tenha cuidado ao realizar esta operação. Se o backup remoto estiver desativado, o HSS não fará mais backup de arquivos em seus diretórios protegidos.

5.2.3 Configuração da proteção WTP programada

Você pode programar a proteção WTP para permitir atualizações do site em períodos específicos.

NOTA

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

Restrições

Apenas os servidores protegidos pela edição WTP do HSS suportam as operações descritas nesta seção.

Regras para definir um período desprotegido

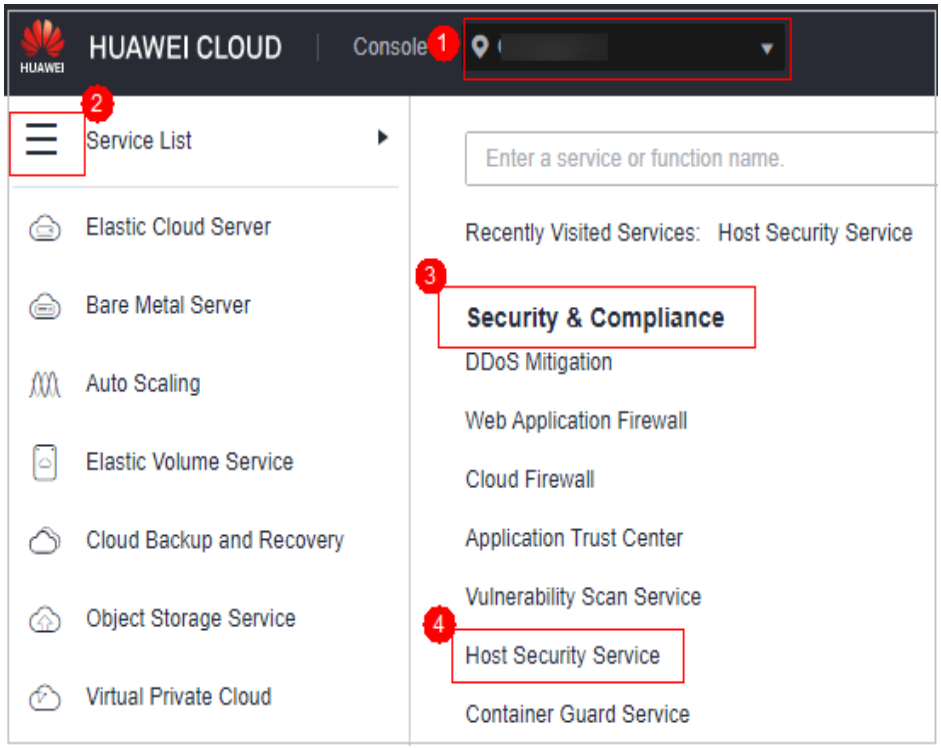
- Período desprotegido >= 5 minutos
- Período desprotegido < 24 horas
- Os períodos (exceto os que começam às 00:00 ou terminam às 23:59) não podem se sobrepor e devem ter um intervalo de pelo menos 5 minutos.
- Um período não pode abranger dois dias.
- A hora do servidor é usada como base de tempo.

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 5-45 Acessar o HSS

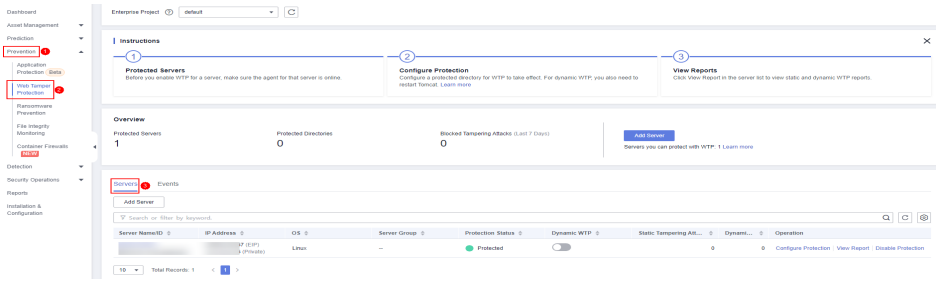


Passo 3 Escolha **Prevention** > **Web Tamper Protection**, clique em **Configure Protection**.

NOTA

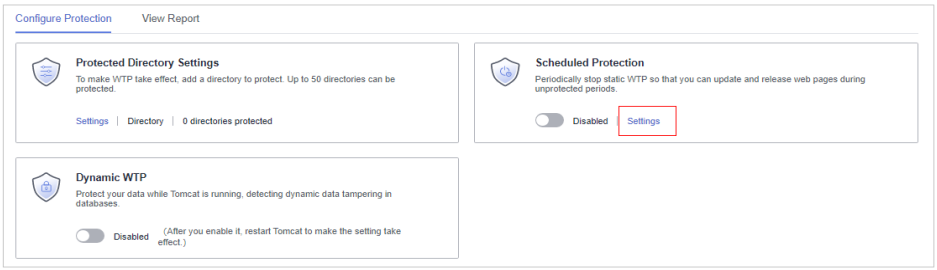
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figura 5-46 Entrar na página para configurações de diretório protegido



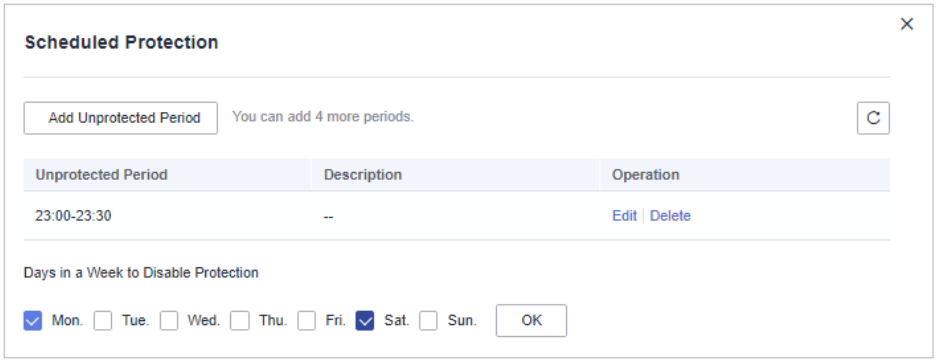
Passo 4 Na guia **Configure Protection**, clique em **Settings** em **Scheduled Protection**.

Figura 5-47 Configuração da proteção agendada



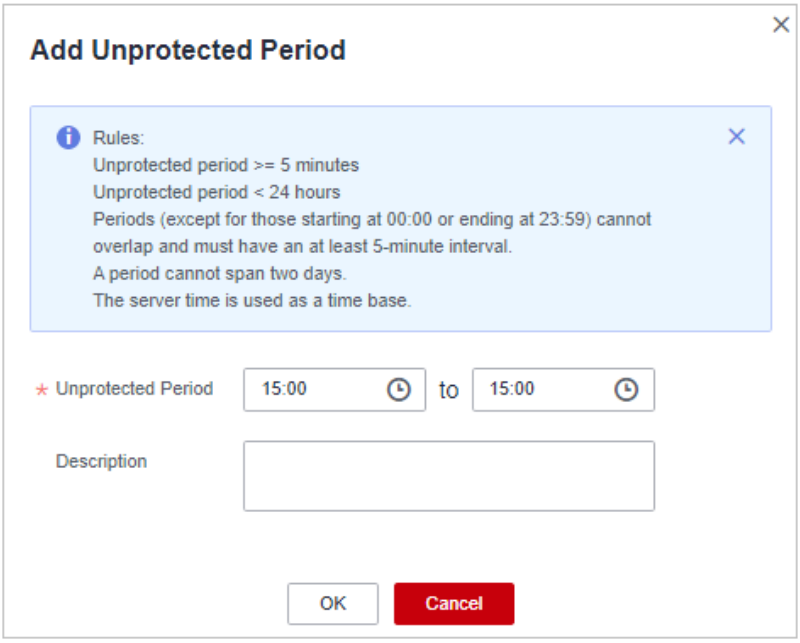
Passo 5 Defina o período desprotegido e os dias em uma semana para desativar automaticamente a proteção.

Figura 5-48 Definição de parâmetros de proteção programados



1. Clique em **Add Unprotected Period**. Configure os parâmetros na caixa de diálogo que é exibida.

Figura 5-49 Adição de um período desprotegido



NOTA

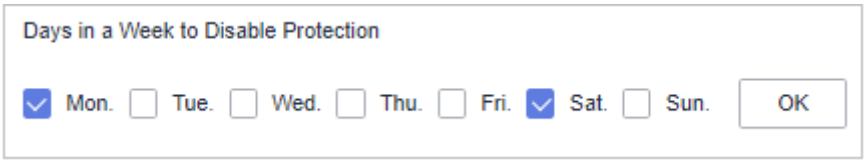
Restrições de configuração:

- Período desprotegido >= 5 minutos
- Período desprotegido < 24 horas
- Os períodos (exceto os que começam às 00:00 ou terminam às 23:59) não podem se sobrepor e devem ter um intervalo de pelo menos 5 minutos.
- Um período não pode abranger dois dias.
- A hora do servidor é usada como base de tempo.

2. Clique em **OK**.
3. Selecione os dias para desativar a proteção.

   Por exemplo, se você selecionar **Mon.**, **Thu.** e **Sat.**, o servidor desativará automaticamente a função WTP durante o período desprotegido nesses dias.

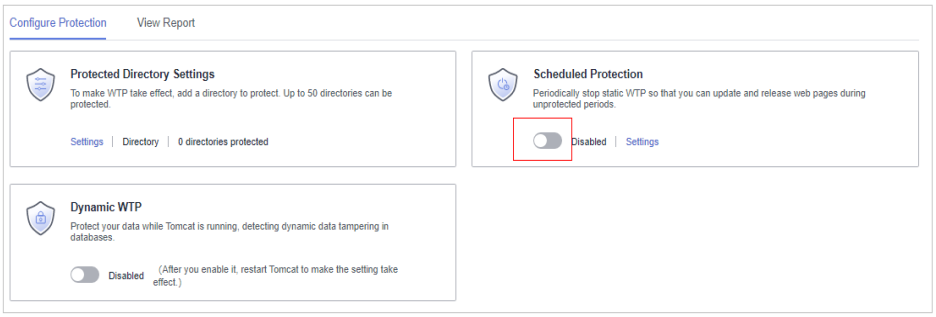
Figura 5-50 Selecionar dias para desativar a proteção



4. Clique em **OK**.

Passo 6 Retorne à guia **Configure Protection** e ative para ativar **Scheduled Protection**.

Figura 5-51 Ativação da proteção programada



----Fim

5.2.4 Habilitação de WTP dinâmica

A WTP dinâmica protege suas páginas da Web enquanto as aplicações de Tomcat estão em execução e pode detectar adulteração de dados dinâmicos, como dados de banco de dados. Pode ser habilitada com WTP estática ou separadamente.

Restrições

Apenas os servidores protegidos pela edição WTP do HSS suportam as operações descritas nesta seção.

Pré-requisitos

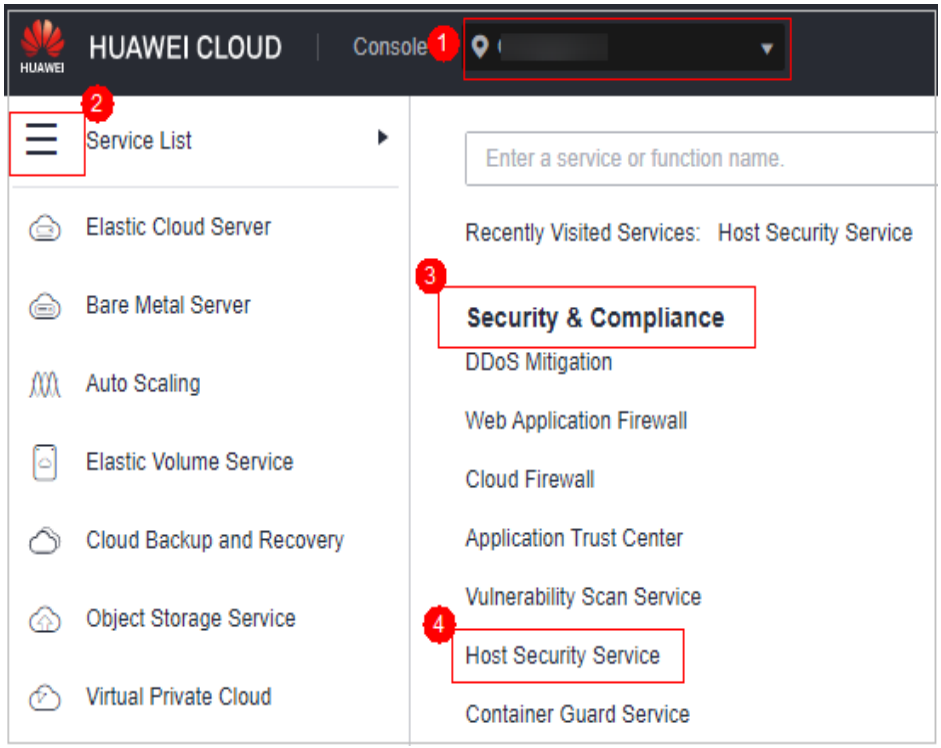
Você está usando um servidor que executa o SO Linux.

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 5-52 Acessar o HSS

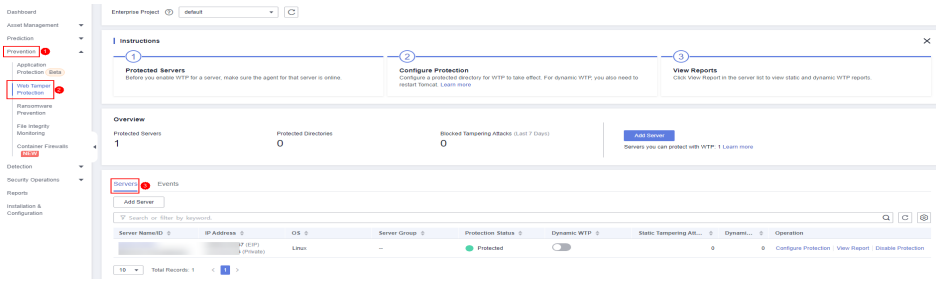


Passo 3 Escolha **Prevention** > **Web Tamper Protection**, clique em **Configure Protection**.

NOTA

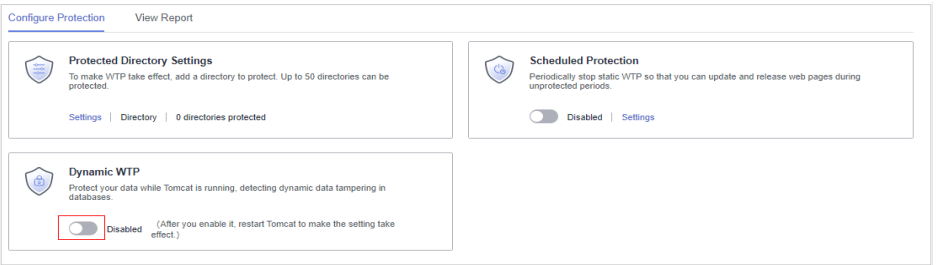
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figura 5-53 Entrar na página para configurações de diretório protegido



Passo 4 Na guia **Configure Protection**, ative  para habilitar **Dynamic WTP**.

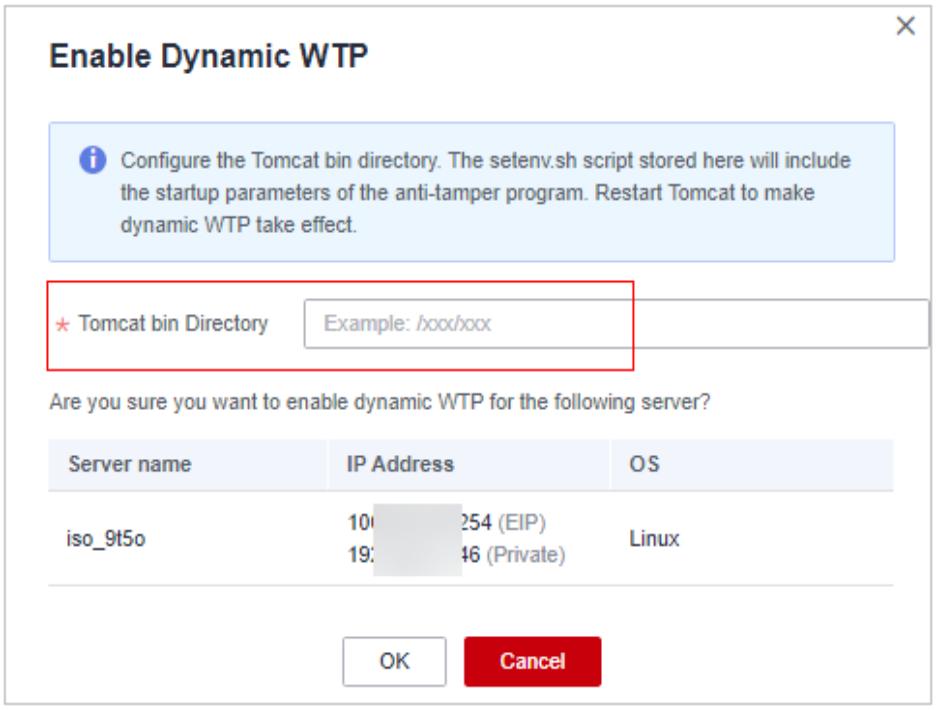
Figura 5-54 Habilitação de WTP dinâmica



Passo 5 Na caixa de diálogo exibida, modifique o **Tomcat bin Directory**.

Para habilitar a WTP dinâmica, primeiro é necessário modificar o diretório bin do Tomcat. O sistema predefine o script **setenv.sh** no diretório bin para definir os parâmetros de inicialização do programa anti-adulteração. Depois de habilitar a WTP dinâmica, reinicie o Tomcat para que essa configuração tenha efeito.

Figura 5-55 Configuração de um diretório do Tomcat



Passo 6 Clique em **OK** para habilitar a WTP dinâmica.

----Fim

5.2.5 Visualização de relatórios de WTP

Assim que a WTP estiver ativada, o HSS verificará de forma abrangente os diretórios protegidos que você especificou. Você pode verificar registros sobre ataques de adulteração detectados.

Restrições

Apenas os servidores protegidos pela edição WTP do HSS suportam as operações descritas nesta seção.

Pré-requisitos

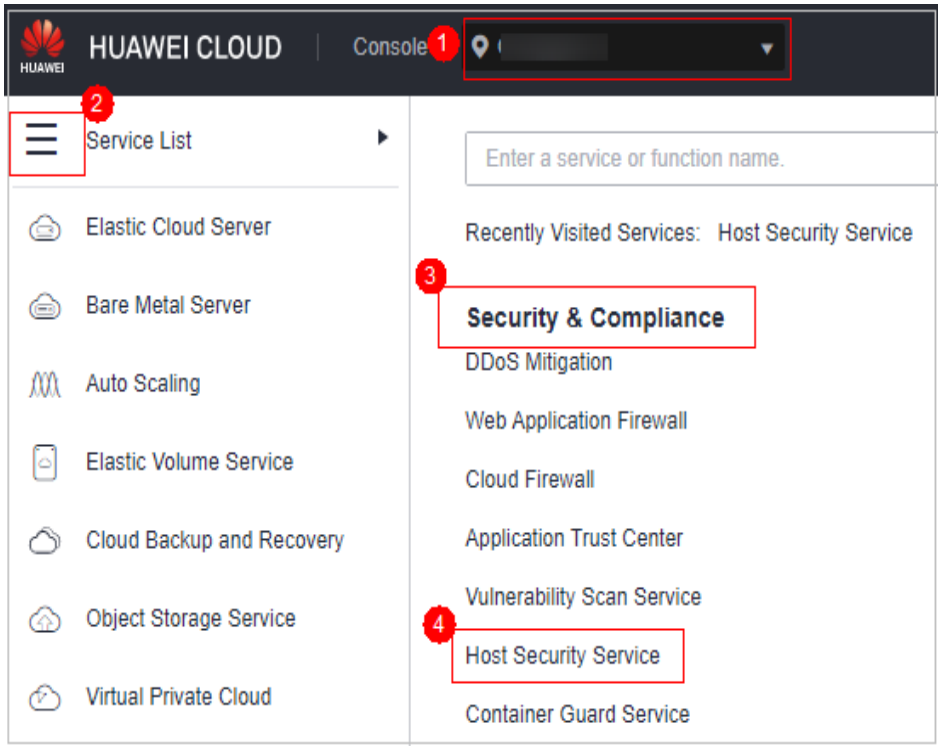
Agent Status do servidor é **Online** e o **WTP Status** é **Enabled**.

Procedimento

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

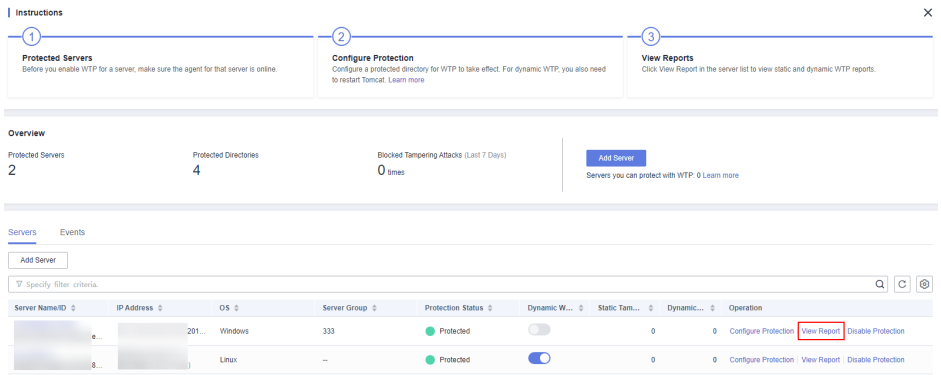
Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 5-56 Acessar o HSS



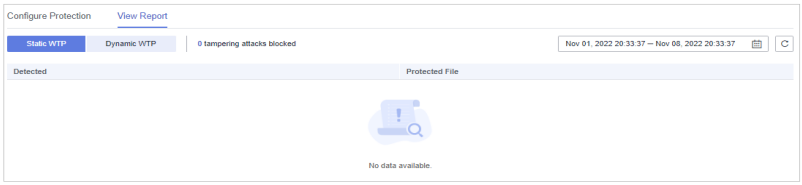
Passo 3 Escolha **Prevention** > **Web Tamper Protection** e clique na guia **Servers**. Localize a linha que contém o servidor de destino e clique em **View Report** na coluna **Operation**.

Figura 5-57 Visualização de um relatório de proteção



Passo 4 Visualize os detalhes na página do relatório.

Figura 5-58 Registros de WTP estáticos



----Fim

5.2.6 Visualização de eventos de WTP

Quando a WTP estática estiver ativada, o serviço HSS verificará de forma abrangente os diretórios protegidos que você especificou. Você pode verificar registros sobre adulteração detectada de arquivos de proteção de host.

Restrições

Apenas os servidores protegidos pela edição WTP do HSS suportam as operações descritas nesta seção.

Pré-requisito

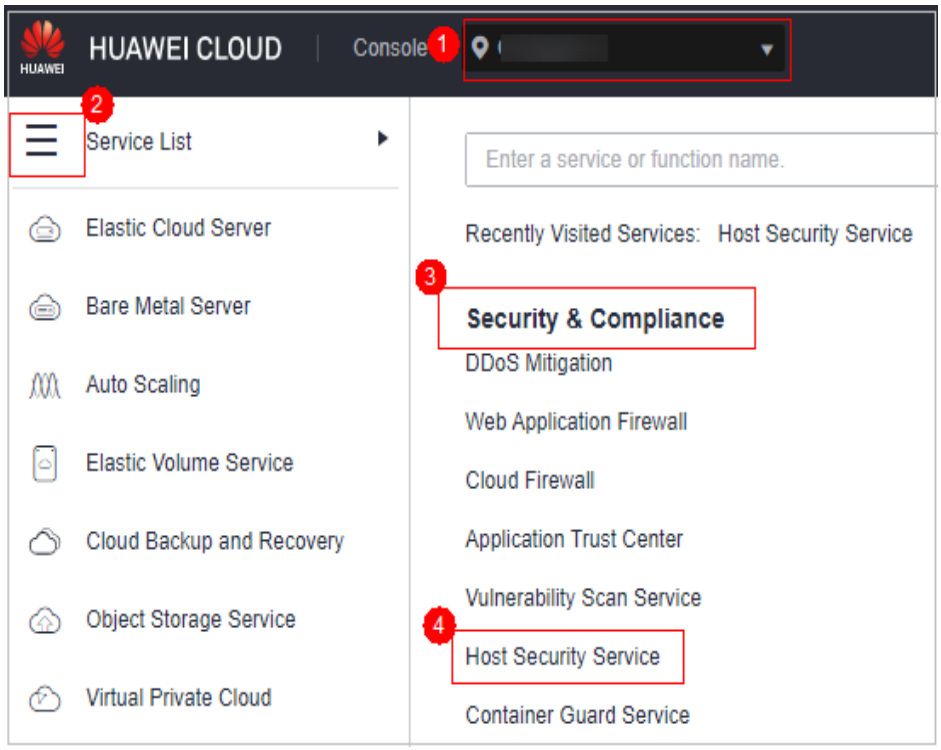
- **Agent Status** do servidor é **Online** e seu **WTP Status** é **Enabled**.
- A WTP estática está ativada.

Procedimento

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

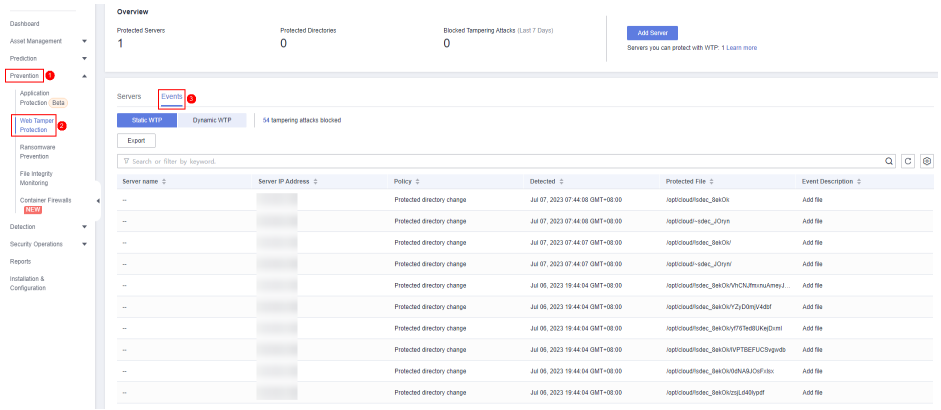
Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 5-59 Acessar o HSS



Passo 3 Escolha **Prevention** > **Web Tamper Protection** e clique em **Events** para visualizar os registros de adulteração de arquivos protegidos nos servidores.

Figura 5-60 Eventos



----Fim

5.2.7 Adição de um processo privilegiado

Se a WTP estiver habilitada, o conteúdo nos diretórios protegidos será somente leitura. Para permitir que determinados processos modifiquem arquivos nos diretórios, adicione-os à lista de processos privilegiados.

Somente a modificação feita por processos privilegiados pode ter efeito. As modificações feitas por outros processos serão revertidas automaticamente.

Tenha cuidado ao adicionar processos privilegiados. Não deixe que processos não confiáveis acessem seus diretórios protegidos.

Restrições

- Apenas os servidores protegidos pela edição de WTP do HSS suportam as operações descritas nesta seção.
- Somente os SOs x86 com kernel 4.18 suportam essa função.
- O processo privilegiado tem efeito apenas para o Agent 3.2.4 ou posterior.
- Um máximo de 10 processos privilegiados podem ser adicionados a cada servidor.

Pré-requisito

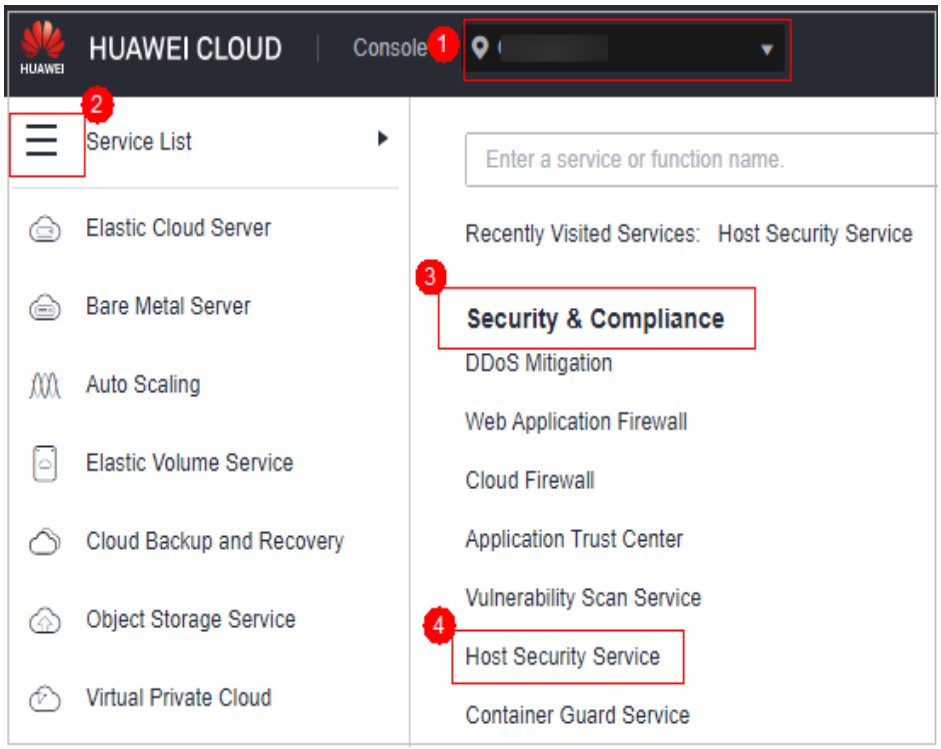
O **Protection Status** do servidor deve ser **Protected**. Para visualizar o status, escolha **Prevention** > **Web Tamper Protection**. Clique na guia **Servers**.

Adição de um processo privilegiado

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 5-61 Acessar o HSS

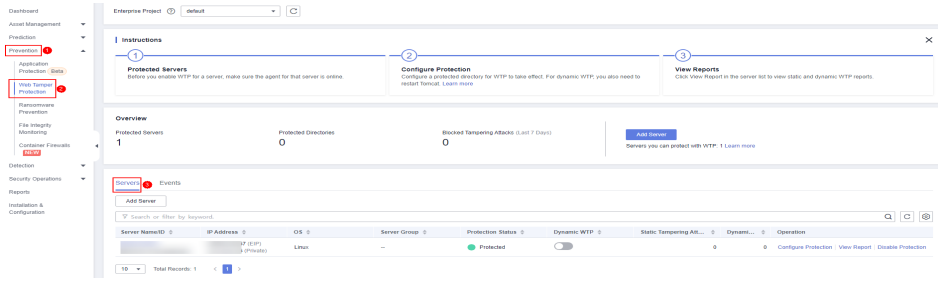


Passo 3 Escolha **Prevention** > **Web Tamper Protection**, clique em **Configure Protection**.

NOTA

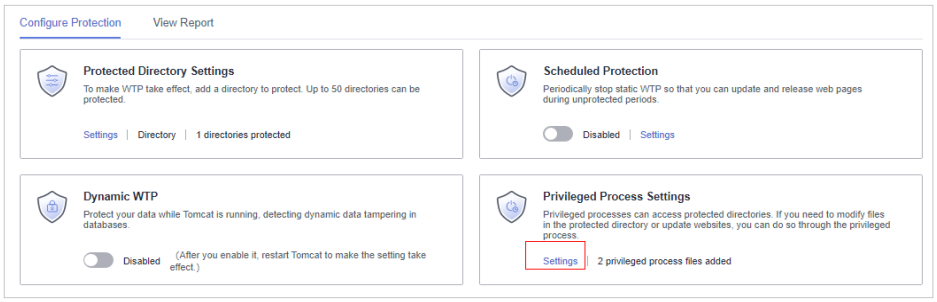
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figura 5-62 Entrar na página para configurações de diretório protegido



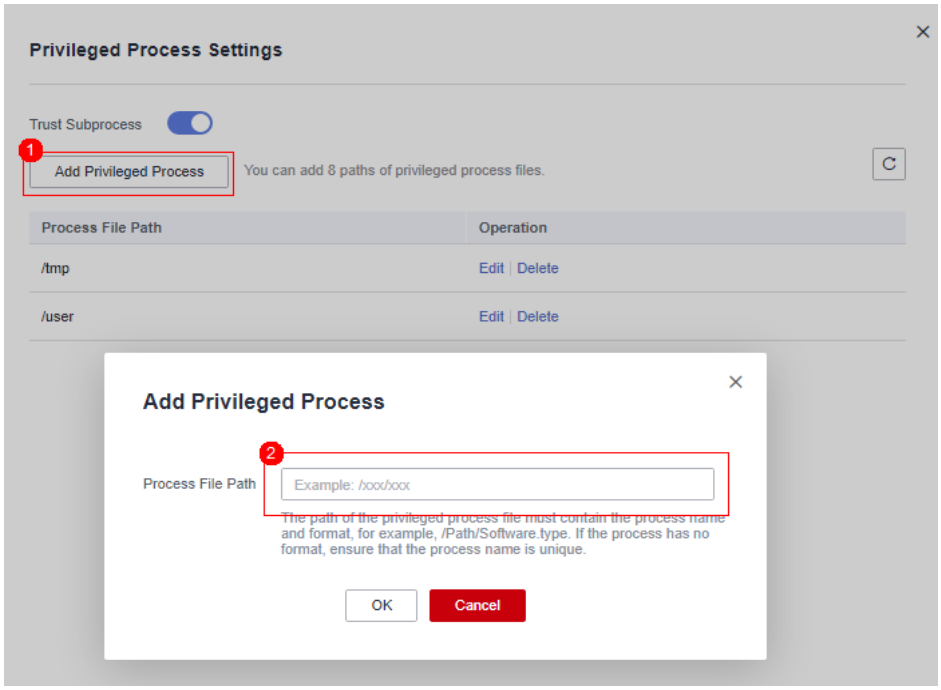
Passo 4 Clique em **Privileged Process Settings** e, em seguida, em **Settings**.

Figura 5-63 Configuração de um processo privilegiado



Passo 5 Na página **Privileged Process Settings**, clique em **Add Privileged Process**.

Figura 5-64 Adição de um processo privilegiado



Passo 6 Na caixa de diálogo**Add Privileged Process**, insira o caminho do processo privilegiado.

O caminho do arquivo do processo deve conter o nome e a extensão do processo, por exemplo, **C:/Path/Software.type**. Se o processo não tiver extensão, certifique-se de que o nome do processo seja exclusivo.

Passo 7 Clique em **OK**.

Passo 8 Ative **Trust Subprocess** para confiar no subprocesso no caminho do arquivo privilegiado adicionado.

NOTA

Quando essa função está ativada, os subprocessos nos cinco níveis de todos os arquivos de processos privilegiados são confiáveis.

----Fim

Procedimento de acompanhamento

Modificar ou excluir processos privilegiados existentes

Na coluna **Operation** de um caminho de arquivo de processo, clique em **Edit** para modificar os processos privilegiados ou clique em **Delete** para excluí-lo se for desnecessário.

NOTA

- Depois de editar ou excluir o caminho do arquivo do processo, o processo privilegiado não poderá modificar os arquivos no diretório protegido. Para evitar impactos nos serviços, tenha cuidado ao realizar essas operações.
- Processos privilegiados desnecessários devem ser excluídos em tempo hábil, pois podem ser explorados por invasores.

5.3 Prevenção contra ransomware

5.3.1 Compra de um cofre de backup

Para melhorar a defesa e reduzir a perda de serviço causada por ataques de ransomware, é aconselhável fazer backup periódico dos dados nos servidores. Antes de ativar o backup, compre um cofre para ser usado para armazenamento de backup.

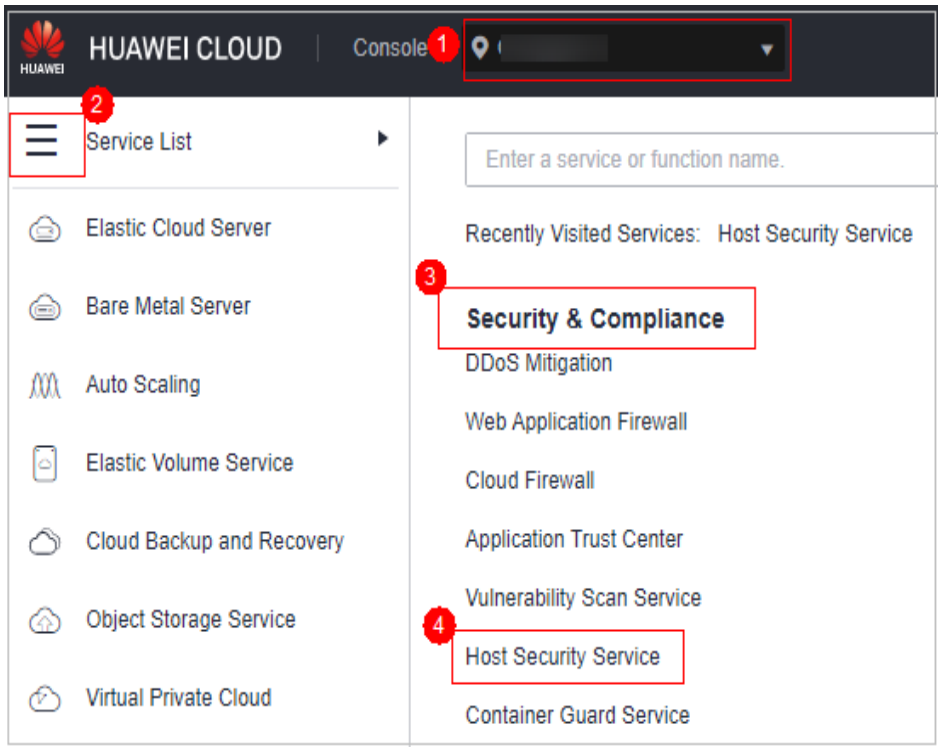
Você pode comprar um cofre de backup no console do HSS consultando esta seção ou no console do CBR consultando **Criação de um backup de backup do servidor em nuvem**.

Compra de um cofre de backup

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 5-65 Acessar o HSS



Passo 3 Escolha **Prevention** > **Ransomware Prevention**.

Passo 4 Clique na guia **Protected Servers**.

Passo 5 Ative o backup de ransomware. Na caixa de diálogo exibida, clique em **Next**.

Passo 6 Na caixa de diálogo que é exibida, defina os parâmetros do cofre, como mostrado em **Buy Capacity**. Para obter detalhes sobre os parâmetros, consulte **Parâmetros para compra de capacidade de backup**.

Figura 5-66 Buy Capacity

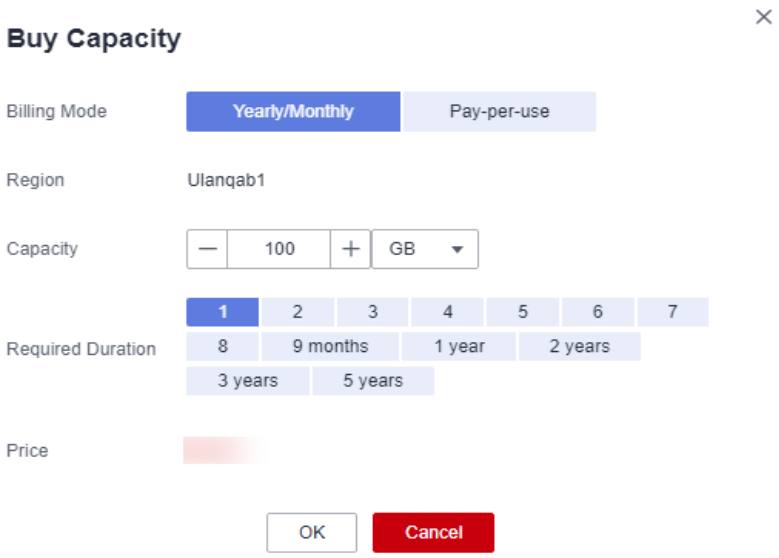


Tabela 5-11 Parâmetros para a compra de capacidade de backup

Parâmetro	Descrição
Billing Mode	Selecione **Yearly/Monthly** ou **On-demand**, conforme necessário. ● **Yearly/Monthly**: você é cobrado com base no período de compra especificado no pedido. ● **On-demand**: você paga pelo tempo de uso dos recursos. Os preços são calculados por hora, e não é necessário pagar uma taxa mínima.
Region	Região do cofre de backup que você deseja comprar
Capacity	Selecione o tamanho do cofre de backup conforme necessário.
Required Duration	Selecione a duração necessária se tiver selecionado **Yearly/Monthly** para **Billing Mode**.
Price	● **Yearly/Monthly**: você é cobrado com base na capacidade de armazenamento e na duração disponível comprada. ● **On-demand**: você é cobrado com base na capacidade de armazenamento usada.

Passo 7 Clique em **OK**.

- Se a opção **Yearly/Monthly** for selecionada:
  a. A página de confirmação do pedido é exibida.
  b. Confirme o pedido e clique em **Pay**.
- Se a opção **On-demand** for selecionada:
  A capacidade é comprada com sucesso.

  NOTA

  O cofre de backup será cobrado depois que a proteção contra ransomware for ativada. Certifique-se de que o saldo da sua conta é suficiente.

----Fim

5.3.2 Ativação da prevenção de ransomware

O ransomware é uma das maiores ameaças de segurança cibernética da atualidade. O ransomware pode invadir um servidor, criptografar dados e pedir resgate, causando interrupção do serviço, vazamento de dados ou perda de dados. Os atacantes podem não desbloquear os dados, mesmo depois de receber o resgate. O HSS fornece prevenção de ransomware estática e dinâmica. Você pode periodicamente fazer backup de dados do servidor para reduzir possíveis perdas.

A prevenção de ransomware será ativada com a edição premium, WTP ou de container do HSS. Para melhorar ainda mais a defesa, ative **a proteção** e **o backup dinâmicos do honeypot**.

Se você tiver desativado a prevenção de ransomware, você pode executar as operações nesta seção para ativá-la novamente.

Pré-requisitos

- Você ativou a edição premium, WTP ou de segurança de container do HSS.
- Foi criada uma política de proteção. Para obter detalhes, consulte **Criação de uma política**.

Restrições

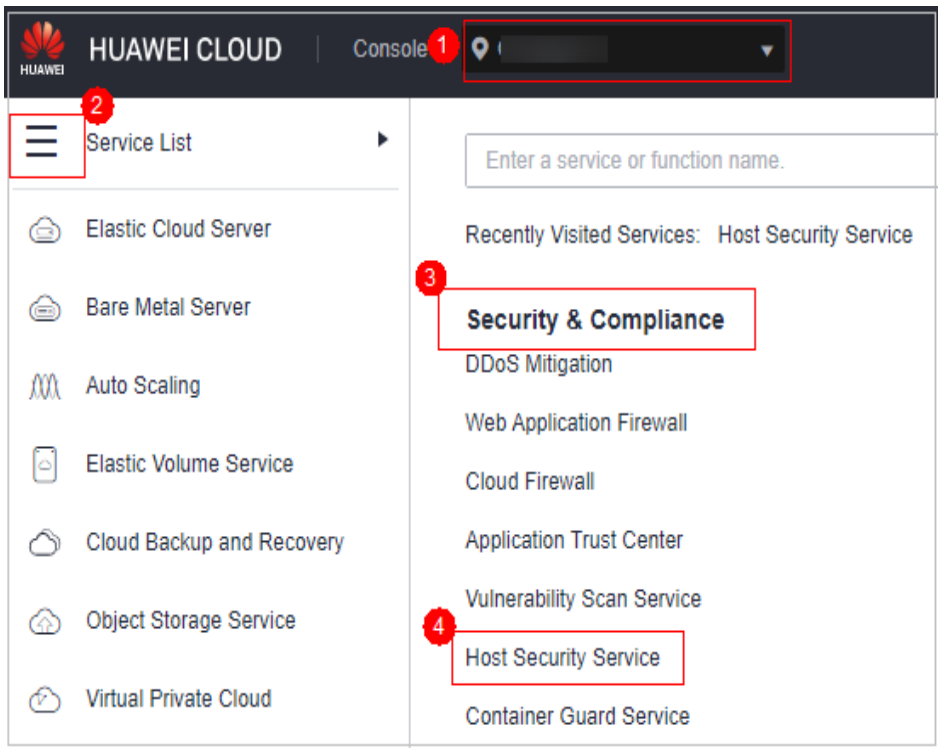
- O backup de ransomware suporta apenas servidores da Huawei Cloud.
- Somente as edições premium, WTP e de container oferecem suporte à proteção contra ransomware.

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 5-67 Acessar o HSS



Passo 3 Escolha **Prevention** > **Ransomware Prevention**.

Passo 4 Clique na guia **Protected Servers**.

Passo 5 Na coluna **Ransomware Protection Status** de um servidor, clique em **Enable**.

Você também pode selecionar vários servidores e clicar em **Enable Ransomware Prevention** acima da lista de servidores.

Passo 6 Na caixa de diálogo **Enable Ransomware Prevention**, confirme as informações do servidor e selecione uma política de proteção.

Passo 7 Clique em **OK**.

Se o **Ransomware Prevention Status** do servidor for alterado para **Enabled**, a proteção contra ransomware será ativada com sucesso.

----Fim

5.3.3 Ativação do backup

Para melhorar a defesa e reduzir a perda de serviço causada por ataques de ransomware, é aconselhável fazer backup periódico dos dados nos servidores.

Pré-requisitos

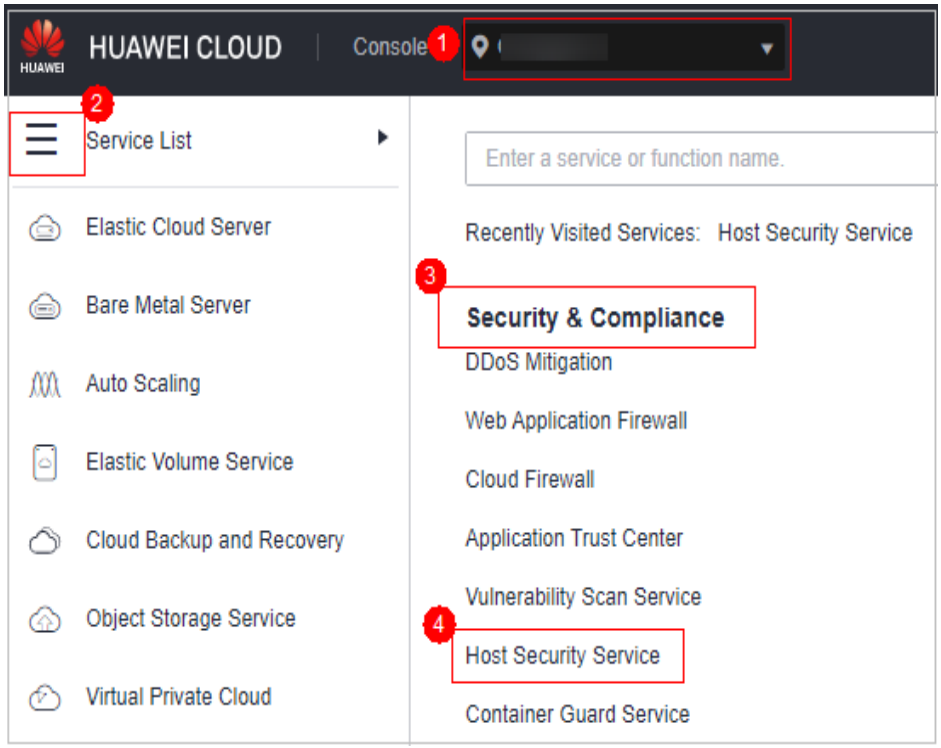
Você comprou um cofre de backup. Para obter detalhes, consulte **Compra de um cofre de backup**.

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 5-68 Acessar o HSS



Passo 3 Escolha **Prevention** > **Ransomware Prevention**.

NOTA

Se os servidores forem gerenciados por projetos empresariais, você poderá selecionar o projeto empresarial de destino para visualizar ou operar as informações sobre ativos e detecção.

Passo 4 Clique na guia **Protected Servers**.

Passo 5 Selecione um servidor e clique em **Enable Backup**.

Passo 6 Na caixa de diálogo **Enable Backup**, selecione um cofre.

NOTA

Um cofre que atenda às seguintes condições pode ser vinculado:

- O cofre está no estado **Available** ou **Locked**.
- A política de backup está no estado **Enabled**.
- O cofre tem capacidade de backup disponível.
- O cofre está vinculado a menos de 256 servidores.

Passo 7 Clique em **OK**.

----Fim

5.3.4 Prevenção de ransomware

Pré-requisito

Você ativou a edição premium, WTP ou de segurança de container do HSS.

Restrições

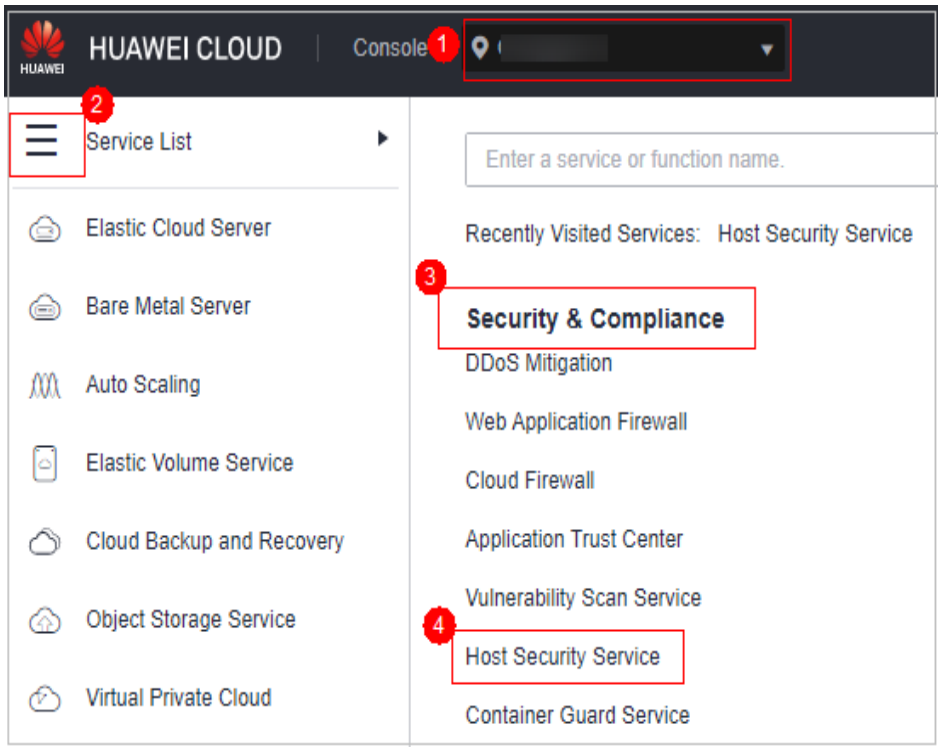
- O backup de ransomware suporta apenas servidores da Huawei Cloud.
- Depois que a proteção contra ransomware é ativada, você precisa lidar com alarmes de ransomware e corrigir as vulnerabilidades em seus sistemas e middleware em tempo hábil.

Visualização de eventos de 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 5-69 Acessar o HSS



Passo 3 Escolha **Prevention** > **Ransomware Prevention**.

NOTA

Se os servidores forem gerenciados por projetos empresariais, você poderá selecionar o projeto empresarial de destino para visualizar ou operar as informações sobre ativos e detecção.

Passo 4 Clique na guia **Events** e verifique os eventos.

Clique em **Handle** na coluna **Operation** de um evento ou selecione servidores e clique em **Batch Handle** acima da lista.

----Fim

Visualização de tarefas de backup e restauração

AVISO

O backup da proteção contra ransomware de HSS depende do Cloud Backup and Recovery (CBR). Antes de ativar o backup do servidor, certifique-se de que você comprou o CBR.

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Prevention** > **Ransomware Prevention**. Clique no número de tarefas de backup e restauração.

Passo 3 Na caixa de diálogo exibida, visualize os detalhes da tarefa de backup e restauração. Você pode filtrar ou procurar um servidor por seu nome ou status. Para obter mais informações, consulte **Tabela 5-12**.

Figura 5-70 Detalhes da tarefa de backup e restauração

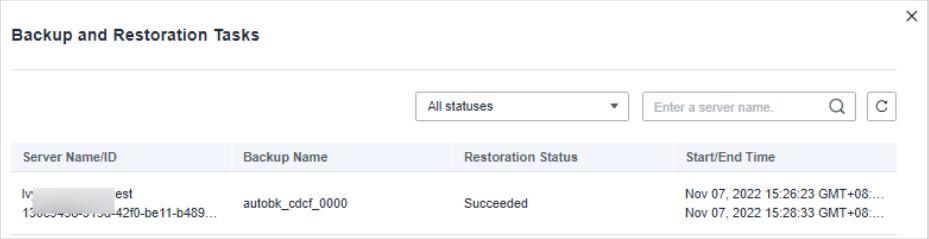


Tabela 5-12 Parâmetros da tarefa de backup e restauração

Parâmetro	Descrição	Exemplo de valor
Server Name/ID	Nome ou ID de um servidor que executa uma tarefa de restauração.	-
Backup Name	Nome de um arquivo de backup.	-
Restoration Status	Status de restauração de um servidor. Pode ser: ● **Succeeded** ● **Skipped** ● **Failed** ● **In progress** ● **Timed out** ● **Waiting** Se uma tarefa foi ignorada, falhou ou expirou, execute a restauração novamente.	Succeeded
Start/End Time	Hora de início e término de backup e restauração.	-

----Fim

Restauração de dados do servidor

AVISO

O backup da proteção contra ransomware de HSS depende do Cloud Backup and Recovery (CBR). Antes de ativar o backup do servidor, certifique-se de que você comprou o CBR.

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 No painel de navegação, escolha **Prevention** > **Ransomware Prevention**. Clique na guia **Protected Servers**. Na coluna **Operation** do servidor de destino, clique em **More** > **Restore Data**.

Passo 3 Na caixa de diálogo exibida, visualize informações sobre o servidor a ser restaurado. Você pode procurar a fonte de dados de backup a ser restaurada filtrando o status do backup e pesquisando o nome do backup. Para obter mais informações, consulte **Tabela 5-13**.

Figura 5-71 Filtragem de origens de dados

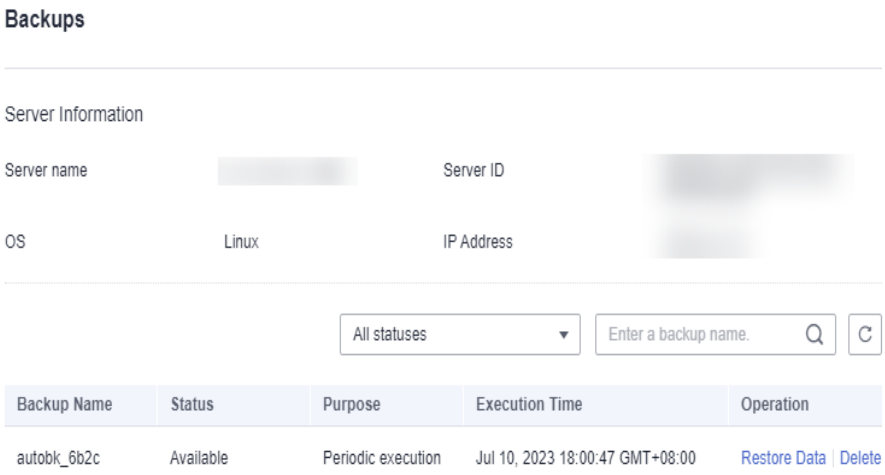


Tabela 5-13 Parâmetros da fonte de dados de backup

Parâmetro	Descrição	Exemplo de valor
Backup Name	Nome de um arquivo de backup.	-
Backup Status	Status do backup. Pode ser: ● **Available** ● **Creating** ● **Deleting** ● **Restoring** ● **Error** Um backup no estado **Available** pode ser usado para restauração.	Available
Purpose	Finalidade do backup. Pode ser: ● **Periodic execution**: o backup dos dados é feito com base no período de backup configurado na política de backup. ● **Ransomware protection**: o backup dos dados é feito imediatamente quando um servidor é atacado por ransomware.	Periodic execution
Execution Time	Hora em que foi feito o backup da fonte de dados.	-

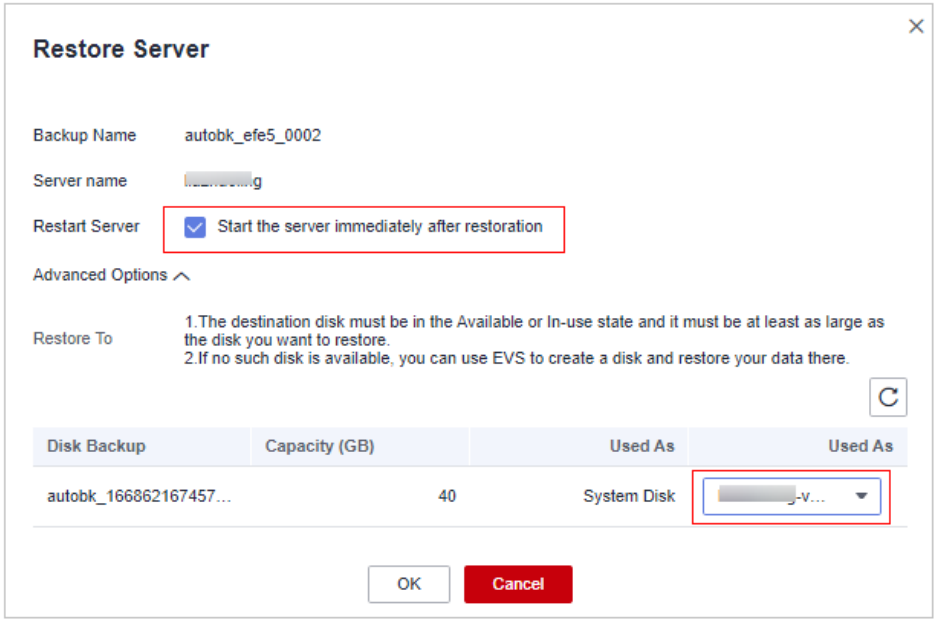
Passo 4 Na coluna **Operation** de um backup, clique em **Restore Data**.

NOTA

Somente um backup no estado disponível pode ser restaurado.

Passo 5 Na caixa de diálogo exibida, confirme as informações do servidor e clique em **OK**.

Figura 5-72 Restaurar um servidor



----Fim

Aumento da capacidade de backup

AVISO

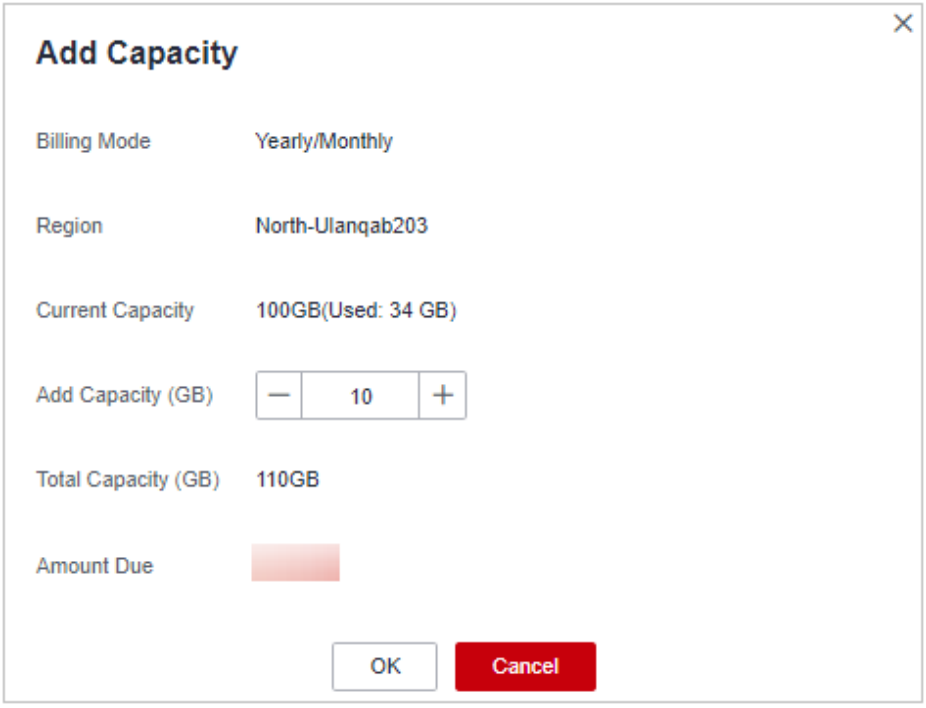
O backup da proteção contra ransomware de HSS depende do Cloud Backup and Recovery (CBR). Antes de ativar o backup do servidor, certifique-se de que você comprou o CBR.

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 Na árvore de navegação, escolha **Prevention** > **Ransomware Prevention**. A lista de servidores protegidos é exibida. Clique em **Add Capacity** na coluna **Operation** do servidor de destino.

Passo 3 Na caixa de diálogo exibida, configure a capacidade.

Figura 5-73 Configurar a capacidade



Passo 4 Se as informações estiverem corretas, clique em **OK**. A página de pagamento é exibida. Após a conclusão do pagamento, retorne à página de guia **Protected Server** para exibir a capacidade de armazenamento do servidor de destino.

- Se o pagamento não for concluído, o **Vault Status** do servidor de destino será exibido como **Locked**. Após o pagamento, o status torna-se normal.

----Fim

Modificação de uma política de backup

AVISO

O backup da proteção contra ransomware de HSS depende do Cloud Backup and Recovery (CBR). Antes de ativar o backup do servidor, certifique-se de que você comprou o CBR.

Passo 1 Faça logon no console de gerenciamento do HSS.

Passo 2 Na árvore de navegação, escolha **Prevention** > **Ransomware Prevention**. A lista de servidores protegidos é exibida. Clique no nome da política na coluna **Backup Policy Status** do servidor de destino.

Passo 3 Configure a política na caixa de diálogo exibida. Para obter mais informações, consulte **Tabela 5-14**.

Figura 5-74 Configurar uma política

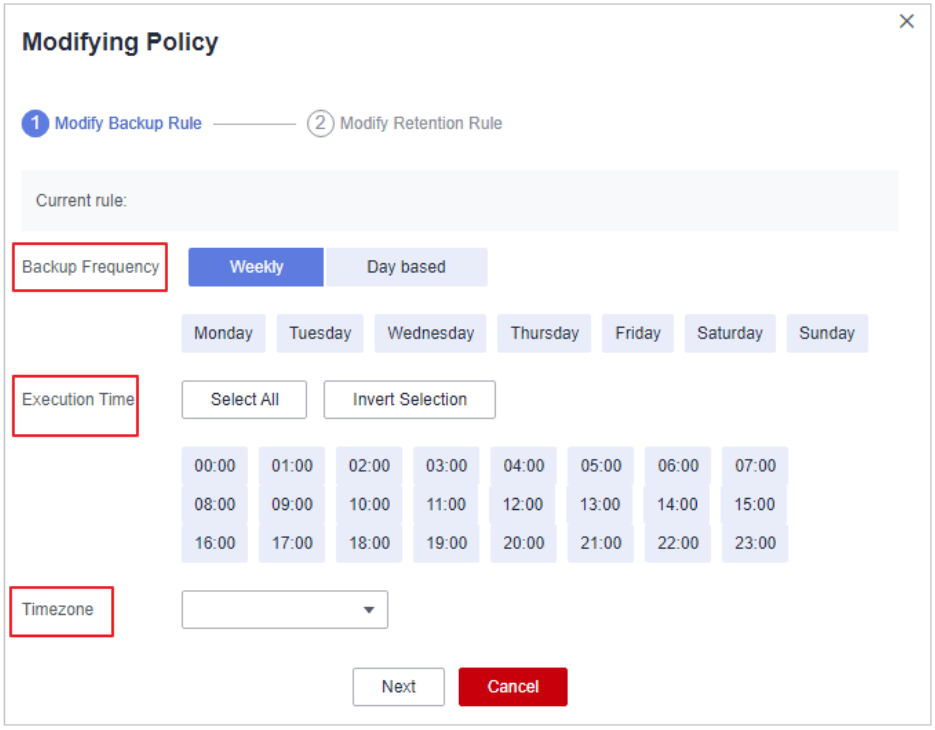


Tabela 5-14 Parâmetros de política

Parâmetro	Descrição	Exemplo de valor
Backup Frequency	O backup dos dados pode ser feito automaticamente em dias específicos de uma semana ou em um intervalo fixo. ● **Weekly**: selecione um ou mais dias em uma semana para fazer backup dos dados. ● **Day based**: o intervalo de backup varia de 1 a 30 dias.	Weekly
Execution Time	Hora em que o backup automático é iniciado. **NOTA** Exemplo de configurações de política Política 1: defina **Backup Frequency** como **Weekly**, selecione **Wednesday** e **Saturday** e defina **Execution Time** como **00:00** e **13:00**. O backup dos dados será feito automaticamente às 00:00 e às 13:00 todas as quartas-feiras e sábados. Política 2: defina **Backup Frequency** como **Day based** e defina o intervalo como dois dias. Defina **Execution Time** para **02:00** e **14:00**. O backup dos dados será feito automaticamente às 02:00 e às 14:00 em um intervalo de dois dias.	00:00, 07:00
Timezone	Selecione o fuso horário da hora de backup.	UTC+08:00

Passo 4 Confirme as configurações e clique em **Next**. Configure a regra de retenção de backup.

- **Type**: **Backup Quantity**

  Configure a política de backup. Para obter mais informações, consulte **Tabela 5-15**.

Figura 5-75 Configurar regras de retenção por quantidade

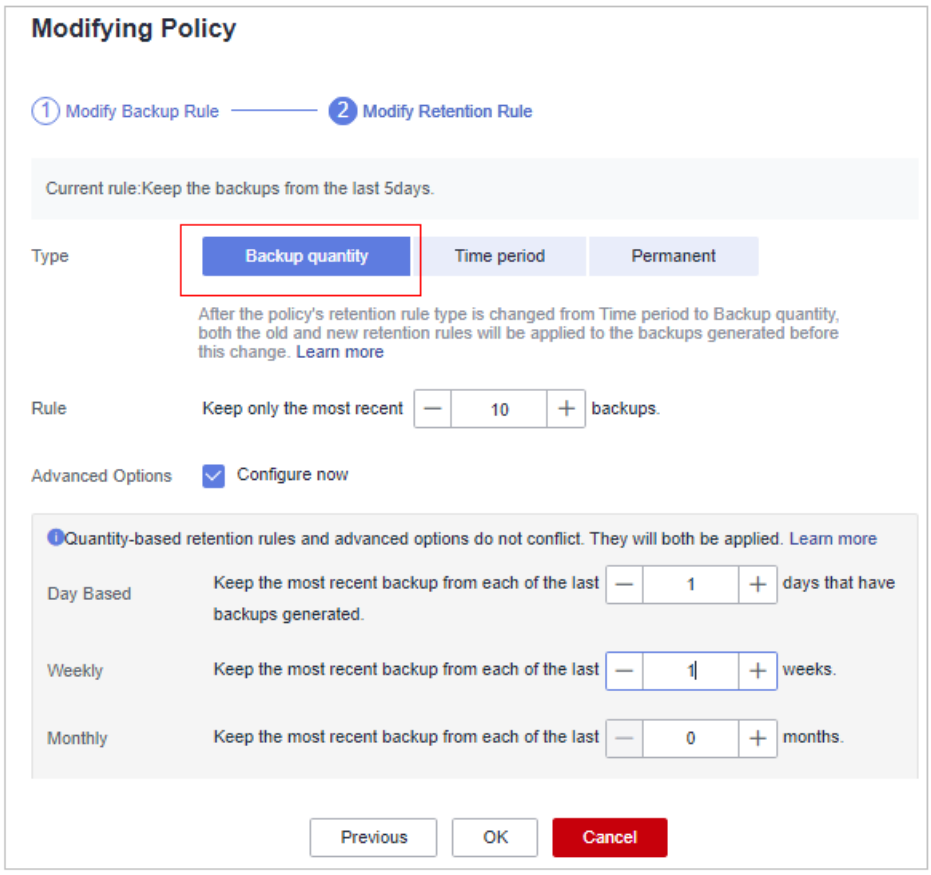


Tabela 5-15 Parâmetros para retenção de dados por quantidade

Parâmetro	Descrição	Exemplo de valor
Rule	Número de backups mais recentes a serem retidos. **AVISO** Essa configuração entra em vigor independentemente de como você configura as opções avançadas. Por exemplo, se a regra estiver configurada para manter os 30 backups mais recentes e **Advanced Options** estiverem configuradas para manter o backup mais recente nos últimos 3 meses (90 dias), os 30 backups mais recentes serão mantidos.	30

Parâmetro	Descrição	Exemplo de valor
(Optional) Advanced Options	Você pode manter o backup mais recente em um dia, uma semana, um mês ou um ano. – Backup diário: o último backup em cada um dos dias especificados é mantido. – Backup semanal: o último backup em cada dia das semanas especificadas é mantido. – Backup mensal: o último backup em cada dia dos meses especificados é retido. – Backup anual: o último backup em cada dia dos anos especificados é mantido. **NOTA** Se várias regras estiverem configuradas, a regra com o período de retenção mais longo entrará em vigor.	Keep the most recent backup from each of the last three months

- **Type**: **Time period**

  Configure a política de backup. Para obter mais informações, consulte **Tabela 5-16**.

Figura 5-76 Configurar regras de retenção por período de tempo

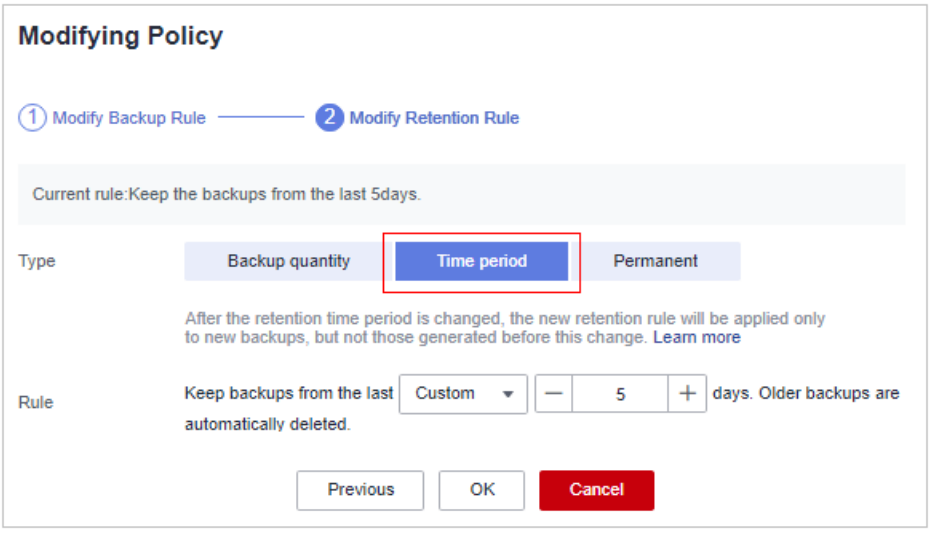


Tabela 5-16 Parâmetros para retenção de dados por período de tempo

Parâmetro	Descrição	Exemplo de valor
Rule	Selecione ou personalize um período de retenção de backup. O sistema manterá automaticamente os backups e excluirá os anteriores com base nas suas configurações. O período de retenção pode ser: – Dias – 1 mês – 3 meses – 6 meses – 1 ano	3 meses

- **Type**: **Permanent**

  Os dados de backup serão armazenados permanentemente.

  NOTA

  Se o **Retention Type** de uma regra for alterado de **Time period** para **Permanent**, os backups históricos ainda serão excluídos seguindo com base nas configurações de **Time period**. Para obter detalhes, consulte **Por que a regra de retenção não entra em vigor após ser modificada?**

Passo 5 Clique em **OK**.

----Fim

5.3.5 Desabilitação da prevenção de ransomware

Cenário

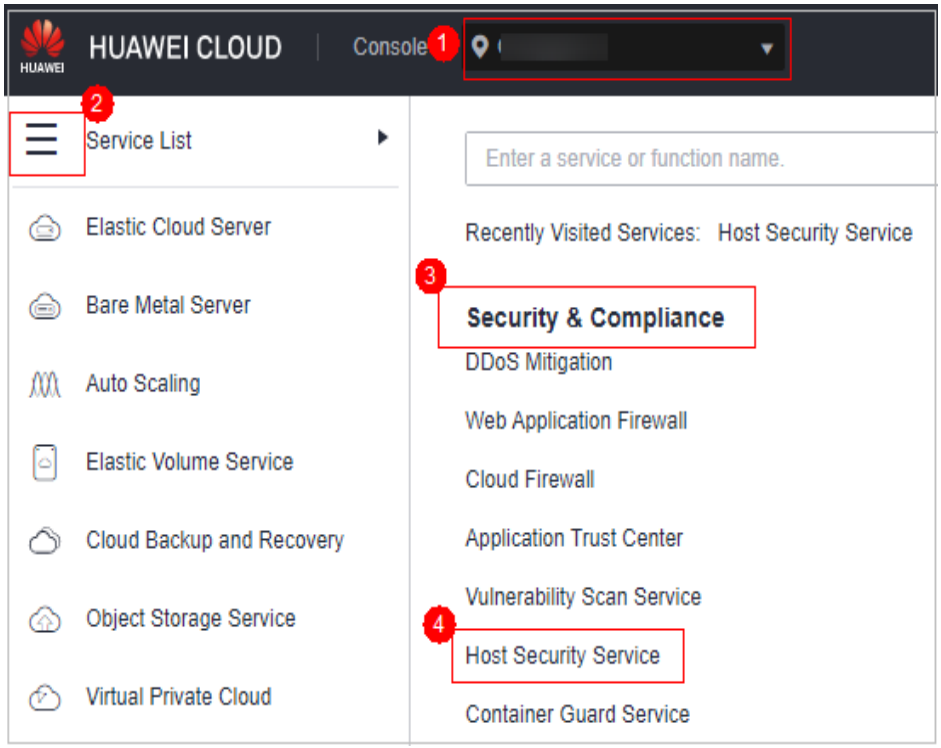
Você pode desabilitar a proteção contra ransomware conforme necessário. Depois que a proteção é desabilitada, seu servidor pode ser invadido por ransomware. Tenha cuidado ao realizar esta operação.

Desabilitação da prevenção de ransomware

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 5-77 Acessar o HSS



Passo 3 No painel de navegação, escolha **Prevention** > **Ransomware Prevention**. Clique na guia **Protected Servers**.

Passo 4 Clique em **More** > **Disable Protection** na coluna **Operation** do servidor de destino.

Passo 5 Confirme as informações e clique em **OK**.

----Fim

Operações de acompanhamento

Desabilitar a prevenção de ransomware não impede o backup de dados. Se você não precisar mais de backup, **desvincule seus servidores de CBR**. Se você não precisar mais de um cofre de backup, poderá **excluí-lo**.

5.3.6 Managing Ransomware Prevention Policies

You can use predefined policies, create or modify ransomware prevention policies, or change the policy associated with a server.

Constraints

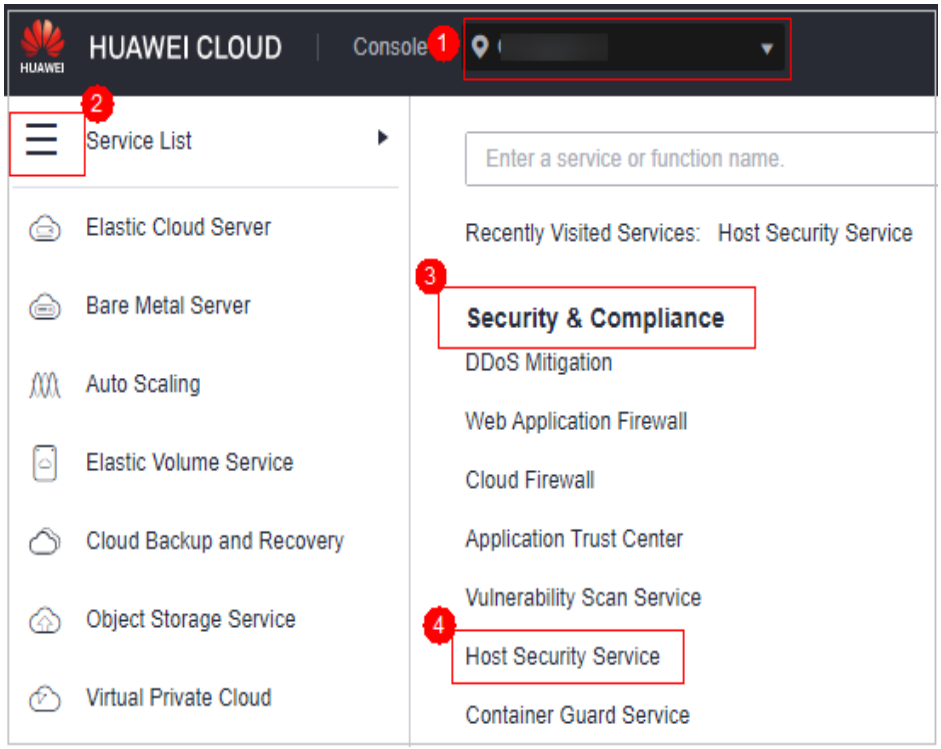
Only premium, WTP, and container editions support ransomware protection.

Creating a Policy

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 5-78 Acessar o HSS



Passo 3 Escolha **Prevention** > **Ransomware Prevention**.

NOTA

Se os servidores forem gerenciados por projetos empresariais, você poderá selecionar o projeto empresarial de destino para visualizar ou operar as informações sobre ativos e detecção.

Passo 4 Click the **Policies** tab and click **Add Policy**.

Passo 5 Configure policy parameters. For more information, see **Tabela 5-17**.

Figura 5-79 Protection policy parameters

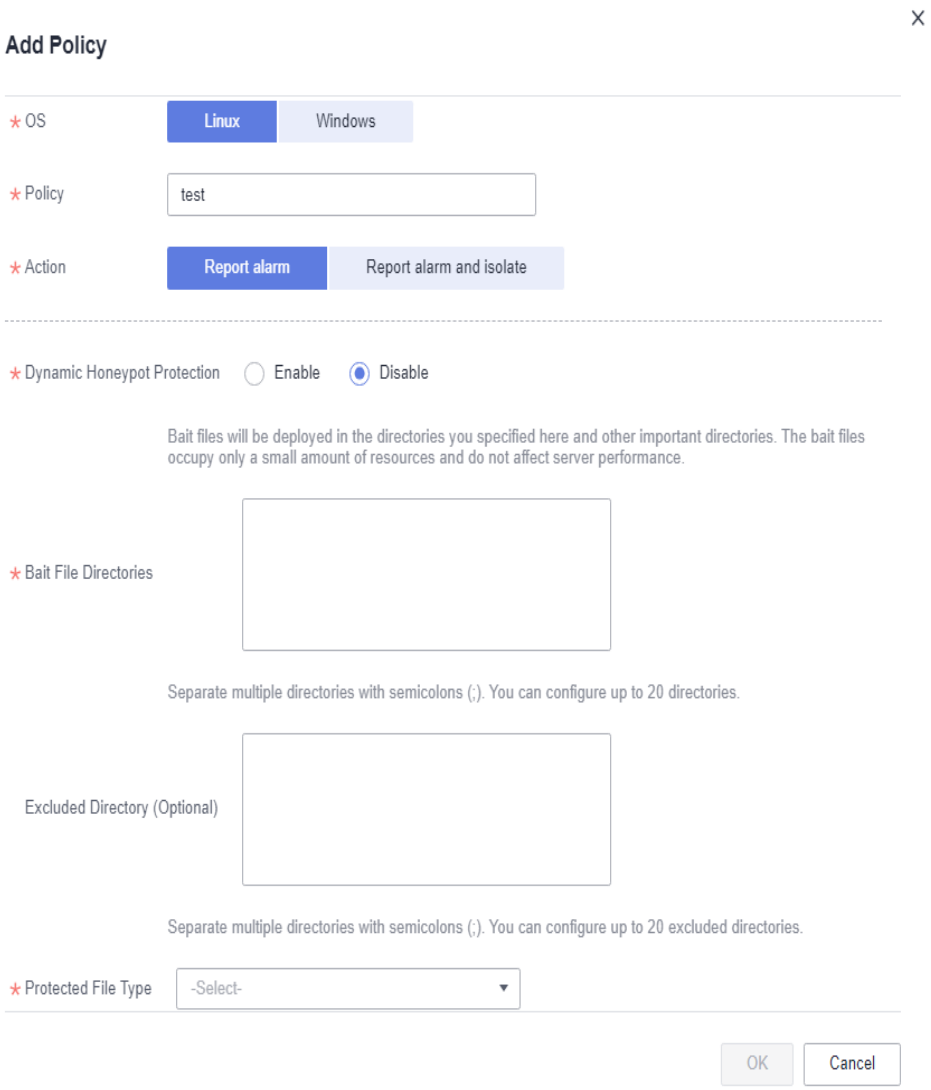


Tabela 5-17 Protection policy parameters

Parameter	Description	Example Value
OS	Server OS.	Linux
Policy	Policy name.	test
Action	How an event is handled. ● **Report alarm and isolate** ● **Report alarm**	Report alarm and isolate

Parameter	Description	Example Value
Dynamic Honeypot Protection	After honeypot protection is enabled, the system deploys honeypot files in protected directories and key directories (unless otherwise specified by users). A honeypot file occupies only a few resources and does not affect your server performance. **NOTA** Currently, Linux servers support dynamic generation and deployment of honeypot files. Windows servers support only static deployment of honeypot files.	Enabled
Honeypot File Directories	Protected directories (excluding subdirectories). You are advised to configure important service directories or data directories. Separate multiple directories with semicolons (;). You can configure up to 20 directories. This parameter is mandatory for Linux servers and optional for Windows servers.	Linux: **/etc/lesuo** Windows: **C:\Test**
Excluded Directory (Optional)	Directories where honeypot files are not deployed. Separate multiple directories with semicolons (;). You can configure up to 20 excluded directories.	Linux: /test Windows: C:\ProData
Protected File Type	Types of files to be protected. More than 70 file formats can be protected, including databases, containers, code, certificate keys, and backups. This parameter is mandatory for Linux servers only.	Select all
(Optional) Process Whitelist	Paths of the process files that can be automatically ignored during the detection, which can be obtained from alarms. This parameter is mandatory only for Windows servers.	-

Passo 6 Click **OK**.

----Fim

Changing a Policy

You can change the protection policy associated with a server.

Passo 1 Click the **Protected Servers** tab.

Passo 2 Select a server and click **Change Policy**.

Passo 3 In the **Change Policy** dialog box, select a protection policy.

Passo 4 Click **OK**.

----Fim

Modifying a Policy

Passo 1 Log in to the management console and go to the HSS page.

Passo 2 In the navigation pane, choose **Prevention** > **Ransomware Prevention**. Click the **Policies** tab.

Passo 3 Click **Edit** in the **Operation** column of a policy. Edit the policy configurations. For more information, see **Tabela 5-18**.

The following uses a Linux server as an example.

Tabela 5-18 Protection policy parameters

Parameter	Description	Example Value
OS	Server OS.	Linux
Policy	Policy name.	test
Action	How an event is handled. ● **Report alarm and isolate** ● **Report alarm**	Report alarm and isolate
Dynamic Honeypot Protection	After honeypot protection is enabled, the system deploys honeypot files in protected directories and key directories (unless otherwise specified by users). A honeypot file occupies only a few resources and does not affect your server performance. **NOTA** Currently, Linux servers support dynamic generation and deployment of honeypot files. Windows servers support only static deployment of honeypot files.	Enabled
Honeypot File Directories	Protected directories (excluding subdirectories). You are advised to configure important service directories or data directories. Separate multiple directories with semicolons (;). You can configure up to 20 directories. This parameter is mandatory for Linux servers and optional for Windows servers.	Linux: **/etc/lesuo** Windows: **C:\Test**

Parameter	Description	Example Value
Excluded Directory (Optional)	Directories where honeypot files are not deployed. Separate multiple directories with semicolons (;). You can configure up to 20 excluded directories.	Linux: /test Windows: C:\ProData
Protected File Type	Types of files to be protected. More than 70 file formats can be protected, including databases, containers, code, certificate keys, and backups. This parameter is mandatory for Linux servers only.	Select all
(Optional) Process Whitelist	Paths of the process files that can be automatically ignored during the detection, which can be obtained from alarms. This parameter is mandatory only for Windows servers.	-

Passo 4 Confirm the policy information and click **OK**.

----Fim

Deleting a Policy

Passo 1 Log in to the management console and go to the HSS page.

Passo 2 In the navigation pane, choose **Prevention** > **Ransomware Prevention**. Click the **Policies** tab.

Passo 3 Click **Delete** in the **Operation** column of the target policy.

NOTA

After a policy is deleted, the associated servers are no longer protected. Before deleting a policy, you are advised to bind its associated servers to other policies.

Passo 4 Confirm the policy information and click **OK**.

----Fim

5.4 Controle de processo de aplicação

5.4.1 Visão geral de controle do processo de aplicação

O HSS pode aprender as características dos processos de aplicações em servidores e gerenciar sua execução. Processos suspeitos e confiáveis podem ser executados, e alarmes são gerados para processos maliciosos.

Restrições

Para habilitar o controle do processo da aplicação, as seguintes condições devem ser atendidas:

- A edição premium do HSS ou superior foi habilitada para seus servidores. Para obter mais informações, consulte **Compra de uma cota do HSS** e **Atualização de sua edição**.
- A versão do agente do servidor se enquadra no escopo a seguir. Para obter mais informações, consulte **Atualização do agente**.
  - Linux: 3.2.7 ou posterior
  - Windows: 4.0.19 ou posterior

Processo de uso do controle de processo de aplicação

Figura 5-80 Processo de uso

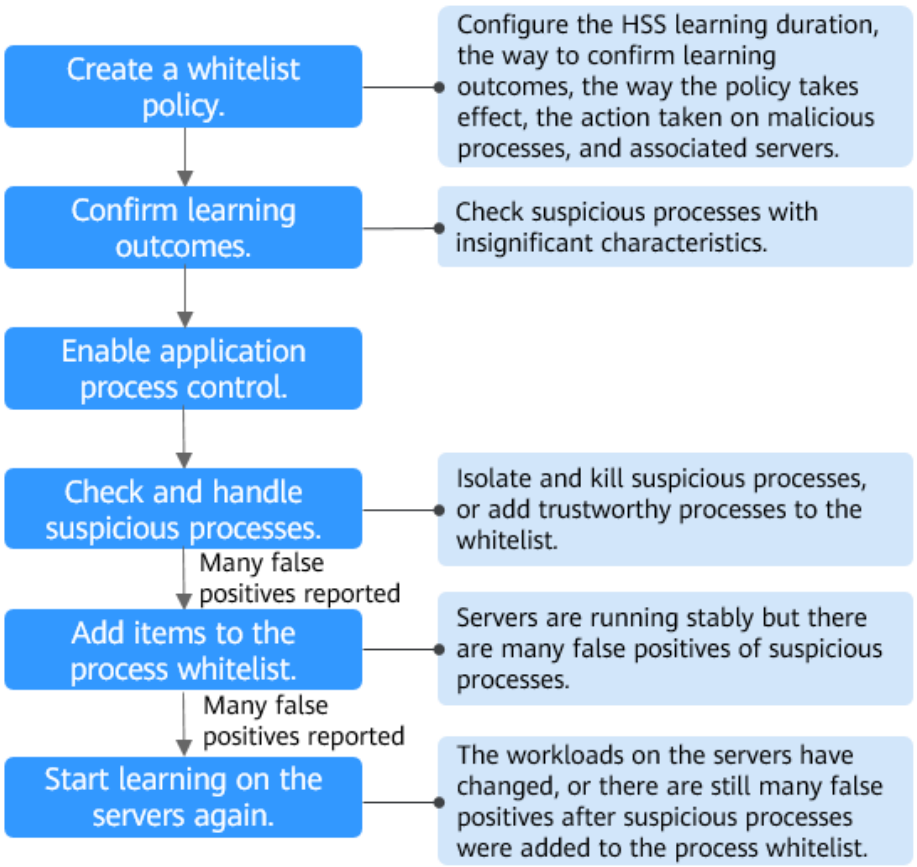


Tabela 5-19 Processo de uso do controle de processo de aplicação

Procedimento	Descrição
Criar uma política de lista branca.	Uma política de lista branca especifica como o HSS aprende os comportamentos do servidor e protege os processos de aplicações. A proteção de processos de aplicações pode ser ativada apenas para servidores vinculados a uma política de lista branca.

Procedimento	Descrição
Confirmar os resultados da aprendizagem.	Depois que o HSS aprende os processos de aplicação em servidores, pode haver alguns processos de aplicação suspeitos com características insignificantes, e o HSS não pode determinar se eles são maliciosos ou confiáveis. Nesse caso, você precisa confirmar os resultados da aprendizagem.
Habilitar o controle do processo de aplicação.	Habilitar o controle do processo de aplicação nos servidores vinculados a uma política.
Verificar e lidar com processos suspeitos.	O HSS não pode determinar se alguns processos de aplicação suspeitos com características insignificantes são confiáveis. Você precisa verificar os detalhes do processo, determinar se eles são confiáveis e adicioná-los à lista branca do processo ou isolá-los e eliminá-los.
(Opcional) **Adicionar itens à lista branca do processo.**	Depois que o HSS concluir a aprendizagem, se considerar muitos processos de aplicações confiáveis como suspeitos, você poderá adicionar esses processos à lista branca. O HSS estenderá a lista branca do processo depois de comparar as impressões digitais dos processos que aprendeu e as detectadas nas verificações de impressões digitais de ativos.
(Opcional) **Começar a aprender nos servidores novamente.**	Se você adicionou processos confiáveis à lista branca, mas ainda há muitos falsos positivos relatados, você pode deixar o HSS começar a aprender novamente nos servidores.

5.4.2 Criação de uma política de lista branca

Antes de ativar o controle do processo da aplicação, você precisa criar uma política de lista branca e configurar a duração do aprendizado do HSS, a forma de confirmar os resultados do aprendizado, a forma como a política entra em vigor e a ação tomada em processos suspeitos ou maliciosos. O HSS gerenciará os processos de aplicações com base em suas políticas.

Pré-requisitos

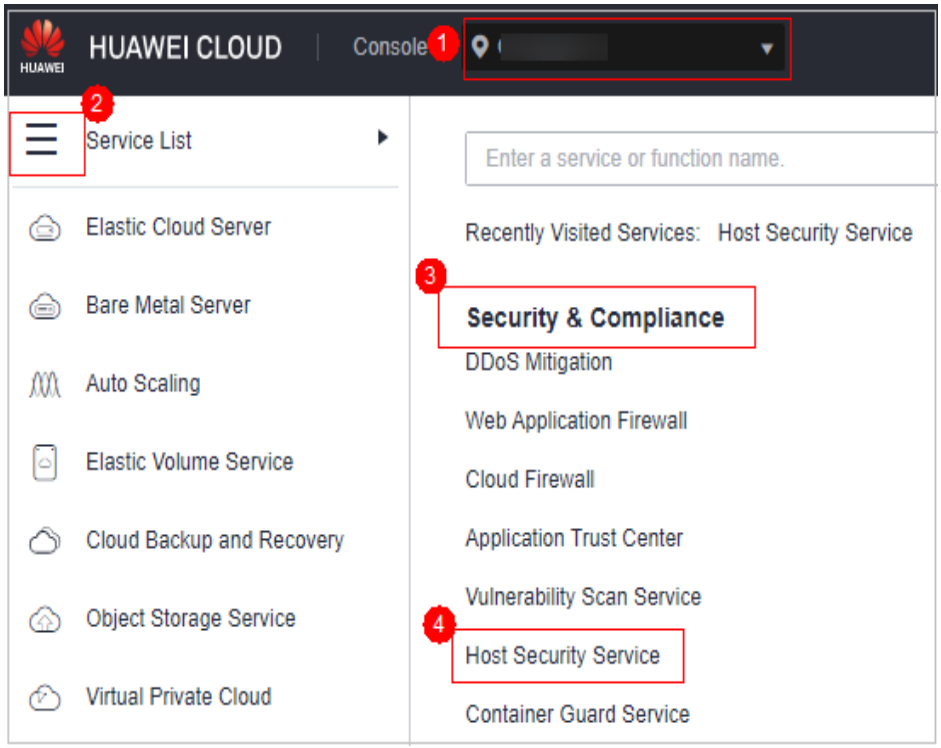
- A edição premium do HSS ou superior foi ativada para seus servidores. Para obter mais informações, consulte **Compra de uma cota do HSS** e **Atualização de sua edição**.
- A versão do agente se enquadra no escopo a seguir. Para obter detalhes sobre como atualizar o agente, consulte **Atualização do agente**.
  - Linux: 3.2.7 ou posterior
  - Windows: 4.0.19 ou posterior

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 5-81 Acessar o HSS



Passo 3 Na árvore de navegação, escolha **Prevention** > **Application Process Control**.

Passo 4 Clique na guia **Whitelist Policies**. Clique em **Create Policy**.

Passo 5 Na caixa de diálogo **Create Policy**, configure os parâmetros da política. Para obter detalhes sobre os parâmetros relacionados, consulte **Tabela 5-20**.

Figura 5-82 Criação de uma política de lista branca

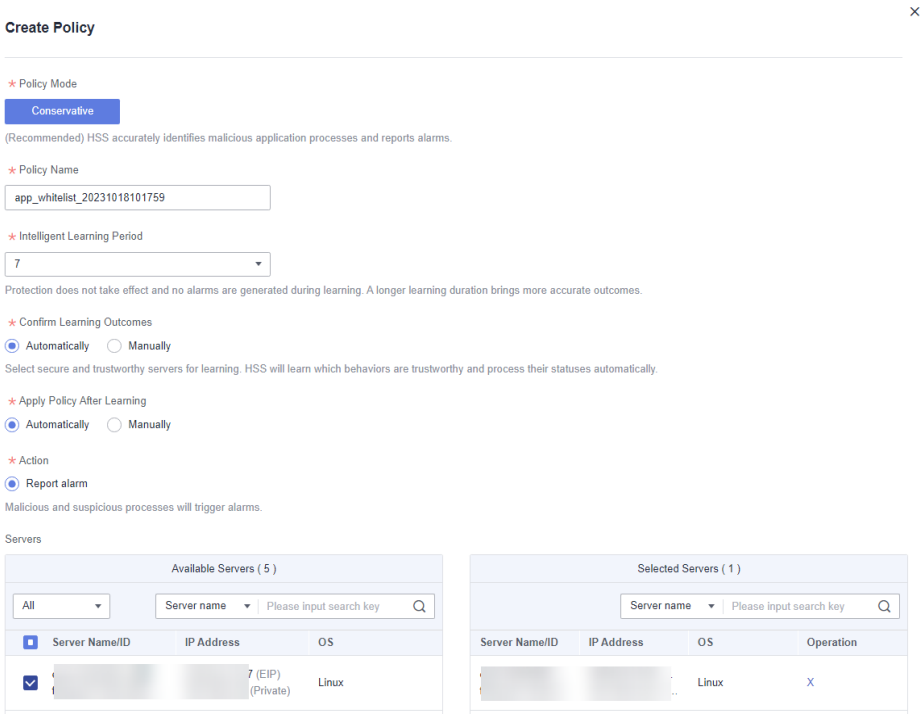


Tabela 5-20 Parâmetros de política da lista branca

Parâmetro	Descrição
Policy Mode	Modo da política de controle do processo da aplicação. O modo conservador é usado por padrão. Processos confiáveis e suspeitos podem ser executados. Os alarmes são gerados apenas para processos maliciosos.
Policy Name	Um nome de política de lista branca é gerado por padrão. É aconselhável definir um nome personalizado para facilitar o gerenciamento.
Intelligent Learning Period	Número de dias em que o HSS aprende os processos de aplicação nos servidores. Um longo período de aprendizado indica resultados precisos de aprendizado.
Confirm Learning Outcomes	A maneira de confirmar processos suspeitos com características insignificantes após o HSS concluir o aprendizado nos servidores vinculados à política. ● **Automatically**: o HSS marca automaticamente processos de aplicação suspeitos com características insignificantes com base no banco de dados de assinatura do processo de aplicação. ● **Manually**: escolha **Application Process Control** > **Whitelist Policies**. Clique em um nome de política. Na página de detalhes da política, clique na guia **Process Files** e filtre processos no estado **To be confirmed**. Marque manualmente processos suspeitos com características insignificantes.

Parâmetro	Descrição
Apply Policy After Learning	A forma como o controle do processo de aplicação é ativado depois que o HSS conclui o aprendizado nos servidores vinculados à política. ● **Automatically**: o controle de processo da aplicação é ativado automaticamente depois que o HSS conclui o aprendizado nos servidores vinculados à política. ● **Manually**: ative manualmente o controle do processo da aplicação conforme necessário após o HSS concluir o aprendizado. Para obter mais informações, consulte **Ativação do controle de processo de aplicação**.
Action	Ação tomada quando um processo malicioso é detectado. Alarmes são gerados para processos maliciosos.
Servers	Servidores a serem protegidos. Um servidor é exibido na lista somente se seu **Protection Status** for **Protected**. Para obter mais informações, consulte **Visualização da lista de servidores**.

Passo 6 Clique em **OK**.

Você pode visualizar a política criada e seu status na lista de políticas.

NOTA

Depois que uma política de lista branca é criada, o HSS começa automaticamente a aprender as características do processo de aplicação dos servidores vinculados à política. Se o status da política for alterado para **Learning complete but not in effect**, você poderá **confirmar os resultados de aprendizado**.

----Fim

Operações relacionadas

Editar uma política de lista branca

Você pode modificar o modo de política, a ação ou os servidores protegidos em uma política de lista branca.

Passo 1 Na linha de uma política, clique em **Edit** na coluna **Operation**.

Passo 2 Na caixa de diálogo **Edit Policy**, modifique os parâmetros e clique em **OK**.

----Fim

Excluir uma política de lista branca

Se você não precisar mais do HSS para fornecer controle de processo de aplicação para os servidores vinculados a uma política e não precisar reter as informações de processo de aplicação aprendidas pelo HSS, poderá excluir a política de lista branca. Se você precisar ativar o controle de processo de aplicação para os servidores após a exclusão, o HSS precisará começar a aprender novamente. Tenha cuidado ao realizar esta operação.

Passo 1 Na linha de uma política, clique em **Delete** na coluna **Operation**.

Passo 2 Na caixa de diálogo exibida, clique em **OK**.

----Fim

5.4.3 Confirmação dos resultados de aprendizagem

Depois que o HSS conclui a aprendizagem nos servidores vinculados a uma política de lista branca, pode haver alguns processos suspeitos com características insignificantes que precisam ser confirmados. Você pode manualmente ou deixar o HSS marcá-los automaticamente como processos suspeitos, maliciosos ou confiáveis.

Você pode configurar como confirmar os resultados de aprendizagem ao criar uma política de lista branca. O valor de **Confirm Learning Outcomes** pode ser:

- **Automatically**: os processos suspeitos são automaticamente marcados com base na inteligência do processo de aplicação.
- **Manually**: você precisa verificar e marcar manualmente processos suspeitos. Esta seção descreve o procedimento detalhado.

Pré-requisitos

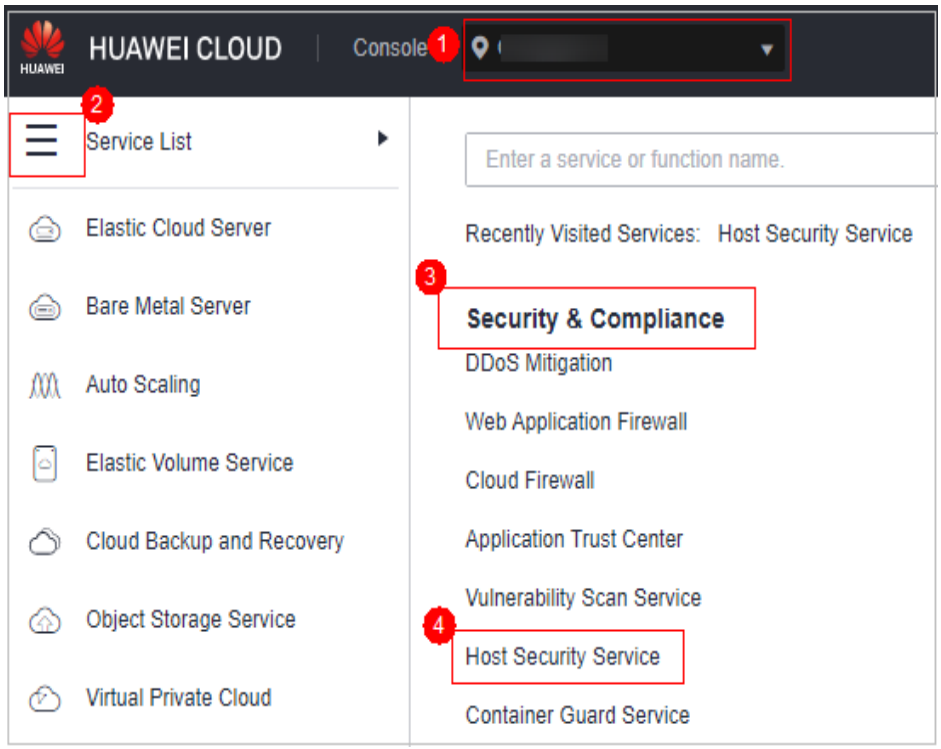
Uma política foi criada e seu status é **Learning complete but not in effect**. Para mais detalhes, consulte **Criação de uma política de lista branca**.

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 5-83 Acessar o HSS



Passo 3 Na árvore de navegação, escolha **Prevention** > **Application Process Control**.

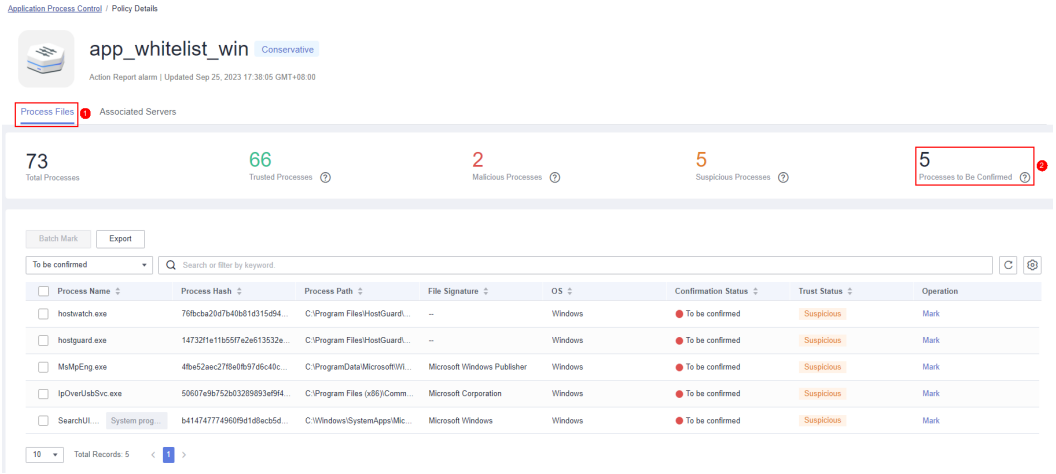
Passo 4 Clique na guia **Whitelist Policies**.

Passo 5 Clique no nome de uma política cujo **Policy Status** é **Learning complete but not in effect**. A página **Policy Details** é exibida.

Passo 6 Clique na guia **Process Files**.

Passo 7 Clique no número de processos a serem confirmados.

Figura 5-84 Visualização de processos a serem confirmados



Passo 8 Verifique se os processos de aplicações são confiáveis com base em seus nomes e caminhos de arquivo.

Passo 9 Na linha de um processo, clique em **Mark** na coluna **Operation**.

Você também pode selecionar todos os processos da aplicação e clicar em **Batch Mark** acima da lista de processos.

Passo 10 Na caixa de diálogo **Mark**, defina **Trust Status**.

Selecione **Suspicious**, **Trusted** ou **Malicious**.

Passo 11 Clique em **OK**.

----Fim

5.4.4 Ativação do controle de processo de aplicação

O HSS pode controlar diferentes tipos de processos de aplicações em servidores. Processos suspeitos e confiáveis podem ser executados, e alarmes são gerados para processos maliciosos.

Você pode configurar como habilitar o controle de processo da aplicação ao criar uma política de lista branca. O valor de **Apply Policy After Learning** pode ser:

- **Automatically**: o controle de processo da aplicação é ativado automaticamente depois que o HSS conclui o aprendizado nos servidores vinculados à política.
- **Manually**: ative manualmente o controle do processo da aplicação conforme necessário após o HSS concluir o aprendizado. Esta seção descreve o procedimento detalhado.

Pré-requisitos

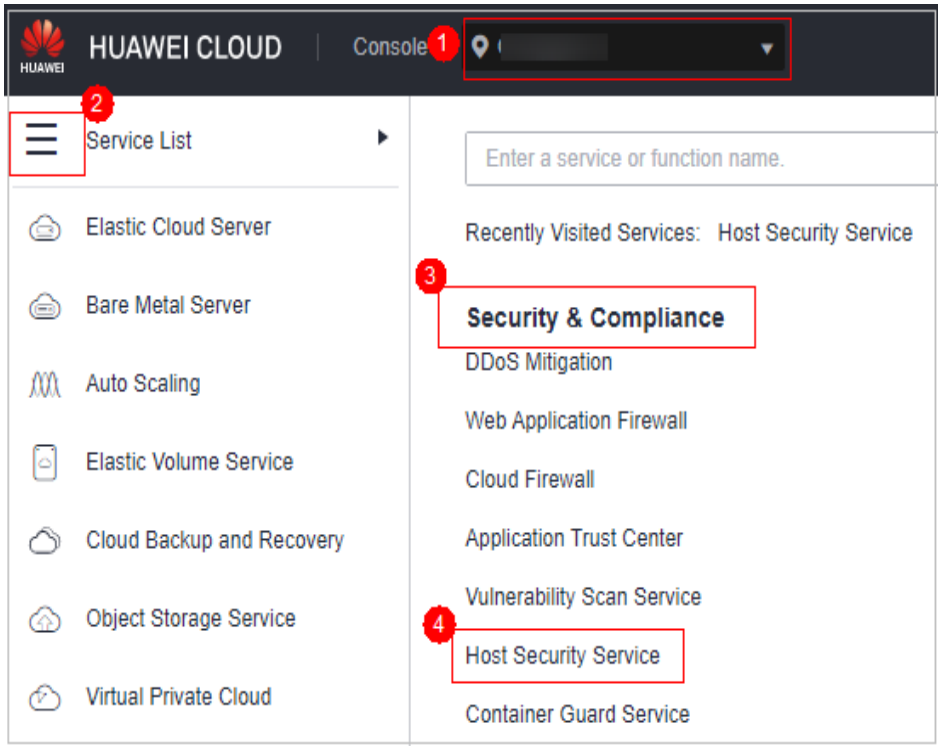
Uma política de lista branca foi criada e os resultados de aprendizado da política foram confirmados. Para mais detalhes, veja **Criação de uma política de lista branca** e **Confirmação dos resultados de aprendizagem**.

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 5-85 Acessar o HSS



Passo 3 Na árvore de navegação, escolha **Prevention** > **Application Process Control**.

Passo 4 Clique na guia **Whitelist Policies**.

Passo 5 Na coluna **Operation** de uma política, clique em **Enable Protection**.

Você também pode selecionar várias políticas e clicar em **Enable Protection** acima da lista de políticas.

Passo 6 Na caixa de diálogo **Enable Protection**, clique em **OK**.

Passo 7 Verifique o status da política. Se **Policy Status** estiver **Learning complete and in effect**, a proteção da aplicação foi ativada.

----Fim

5.4.5 Verificação e tratamento de processos suspeitos

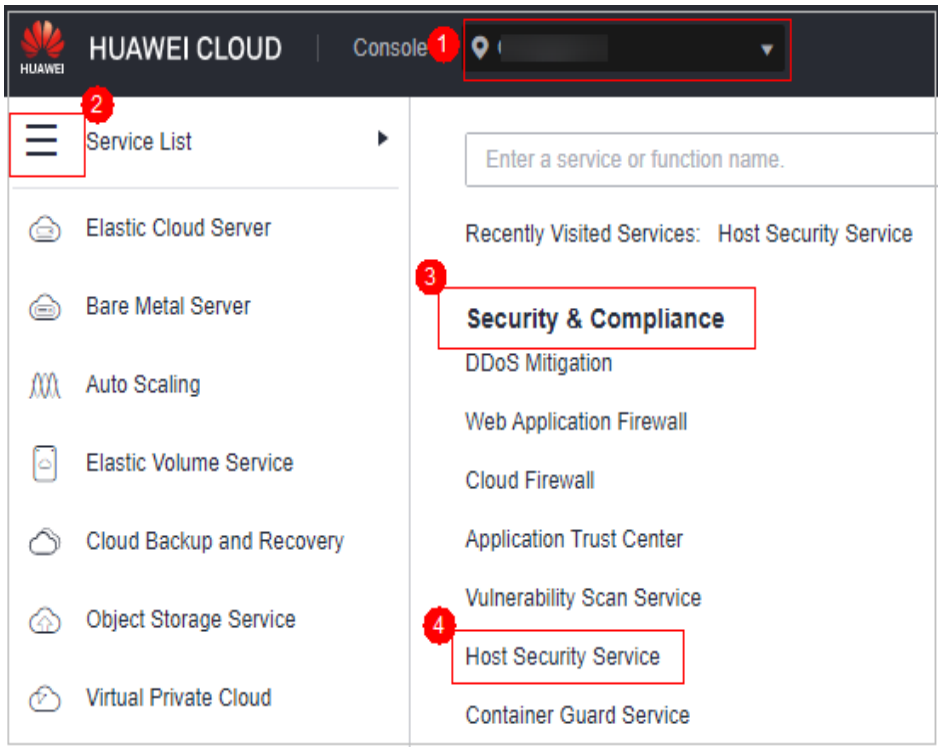
Se o HSS detectar processos suspeitos em servidores, os processos serão exibidos na lista de processos suspeitos, mas não acionarão alarmes. O HSS não pode determinar se esses processos são confiáveis com base nas características do processo da aplicação. Para evitar afetar os serviços, você precisa verificar se os processos podem ser confiáveis, adicionar os confiáveis à lista branca do processo e isolar e eliminar os maliciosos.

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**.

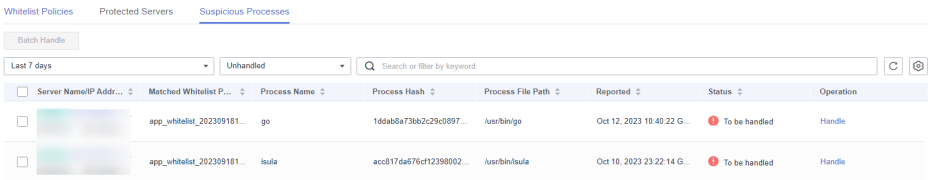
Figura 5-86 Acessar o HSS



Passo 3 Na árvore de navegação, escolha **Prevention** > **Application Process Control**.

Passo 4 Clique na guia **Suspicious Processes**.

Figura 5-87 Visualizar processos suspeitos



Passo 5 Determine se um processo suspeito é malicioso com base em suas informações, como o valor de hash e o caminho do arquivo.

Passo 6 Na linha do processo, clique em **Handle** na coluna **Operation**.

Você também pode selecionar vários processos suspeitos e clicar em **Batch Handle** acima da lista.

Passo 7 Na caixa de diálogo exibida, selecione uma ação.

Selecione **Add to process whitelist** ou **Isolate and kill**.

Passo 8 Clique em **OK**.

----Fim

5.4.6 Extensão da lista branca de processos

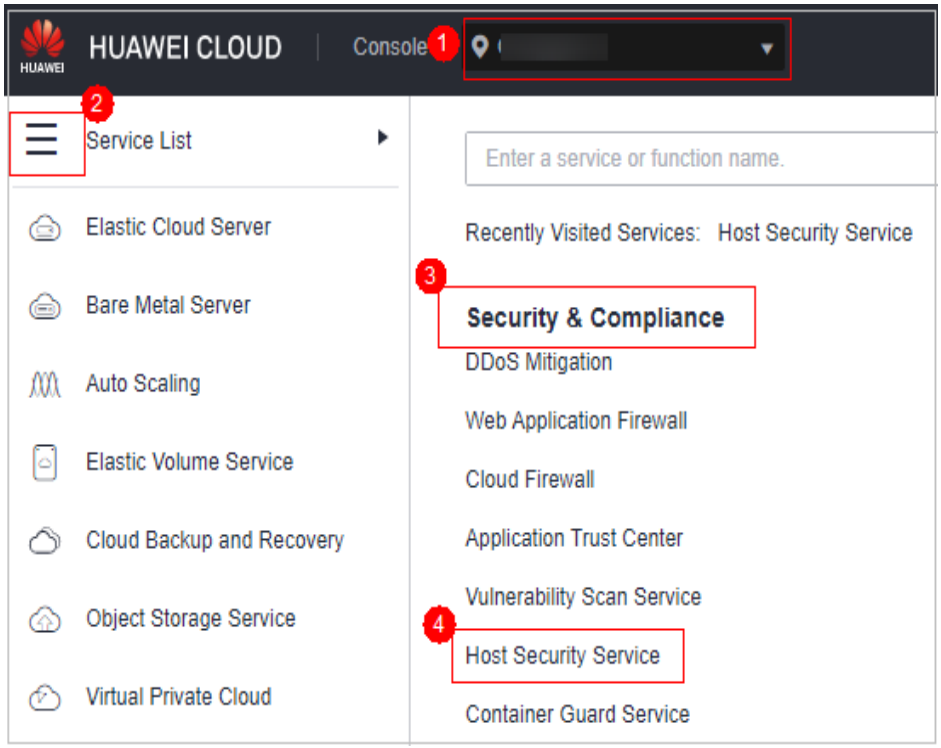
Depois que o HSS concluir o aprendizado nos servidores vinculados a uma política, se você descobrir que os resultados do aprendizado são muito menores do que as impressões digitais do processo detectadas pelo HSS ou se muitos processos suspeitos forem relatados, poderá estender a lista branca. O HSS comparará os processos de aplicação com os quais aprendeu e as impressões digitais de ativos que detectou, identificará processos confiáveis e os adicionará à lista branca do processo.

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 5-88 Acessar o HSS



Passo 3 Na árvore de navegação, escolha **Prevention** > **Application Process Control**.

Passo 4 Clique na guia **Whitelist Policies**.

Passo 5 Clique em um nome de política. A página **Policy Details** é exibida.

Passo 6 Clique na guia **Associated Servers**.

Passo 7 Na linha de um servidor, escolha **More** > **Add to Whitelist** na coluna **Operation**.

Passo 8 Clique em **Compare** para comparar a impressão digital do processo do servidor com os processos da aplicação aprendidos pelo HSS.

Passo 9 Selecione processos confiáveis e clique em **Add**.

----Fim

5.4.7 Começar a aprender novamente nos servidores

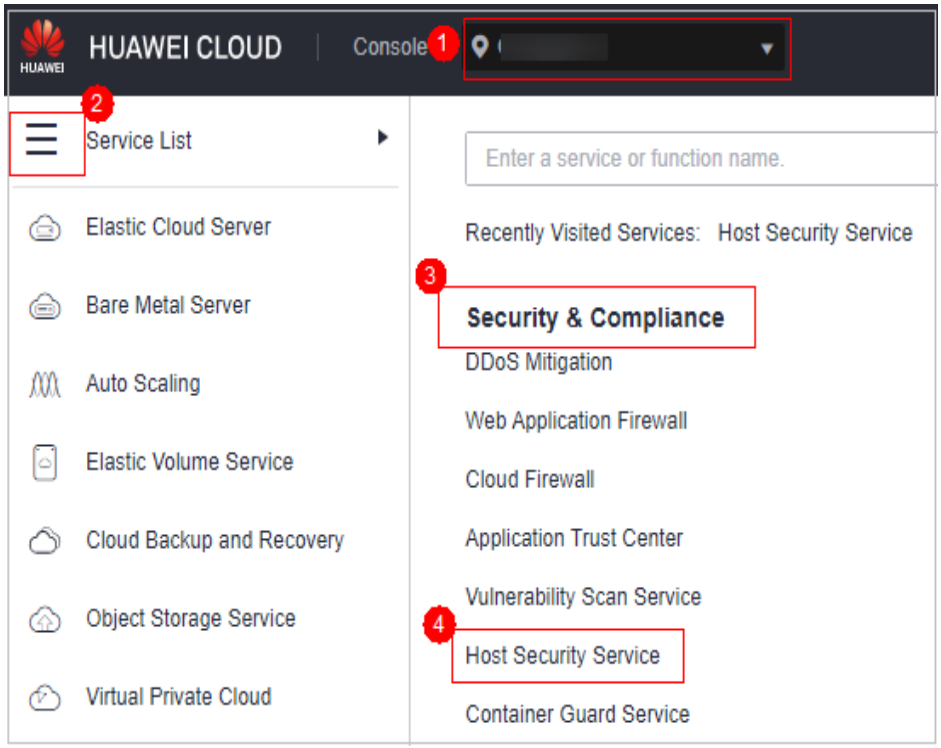
Se você adicionou processos confiáveis à lista branca, mas ainda há muitos falsos positivos relatados, você pode deixar o HSS começar a aprender novamente nos servidores.

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 5-89 Acessar o HSS



Passo 3 Na árvore de navegação, escolha **Prevention** > **Application Process Control**.

Passo 4 Clique na guia **Whitelist Policies**.

Passo 5 Clique em um nome de política. A página **Policy Details** é exibida.

Passo 6 Clique na guia **Associated Servers**.

Passo 7 Selecione servidores e clique em **Learn Again** acima da lista.

Passo 8 Na caixa de diálogo exibida, clique em **OK**.

----Fim

5.4.8 Desativação do controle do processo da aplicação

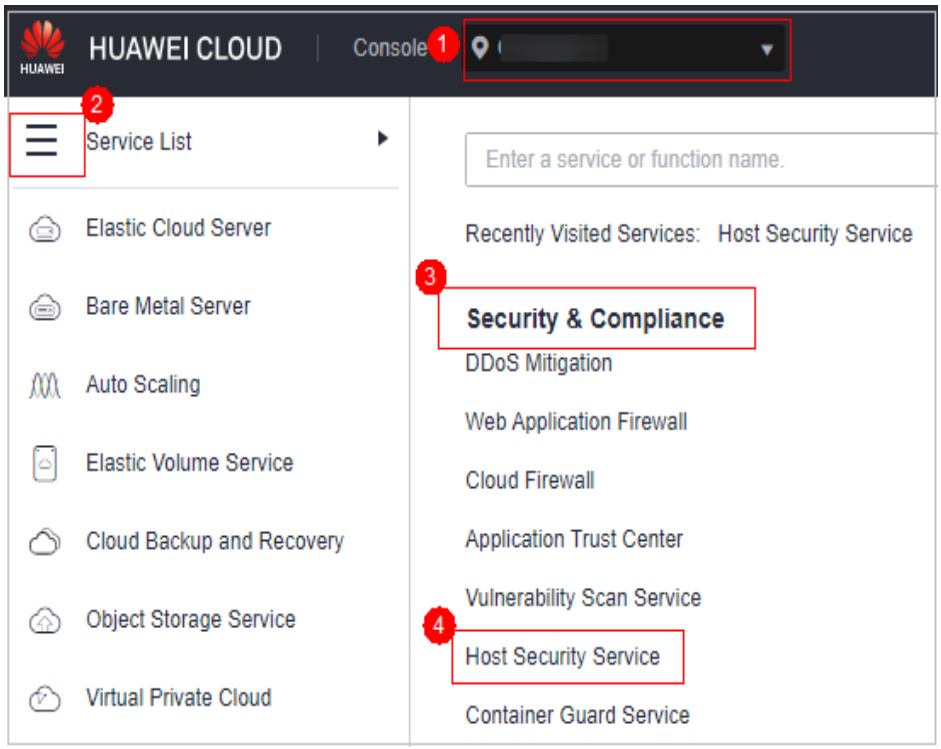
Você pode desativar o controle do processo da aplicação para um ou vários servidores por vez.

Desativação da proteção para servidores vinculados a uma política

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 5-90 Acessar o HSS



Passo 3 Na árvore de navegação, escolha **Prevention** > **Application Process Control**.

Passo 4 Clique na guia **Whitelist Policies**.

Passo 5 Desative o controle de processo da aplicação.

- Desative a proteção, mas retenha as características do processo da aplicação aprendidas pelo HSS.

a. Na coluna **Operation** de uma política, clique em **Disable Protection**. Como alternativa, selecione várias políticas e clique em **Disable** acima da lista de políticas.

b. Clique em **OK**.

- Desative a proteção e exclua as características do processo da aplicação aprendidas pelo HSS.

a. Na linha de uma política, clique em **Delete** na coluna **Operation**.

b. Clique em **OK**.

Passo 6 Verifique a lista de políticas.

- Desative a proteção, mas retenha as características do processo da aplicação aprendidas pelo HSS.

  Se o **Policy Status** da política for **Learning complete but not in effect**, o controle do processo da aplicação foi desativado.
- Desative a proteção e exclua as características do processo da aplicação aprendidas pelo HSS.

  Se a política for eliminada da lista de políticas, o controle do processo da aplicação foi desativado.

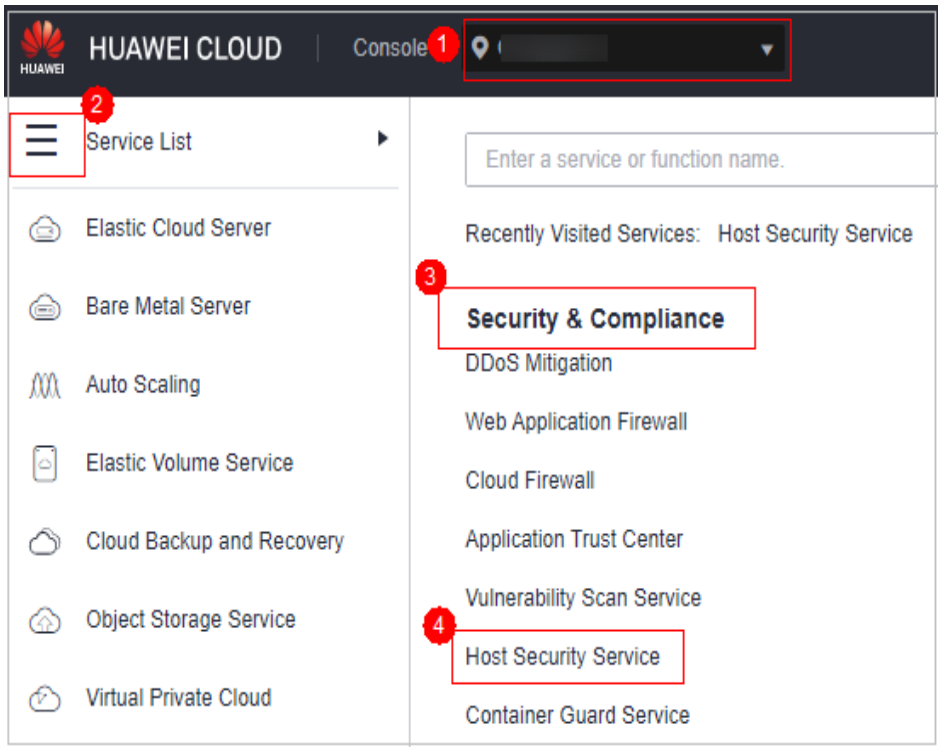
----Fim

Desativação da proteção para um único 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 5-91 Acessar o HSS



Passo 3 Na árvore de navegação, escolha **Prevention** > **Application Process Control**.

Passo 4 Clique na guia **Whitelist Policies**.

Passo 5 Clique em um nome de política. A página **Policy Details** é exibida.

Passo 6 Clique na guia **Associated Servers**.

Passo 7 Desative o controle de processo da aplicação.

- Desative a proteção, mas mantenha a vinculação entre o servidor e a política.
  a. Na coluna **Operation** de uma política, clique em **Disable Protection**. Como alternativa, selecione várias políticas e clique em **Disable** acima da lista de políticas.
  b. Clique em **OK**.
- Desative a proteção e desvincule o servidor da política.

  NOTA

  Para alterar a política de proteção vinculada a um servidor, remova o servidor das definições de política e, em seguida, crie ou edite outra política de proteção para vincular ao servidor.

  a. Na linha que contém a instância desejada, clique em **Delete** na coluna **Operation**.
  b. Clique em **OK**.

Passo 8 Verifique a lista de servidores.

- Desative a proteção, mas mantenha a vinculação entre o servidor e a política.

  Se o **Policy Status** do servidor for **Learning complete but not in effect**, o controle do processo da aplicação foi desativado.
- Desative a proteção e desvincule o servidor da política.

  Se o servidor for excluído da lista, o controle do processo da aplicação será desativado.

----Fim

5.5 Monitoramento da integridade de arquivos

Você pode verificar as estatísticas e detalhes sobre as alterações de arquivo em seus servidores, incluindo servidores afetados, tipos de arquivo, caminhos e conteúdo.

5.5.1 Visualização do gerenciamento de integridade de arquivos

Restrições

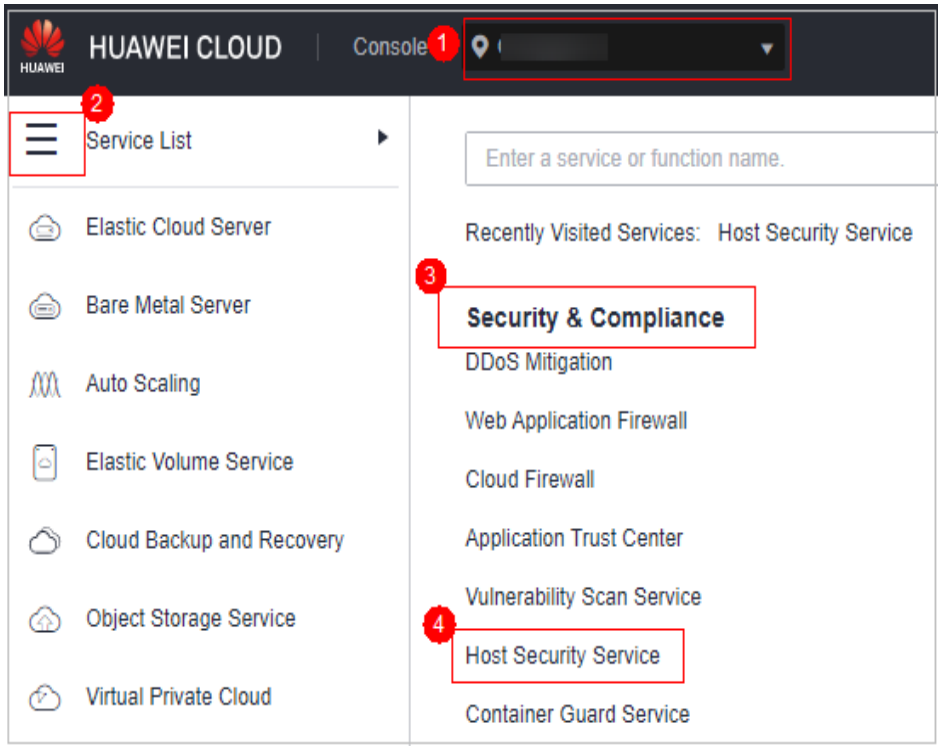
As edições premium e superiores suportam operações relacionadas à integridade do arquivo.

Procedimento

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

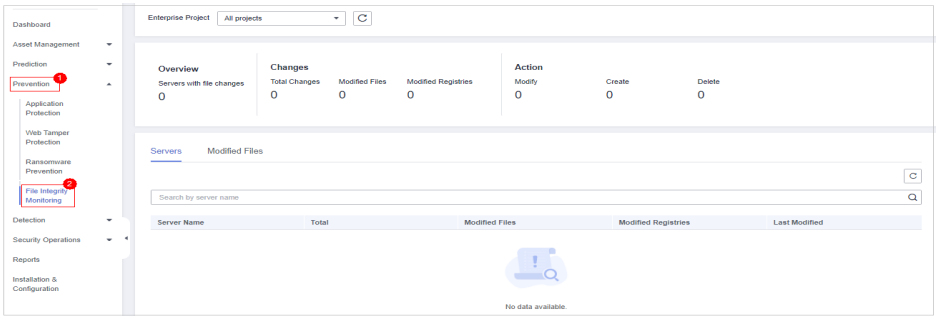
Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 5-92 Acessar o HSS



Passo 3 Escolha **Prevention** > **File Integrity Monitoring**. Na página de gerenciamento de arquivos exibida, selecione um projeto empresarial e verifique seus servidores e arquivos modificados.

Figura 5-93 Monitoramento da integridade de arquivos



----Fim

5.5.2 Verificação de detalhes da alteração

Restrições

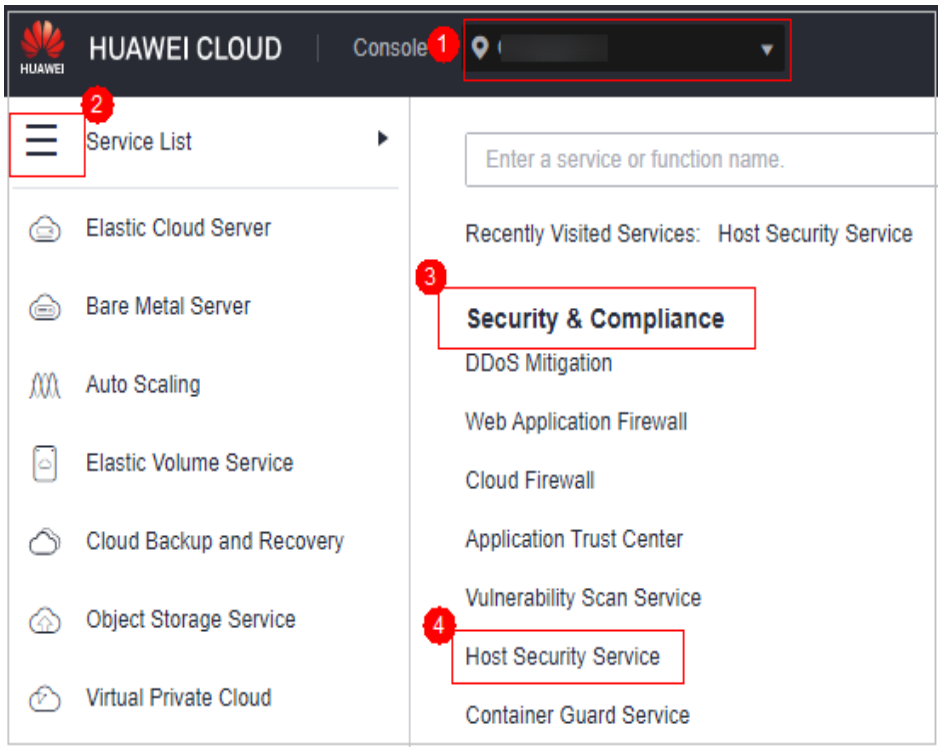
As edições premium e superiores suportam operações relacionadas à integridade do arquivo.

Procedimento

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

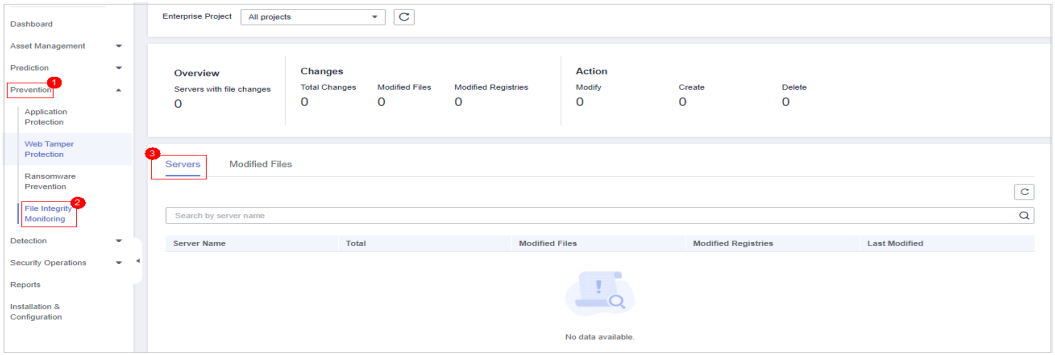
Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 5-94 Acessar o HSS



Passo 3 Escolha **Prevention** > **File Integrity Monitoring**. A guia **Server** será exibida.

Figura 5-95 Visualização da lista de servidores



Passo 4 Clique no nome de um servidor para acessar a página de detalhes da alteração.

Tabela 5-21 Parâmetros sobre alterações de arquivo

Parâmetro	Descrição	Exemplo de valor
File Name	Nome de um arquivo modificado.	du
Path	Caminho de um arquivo modificado.	-
Change Description	Descrição da alteração. Para visualizar os detalhes da alteração, passe o cursor sobre o conteúdo da alteração.	**SHA2560ba0c4b5e48e55a6** é alterado para **4f6079f5b37d1513**.

Parâmetro	Descrição	Exemplo de valor
Server Name	Nome do servidor onde a alteração foi detectada.	-
Type	Tipo de um arquivo modificado. Seu valor pode ser: ● **File**	File
Action	Como um arquivo foi modificado. ● Create ● Modify ● Delete	Modify
Time Range	Hora em que um arquivo foi modificado.	-

----Fim

5.5.3 Verificação de arquivos modificados

Restrições

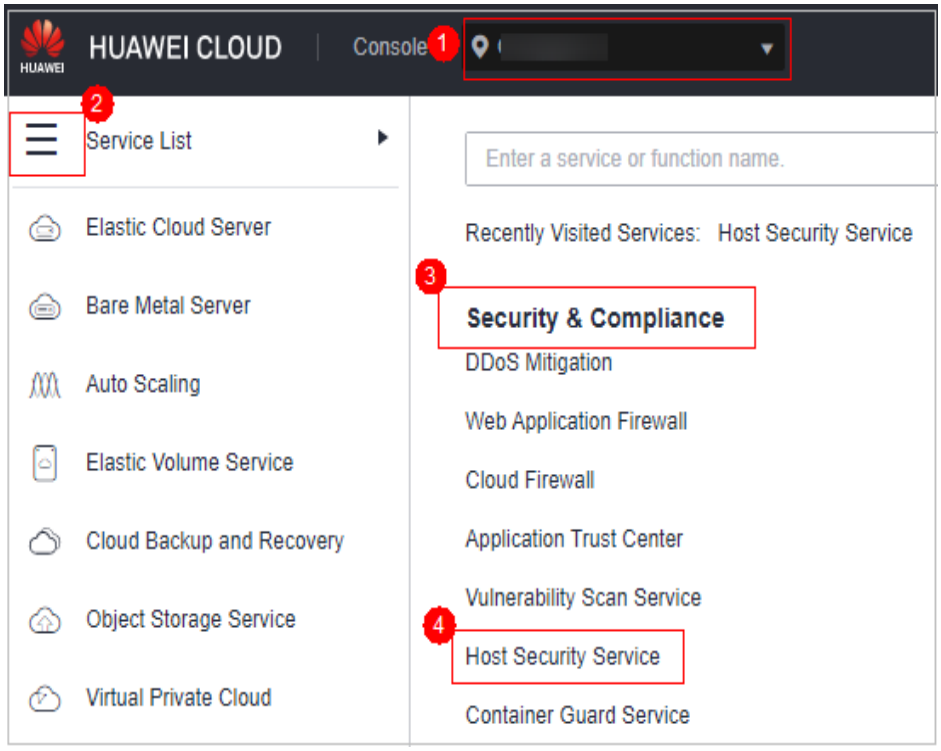
As edições premium e superiores suportam operações relacionadas à integridade do arquivo.

Procedimento

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

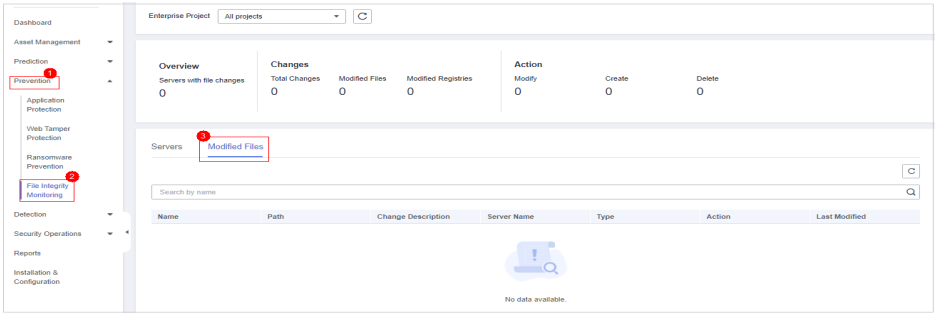
Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security & Compliance** > **Host Security Service**.

Figura 5-96 Acessar o HSS



Passo 3 No painel de navegação, escolha **Prevention** > **File Integrity Monitoring**. Clique na guia **Monitored Files**. Você pode manter o valor padrão para **Enterprise Project**. Para obter detalhes sobre parâmetros, consulte **Tabela 5-21** em **Verificação de detalhes da alteração**.

Figura 5-97 Verificar arquivos modificados



----Fim

5.6 Firewalls de container

5.6.1 Visão geral do firewall de container

Um firewall de container controla e intercepta o tráfego de rede dentro e fora de um cluster de containers para evitar acesso e ataques maliciosos.

Restrições de versões

Somente a edição de container do HSS suporta essa função. Para obter detalhes sobre como comprar e atualizar o HSS, consulte **Compra de uma cota de HSS** e **Atualização de sua edição**.

Como funciona

Um firewall de container controla o escopo de acesso de containers de origem e destino com base nas políticas de acesso para pods e servidores, bloqueando acessos e ataques maliciosos internos e externos.

Tipo de cluster protegido

Clusters comprados no CCE.

Operações relacionadas

- **Criação de uma política (para um cluster usando o modelo de rede de túnel de container)**
- **Criação de uma política (para um cluster usando o modelo de rede da VPC)**

5.6.2 Criação de uma política (para um cluster usando o modelo de rede de túnel de container)

Você pode configurar políticas de rede para limitar o tráfego de acesso aos pods em um cluster usando o modelo de rede de túnel de container. Se nenhuma política de rede estiver configurada, todo o tráfego de entrada e saída dos pods em um namespace será permitido por padrão.

Restrições

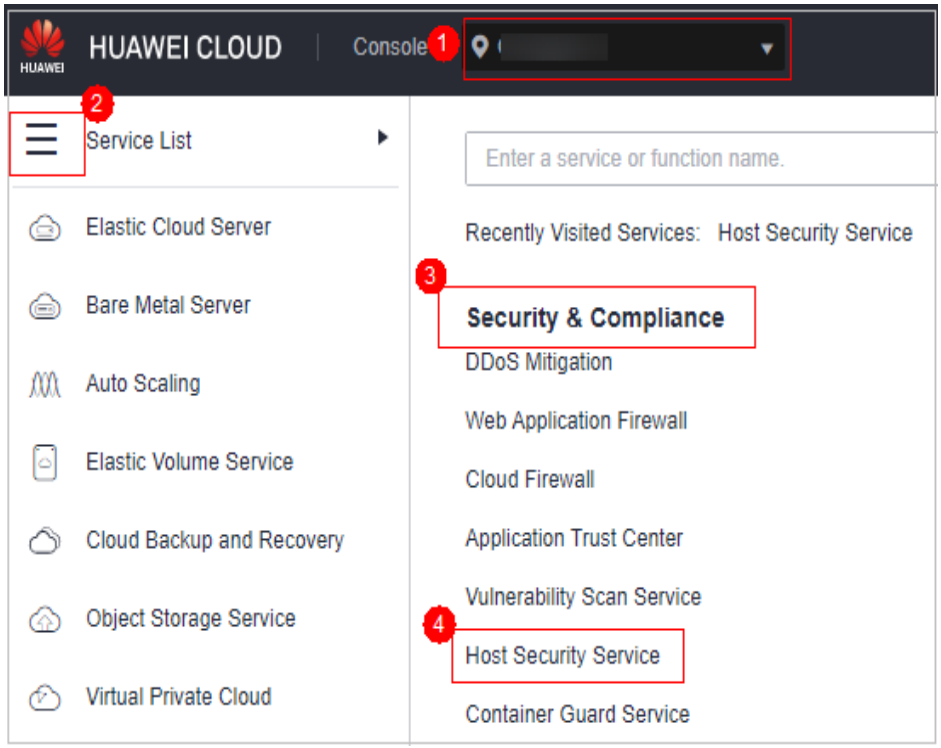
- Apenas os clusters que usam o modelo de rede de túnel suportam políticas de rede. As políticas de rede são classificadas nos seguintes tipos:
  - Regras de entrada, que são suportadas por todas as versões de cluster do CCE.
  - Regras de saída, que são suportadas apenas por clusters do CCE na versão 1.23 e posterior.
- O isolamento de rede não é suportado para endereços IPv6.

Criação de uma política de rede a partir de YAML

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 5-98 Acessar o HSS



Passo 3 No painel de navegação, escolha **Prevention** > **Container Firewalls**.

Passo 4 Clique em **Manage Policy** na coluna **Operation** de um cluster usando o modelo de rede de túnel de container.

Passo 5 Clique em **Create from YAML** acima da lista de políticas.

Passo 6 Na página de criação de YAML, insira o conteúdo ou clique em **Import**.

Um exemplo de uma política de rede criada a partir de YAML é o seguinte:

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: test-network-policy
  namespace: default
spec:
  podSelector:                  # The rule takes effect for pods with the role=db
label.
    matchLabels:
      role: db
  policyTypes:
    - Ingress
    - Egress
  ingress:                      # Ingress rule
    - from:
        - namespaceSelector: # Only namespaces with project=myproject can be
accessed.
            matchLabels:
              project: myproject
        - podSelector:              # Only the traffic from the pods with the
role=frontend label is allowed.
            matchLabels:
              role: frontend
      ports                       # Only TCP can be used to access port 6379.
        - protocol: TCP
          port: 6379
```



```
  egress:                           # Egress rule
    - to:
        - ipBlock:                  #Only the 10.0.0.0/24 network segment of the
destination object can be accessed.
            cidr: 10.0.0.0/24
      ports:                        # Only TCP can be used to access port 6379 of
the destination object.
        - protocol: TCP
          port: 6379
```

Passo 7 Clique em **OK**.

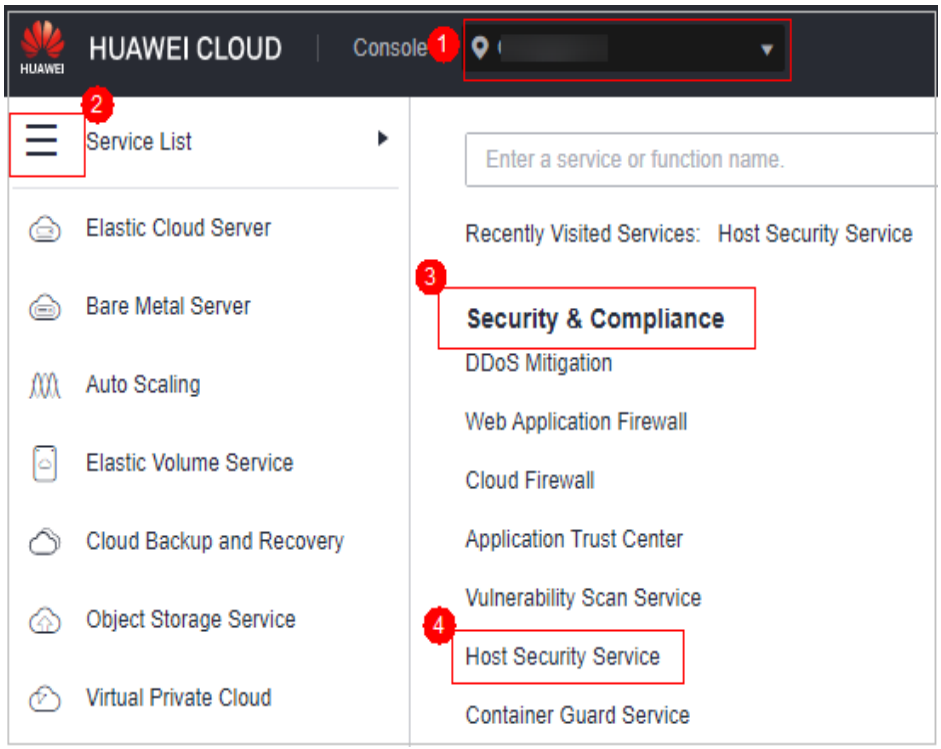
----Fim

Criação de uma política de rede na GUI

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 5-99 Acessar o HSS



Passo 3 No painel de navegação, escolha **Prevention** > **Container Firewalls**.

Passo 4 Clique em **Manage Policy** na coluna **Operation** de um cluster usando o modelo de rede de túnel de container.

Passo 5 Clique em **Create Network Policy** acima da lista de políticas de rede.

- **Policy Name**: insira um nome de política de rede.
- **Namespace**: selecione um namespace para a política de rede.
- **Selector**: insira uma chave e um valor para definir o pod a ser vinculado e clique em **Add**. Você também pode clicar em **Reference Workload Label** para fazer referência ao

rótulo de uma carga de trabalho existente. Se esse parâmetro não for especificado, todos os pods no namespace serão vinculados por padrão.

- Regra de entrada: clique em **Add Rule** na área **Inbound Rules**. Para obter mais informações, consulte **Tabela 5-22**.

Tabela 5-22 Adicionar uma regra de entrada

Parâmetro	Descrição
Protocol & Port	Insira o tipo de protocolo de entrada e o número da porta dos pods a serem vinculados. Atualmente, TCP e UDP são suportados. Se este parâmetro não for especificado, todo o tráfego de acesso será permitido.
Source Namespace	Selecione um namespace cujos objetos possam ser acessados. Se esse parâmetro não for especificado, será permitido o acesso aos objetos que pertencem ao mesmo namespace que a política atual.
Source Pod Label	Selecione um rótulo. Pods com este rótulo podem ser acessados. Se esse parâmetro não for especificado, todos os pods no namespace poderão ser acessados.

- Regra de saída: clique em **Add Rule** na área **Outbound Rules**. Para obter mais informações, consulte **Tabela 5-23**.

Tabela 5-23 Adicionar uma regra de saída

Parâmetro	Descrição
Protocol & Port	Insira a porta e o protocolo dos objetos de destino. Se este parâmetro não for especificado, o acesso não é limitado.
Destination CIDR Block	Configure blocos CIDR. Este parâmetro permite que as solicitações sejam roteadas para um bloco CIDR especificado (e não para os blocos CIDR de exceção). Separe os blocos CIDR de destino e exceção por barras verticais (|), e separe vários blocos CIDR de exceção por vírgulas (,). Por exemplo, 172.17.0.0/16|172.17.1.0/24,172.17.2.0/24 indica que 172.17.0.0/16 está acessível, mas não para 172.17.1.0/24 ou 172.17.2.0/24.
Destination Namespace	Namespace onde o objeto de destino está localizado. Se não for especificado, o objeto pertence ao mesmo namespace da política atual.
Destination Pod Label	Selecione um rótulo. Pods com este rótulo podem ser acessados. Se esse parâmetro não for especificado, todos os pods no namespace poderão ser acessados.

Passo 6 Clique em **OK**.

----Fim

Operações relacionadas

Sincronização de políticas de rede do CCE

As políticas de rede criadas no CCE podem ser sincronizadas com o HSS.

Passo 1 Clique em **Synchronize** acima da lista de políticas de rede.

Passo 2 Verifique o valor de **Last synchronized**. Se ele mudar para a hora de conclusão da tarefa de sincronização mais recente, a sincronização está concluída.

----Fim

5.6.3 Criação de uma política (para um cluster usando o modelo de rede da VPC)

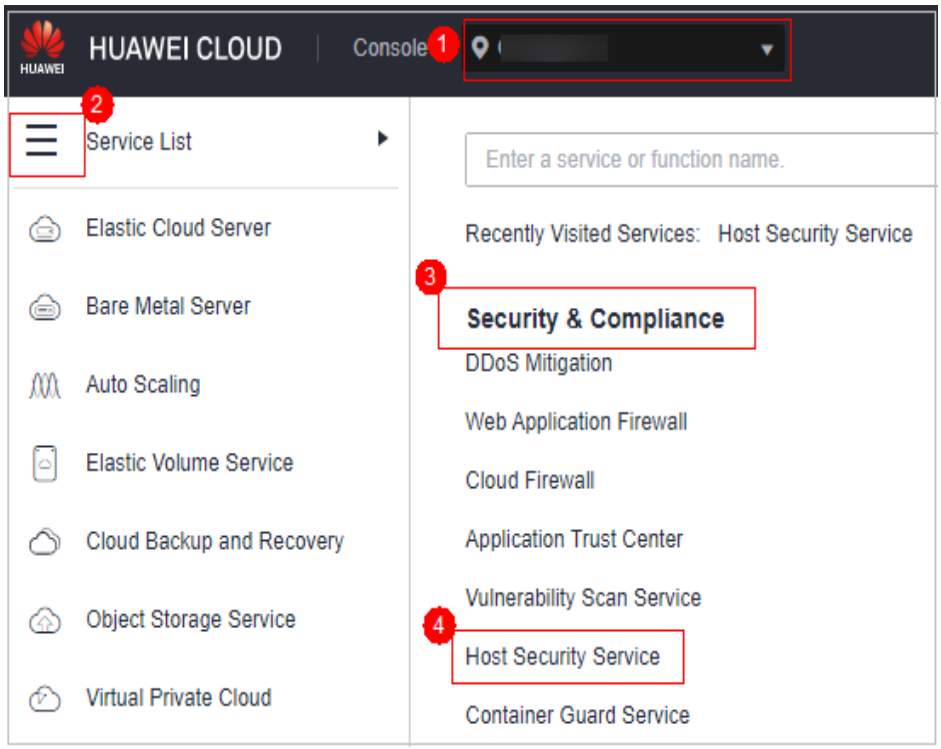
Para clusters que usam o modelo de rede da VPC, você pode configurar regras de grupo de segurança para limitar o tráfego que acessa os servidores nos quais os containers são implementados. Se nenhuma regra de grupo de segurança estiver configurada, todo o tráfego de entrada e saída dos servidores será permitido por padrão.

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 5-100 Acessar o HSS



Passo 3 No painel de navegação, escolha **Prevention** > **Container Firewalls**.

Passo 4 Clique em **Manage Policy** na coluna **Operation** de um cluster usando o modelo de rede da VPC.

Passo 5 Na coluna **Operation** de um nó, clique em **Configure Policy**.

Passo 6 Na caixa de diálogo exibida, clique em **OK** para ir para o console do servidor de nuvem.

Passo 7 Clique na guia **Security Groups** e visualize as regras do grupo de segurança.

Passo 8 Clique em **Manage Rule**. A página do grupo de segurança é exibida.

Passo 9 Configure regras de entrada e saída.

Para obter detalhes, consulte **Adição de uma regra de grupo de segurança**.

----Fim

5.6.4 Gerenciamento de políticas (para um cluster que usa o modelo de rede de túnel de containers)

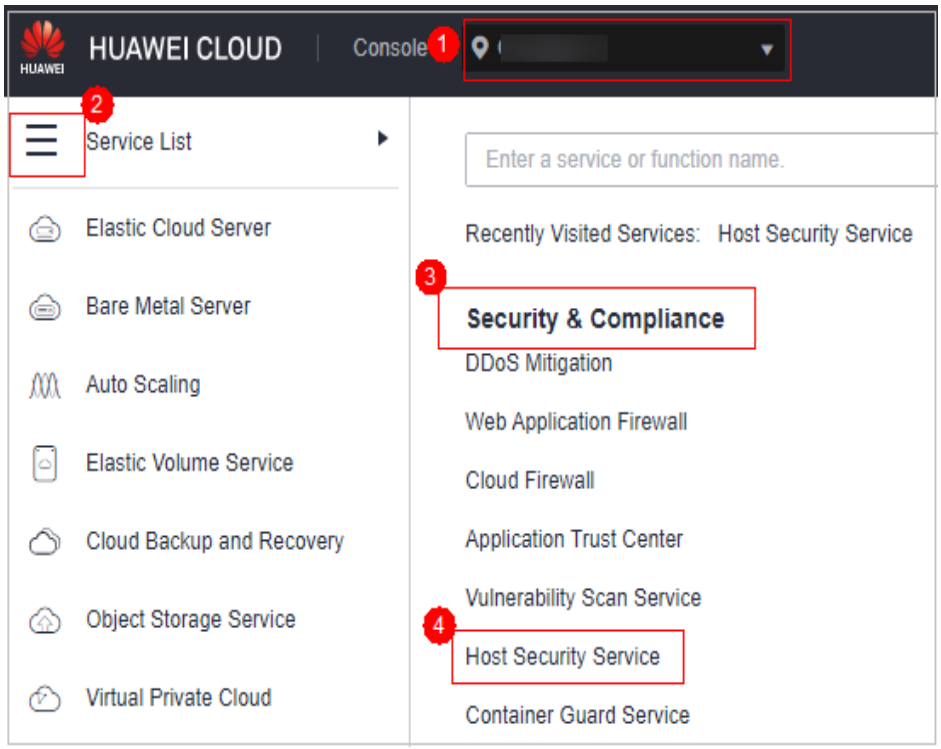
Você pode modificar ou excluir as políticas de um cluster usando o modelo de rede de túnel de container.

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 5-101 Acessar o HSS



Passo 3 No painel de navegação, escolha **Prevention** > **Container Firewalls**.

Passo 4 Clique em **Manage Policy** na coluna **Operation** de um cluster usando o modelo de rede da VPC.

Passo 5 Clique em **Synchronize** acima da lista de políticas de rede.

Passo 6 Verifique o valor de **Last synchronized**. Se ele mudar para a hora de conclusão da tarefa de sincronização mais recente, a sincronização está concluída.

Passo 7 Gerencie políticas conforme necessário.

- Modificação de uma política
  - Na coluna **Operation** de uma política, clique em **Edit YAML**. Na página de YAML, modifique o conteúdo de YAML e clique em **OK**.
  - Na coluna **Operation** de uma política, clique em **Update**. Modifique as informações da política de rede e clique em **OK**.
- Exclusão de uma política
  - Na coluna **Operation** de uma política, clique em **Delete**. Na caixa de diálogo de confirmação, clique em **OK**.
  - Selecione uma ou várias políticas e clique em **Delete** acima da lista de políticas. Na caixa de diálogo exibida, clique em **OK**.

----Fim

5.6.5 Gerenciamento de políticas (para um cluster que usa o modelo de rede da VPC)

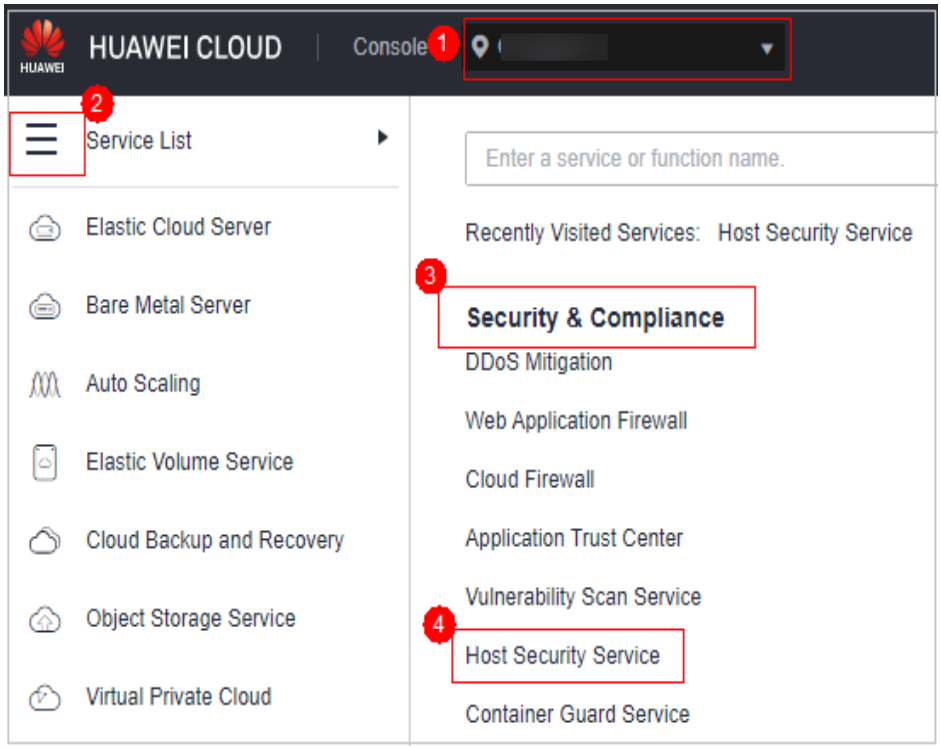
Você pode modificar ou excluir as políticas de um cluster usando o modelo de rede da VPC.

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 5-102 Acessar o HSS



Passo 3 No painel de navegação, escolha **Prevention** > **Container Firewalls**.

Passo 4 Clique em **Manage Policy** na coluna **Operation** de um cluster usando o modelo de rede da VPC.

Passo 5 Clique em **Synchronize** acima da lista de nós para sincronizar as informações do nó.

Passo 6 Verifique o valor de **Last synchronized**. Se ele mudar para a hora de conclusão da tarefa de sincronização mais recente, a sincronização está concluída.

Passo 7 Na coluna **Operation** de um nó, clique em **Configure Policy**.

Passo 8 Na caixa de diálogo exibida, clique em **OK** para ir para o console do servidor de nuvem.

Passo 9 Clique na guia **Security Groups** e visualize as regras do grupo de segurança.

Passo 10 Clique em **Manage Rule**. A página do grupo de segurança é exibida.

Passo 11 Clique em uma guia de regras e gerencie as regras conforme necessário.

- Modificar uma regra

  Na coluna **Operation** de uma regra, clique em **Modify**. Modifique a regra e clique em **OK**.
- Excluir uma regra

  Na coluna **Operation** de uma regra, clique em **Delete**. Na caixa de diálogo de confirmação, clique em **OK**.

----Fim

5.7 Proteção do cluster de containers

5.7.1 Visão geral da proteção de cluster de containers

O HSS pode verificar problemas de linha de base de não conformidade, vulnerabilidades e arquivos maliciosos quando uma imagem de container é iniciada e relatar alarmes ou bloquear a inicialização do container que não foi autorizada ou pode incorrer em altos riscos.

Você pode configurar políticas de proteção de cluster de container para bloquear imagens com vulnerabilidades, arquivos maliciosos, linhas de base não compatíveis ou outras ameaças, reforçando a segurança do cluster.

Restrições

Para ativar a proteção de cluster de containers, as seguintes condições devem ser atendidas:

- Você comprou um cluster do CCE na versão 1.20 ou posterior.
- A edição de container do HSS foi ativada para servidores de nó de container. Para obter mais informações, consulte **Compra de cotas do HSS**.
- A versão do agente do servidor se enquadra no escopo a seguir. Para obter mais informações, consulte **Atualização do agente**.
  - Linux: 3.2.7 ou posterior
  - Windows: 4.0.19 ou posterior

Processo de uso da proteção de cluster de container

Figura 5-103 Processo de uso

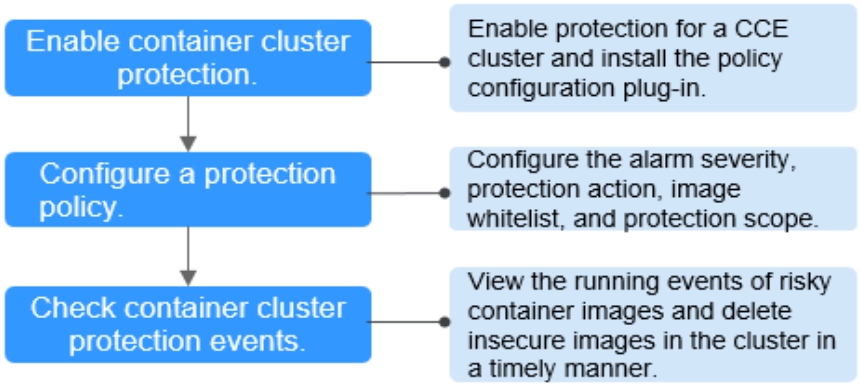


Tabela 5-24 Processo de uso da proteção de cluster de containers

Procedimento	Descrição
Ativar proteção de cluster de containers.	Ativar a proteção de um cluster do CCE para proteger suas cargas de trabalho e a segurança de dados críticos. Quando a proteção é ativada, o HSS instala automaticamente o plug-in de gerenciamento de políticas no cluster.

Procedimento	Descrição
Configurar uma política de proteção.	Configurar a gravidade dos riscos de linha de base, vulnerabilidade e arquivo malicioso que acionam alarmes; escopo de proteção de clusters de containers; lista branca de imagens; e ações a serem tomadas em alarmes.
Verificar os eventos de proteção do cluster de container.	No console do HSS, você pode visualizar eventos de execução de imagens de container não autorizados ou de alto risco que são relatados ou bloqueados e verificar e limpar imagens de container inseguras em tempo hábil.

5.7.2 Ativação da proteção de cluster de container

A proteção de cluster de containers pode detectar riscos em linhas de base, vulnerabilidades e arquivos maliciosos; e pode relatar alarmes ou bloquear imagens de container inseguras. Você pode ativar a proteção para aprimorar a defesa de clusters e proteger containers.

Pré-requisitos

Para ativar a proteção de cluster de containers, as seguintes condições devem ser atendidas:

- Você comprou um cluster do CCE na versão 1.20 ou posterior.
- A edição de container do HSS foi ativada para servidores de nó de container. Para obter mais informações, consulte **Compra de cotas do HSS**.
- A versão do agente do servidor se enquadra no escopo a seguir. Para obter mais informações, consulte **Atualização do agente**.
  - Linux: 3.2.7 ou posterior
  - Windows: 4.0.19 ou posterior

Restrições

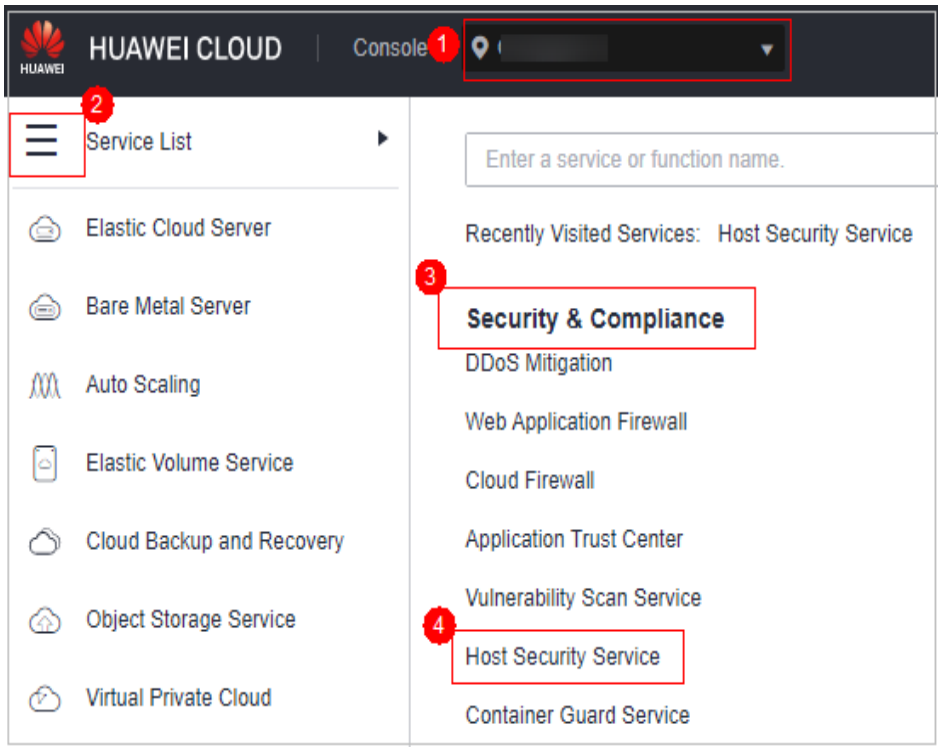
Depois que a proteção de cluster de containers estiver ativada, você precisará configurar uma política para que a proteção tenha efeito. Para obter mais informações, consulte **Configuração de uma política de proteção de cluster de container**.

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 5-104 Acessar o HSS



Passo 3 No painel de navegação, escolha **Prevention** > **Container Cluster Protection**.

Passo 4 Clique na guia **Protected Clusters**.

Passo 5 Clique em **Synchronize** para sincronizar os clusters do CCE.

Passo 6 Na coluna **Operation** de um cluster, clique em **Enable Protection**.

Para ativar a proteção para clusters em lotes, selecione clusters e clique em **Enable Protection** no canto superior esquerdo da lista de clusters.

AVISO

- Depois que a proteção de cluster de containers estiver ativada para um cluster, o plug-in de gerenciamento de políticas será instalado no cluster e ocupará alguns recursos do cluster.
- Ao ativar a proteção para um cluster de containers, não execute nenhuma operação no cluster. Caso contrário, a proteção não será ativada.

Passo 7 Clique em **OK**.

Se o **Protection Status** do cluster de container estiver **Enabled but not configured**, isso indicará que a proteção foi configurada para o cluster e o plug-in de gerenciamento de políticas foi instalado, mas o HSS não foi iniciado para proteger o cluster. Nesse caso, você precisa configurar uma política de proteção. Para obter mais informações, consulte **Configuração de uma política de proteção de cluster de container**.

----Fim

5.7.3 Configuração de uma política de proteção de cluster de container

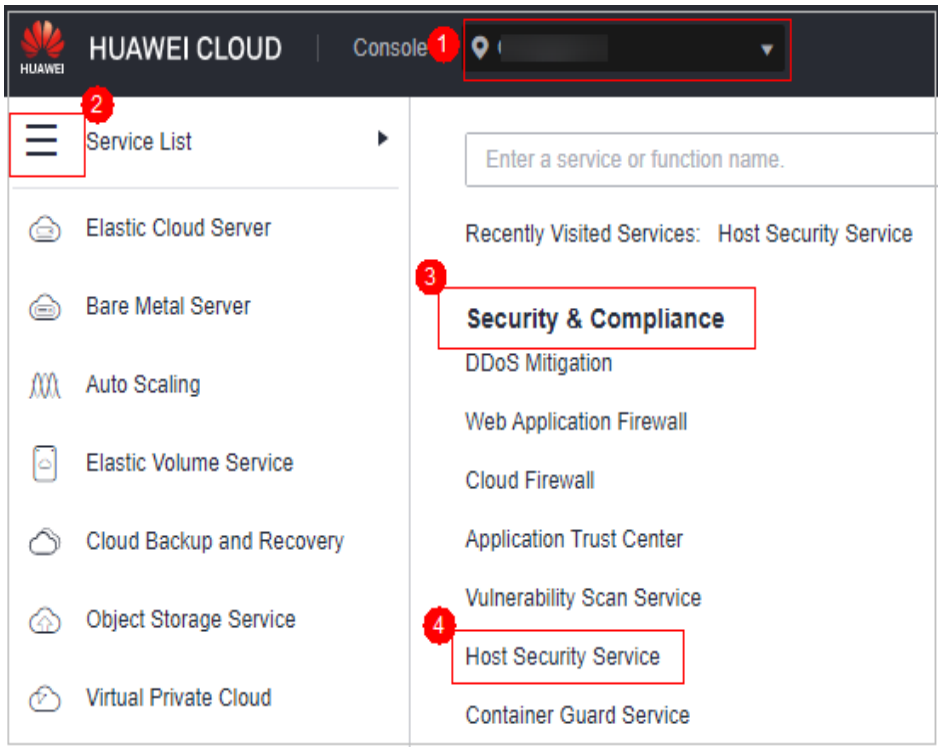
Você pode configurar políticas de proteção de clusters de containers para especificar o nível de riscos (linhas de base inseguras, vulnerabilidades ou arquivos maliciosos) que acionam alarmes, escopo de proteção de cluster, lista branca de imagens e as ações realizadas em um alarme.

Criação de uma política

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 5-105 Acessar o HSS



Passo 3 No painel de navegação, escolha **Prevention** > **Container Cluster Protection**.

Passo 4 Clique na guia **Protection Policies** e clique em **Create Policy**.

Passo 5 Configure os parâmetros na caixa de diálogo **Create Policy**.

1. Configure uma política de proteção. A tabela a seguir descreve os parâmetros.

Tabela 5-25 Parâmetros de política de proteção de clusters de containers

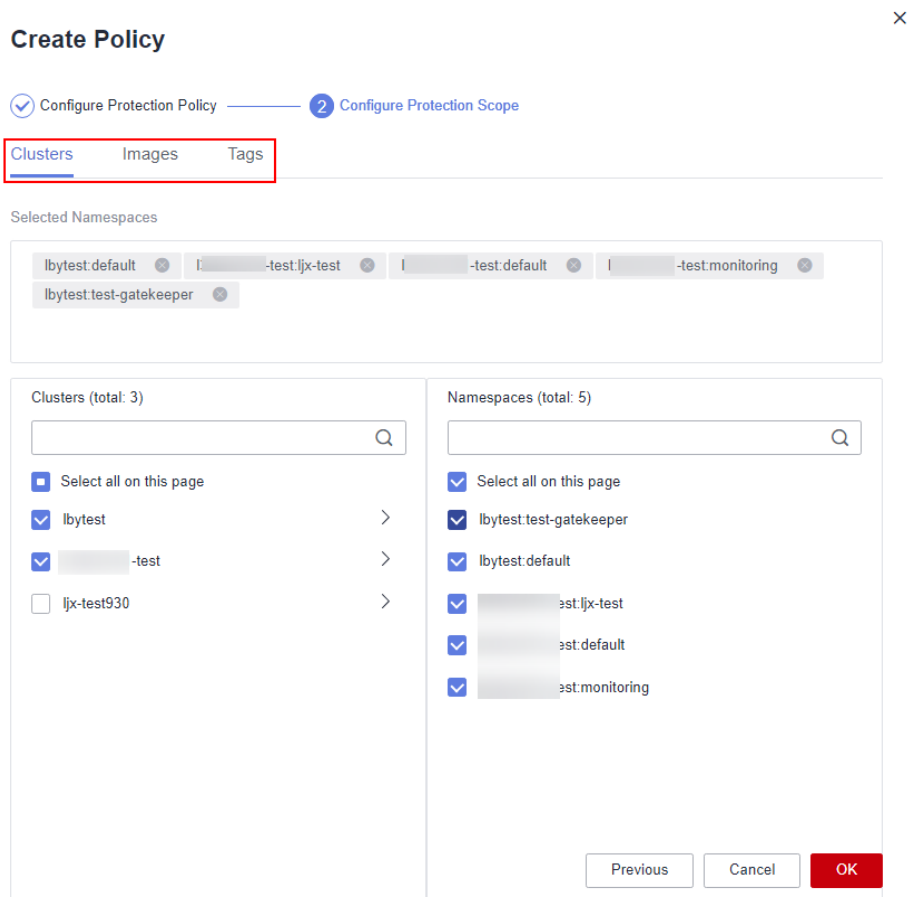
Parâmetro	Descrição
Policy Template	Selecione um modelo de política.
Policy Name	Nome da política definida pelo usuário.
Policy Description	Descrição sobre a política.
Block Unscanned Images	Se deve bloquear imagens que não foram verificadas usando a função de segurança de imagens de container de HSS. –  : desabilitar –  : habilitar
Política de alarme	Tipo de política de alarme. – **Baseline** – **Vulnerability** – **Malicious script**
Risk Level	Nível de risco que aciona um alarme. – **High** – **Medium** – **Low**
Baseline Item	Configure itens de linha de base não seguros. Se uma imagem a ser iniciada contiver qualquer um desses itens, o HSS tomará as ações especificadas imediatamente.
Vulnerability Item	Configure vulnerabilidades. Se uma imagem a ser iniciada contiver qualquer uma dessas vulnerabilidades, o HSS tomará as ações especificadas imediatamente.
Malicious Sample	Configure amostras maliciosas. Se uma imagem a ser iniciada contiver qualquer uma dessas amostras, o HSS tomará as ações especificadas imediatamente.
Action	Ação tomada pelo HSS se detectar que uma imagem a ser iniciada contém itens de linha de base não seguros especificados, vulnerabilidades ou scripts maliciosos. – **Alarm**: gerar um evento cuja **Action** seja **Alarm** na guia **Protection Events** da página **Container Cluster Protection**. – **Block**: bloquear uma imagem insegura e gerar um evento cuja **Action** é **Block** na guia **Protection Events** da página **Container Cluster Protection**. – **Allow**: gerar um evento cuja **Action** seja **Allow** na guia **Protection Events** da página **Container Cluster Protection**.

Parâmetro	Descrição
Add to Whitelist	Imagens a serem adicionadas à lista branca. Insira os valores no formato *ImageName*:*ImageVersion*. Um nome de imagem pode conter apenas números, letras, sublinhados (_), hifens (-) e pontos (.). Cada nome de imagem ocupa uma linha separada. Exemplo: – Uma única imagem **image:1.0** – Várias imagens **image1:1.0** **image2:1.0** **AVISO** Tenha cuidado ao realizar esta operação. O HSS não verifica as imagens na lista branca quando elas são iniciadas.

2. Clique em **Next**.
3. Configure o escopo de proteção.

   Configure o escopo de proteção de clusters, imagens e tags.

Figura 5-106 Configuração do escopo de proteção



Passo 6 Clique em **OK**.

Você pode exibir a nova política de proteção na lista de políticas.

----Fim

Edição ou exclusão de uma política de proteção de cluster

Passo 1 Escolha **Container Cluster Protection** e clique na guia **Protection Policies**.

Passo 2 Na coluna **Operation** de uma política, clique em um botão conforme necessário.

- **Edit**: modificar uma política de proteção.
- **Delete**: excluir uma política de proteção.

AVISO

Depois que uma política for excluída, os clusters de containers vinculados a ela não serão protegidos. Tenha cuidado ao realizar esta operação.

Passo 3 Clique em **OK**.

----Fim

5.7.4 Verificação de eventos de proteção de cluster de container

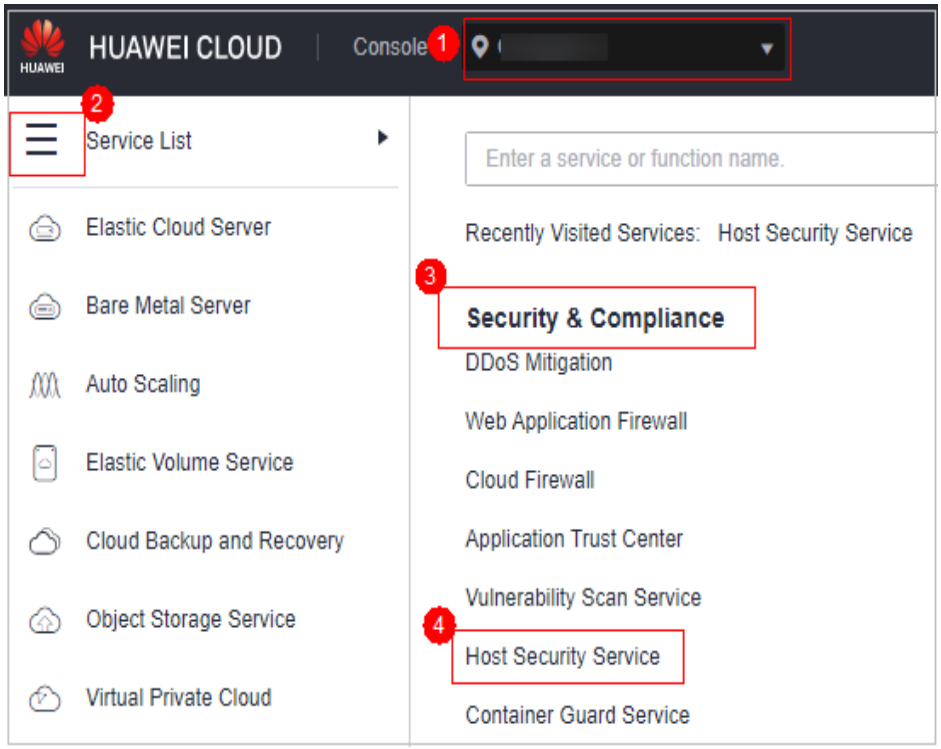
O HSS detecta riscos e exibe eventos de segurança na lista de eventos de proteção. Esta seção descreve como verificar os eventos.

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 5-107 Acessar o HSS



Passo 3 No painel de navegação, escolha **Prevention** > **Container Cluster Protection**.

Passo 4 Clique na guia **Protection Events** e verifique os eventos no cluster.

Passo 5 Clique em um nome de alarme para visualizar os recursos afetados.

----Fim

5.7.5 Desativação da proteção de cluster de containers

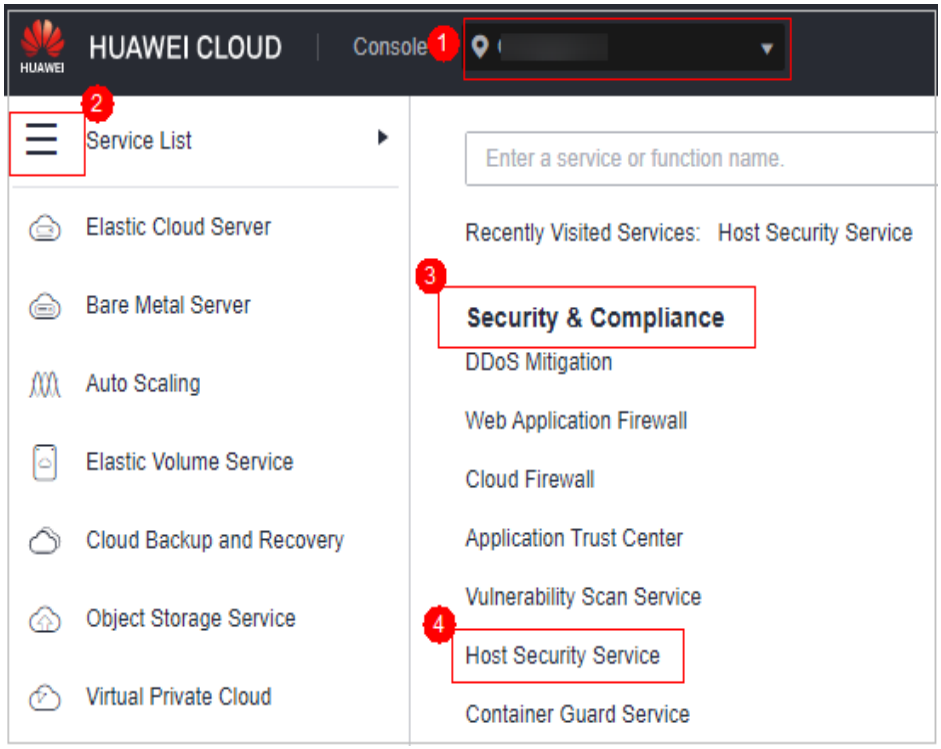
Se você não precisar mais do HSS para proteger seus clusters de container, poderá desativar a proteção de cluster de container.

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 5-108 Acessar o HSS



Passo 3 No painel de navegação, escolha **Prevention** > **Container Cluster Protection**.

Passo 4 Clique na guia **Protected Clusters**.

Passo 5 Na coluna **Operation** de um cluster, clique em **Disable Protection**.

Para desativar a proteção de clusters em lotes, selecione clusters e clique em **Disable Protection** no canto superior esquerdo da lista de clusters.

Passo 6 Na caixa de diálogo exibida, determine se deve selecionar a caixa de seleção **Delete policy plug-in of the cluster**.

- Se você selecioná-la, as políticas de proteção de cluster de container e o plug-in de configuração de política serão excluídos. Se ativar a proteção novamente, você precisará instalar o plug-in de configuração de política e configurar as políticas de proteção novamente.
- Se você desmarcá-la, as políticas de proteção de cluster de container serão excluídas, mas o plug-in de configuração de política será mantido. Se ativar a proteção novamente, você só precisará configurar as políticas de proteção. Se desejar excluir o plug-in de configuração de política mais tarde, repita as etapas anteriores para desativar a proteção e selecione **Delete policy plug-in of the cluster**.

Passo 7 Clique em **OK**.

Se você não tiver selecionado **Delete policy plug-in of the cluster** e o **Protection Status** do cluster mudar para **Enabled but not configured**, isso indicará que a proteção foi desativada.

Se você selecionou **Delete policy plug-in of the cluster** e o **Protection Status** do cluster for alterado para **Unprotected**, isso indicará que a proteção foi desativada.

----Fim

Pergunta frequente

Se a rede do cluster estiver anormal ou o plug-in estiver funcionando, você provavelmente não conseguirá desinstalar o plug-in no console do HSS. Nesse caso, você pode desinstalar manualmente o plug-in consultando **O que devo fazer se o plug-in de proteção de cluster de containers não for desinstalado?**

6 Detecção de intrusão

6.1 Alarmes

6.1.1 Alarmes do HSS

6.1.1.1 Alarmes do servidor

O HSS gera alarmes em uma variedade de eventos de intrusão, incluindo ataques de força bruta, comportamentos anormais de processos, web shells, logons anormais e processos maliciosos. Você pode aprender todos esses eventos no console e eliminar os riscos de segurança em seus ativos em tempo hábil.

NOTA

Os alarmes gerados pela detecção AV e detecção HIPS são exibidos em diferentes tipos de eventos.

- Os alarmes gerados pela detecção AV são exibidos apenas sob os eventos **Malware**.
- Os alarmes gerados pela detecção HIPS são exibidos em subcategorias de todos os eventos.

Restrições

Os servidores que não estão protegidos pelo HSS não suportam operações relacionadas com alarmes.

Alarmes e eventos suportados

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
Malware	Unclassified malware	Os programas maliciosos incluem cavalos de Troia e web shells implementados por hackers para roubar seus dados ou controlar seus servidores. Por exemplo, hackers provavelmente usarão seus servidores como mineiros ou zumbis DDoS. Isso ocupa um grande número de recursos de CPU e rede, afetando a estabilidade do serviço. Verificar malware, como web shells, cavalos de Troia, software de mineração, worms e outros vírus e variantes, e elimine-os com um clique. O malware é encontrado e removido pela análise das características e comportamentos do programa, algoritmos de impressão digital de imagem de IA e verificação e eliminação na nuvem.	×	√	√	√	√	Linux e Windows	√	√
	Viruses	Detectar vírus em ativos do servidor, informar alarmes e suportar ao isolamento e eliminação automáticos ou manuais de vírus com base nos alarmes.	×	√	√	√	√	Linux e Windows	√	√

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
	Worms	Detectar e eliminar worms em servidores e relatar alarmes.	×	√	√	√	√	Linux e Windows	√	√
	Trojans	Detectar e remover cavalos de Troia e vírus em servidores e informar alarmes.	×	√	√	√	√	Linux e Windows	√	√
	Botnets	Detectar e eliminar botnets em servidores e relatar alarmes.	×	√	√	√	√	Linux e Windows	√	√
	Backdoors	Detectar backdoors em servidores e relatar alarmes.	×	√	√	√	√	Linux e Windows	√	√
	Rootkits	Detectar ativos do servidor e relatar alarmes para módulos, arquivos e pastas do kernel suspeitos.	×	√	√	√	√	Linux	√	×

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
	Ransomware	Verificar se há ransomware em páginas da Web, software, e-mails e mídia de armazenamento. O ransomware pode criptografar e controlar seus ativos de dados, como documentos, e-mails, bancos de dados, código-fonte, imagens e arquivos compactados, para aproveitar a extorsão da vítima.	×	×	×	√	√	Linux e Windows	√	√ (Parcialmente suportado)
	Hacker tools	Detectar e eliminar ferramentas de hackers em servidores e relatar alarmes.	×	×	√	√	√	Linux e Windows	√	√

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
	Web shells	Verificar se os arquivos (frequentemente arquivos PHP e JSP) detectados pelo HSS em seus diretórios da Web são web shells. Você pode configurar a regra de detecção de web shell na regra de **Web Shell Detection** na página **Policies**. O HSS verificará se há comandos suspeitos ou executados remotamente. Você precisa adicionar um diretório protegido no gerenciamento de políticas. Para mais detalhes, consulte **Detecção de web shell**.	×	√	√	√	√	Linux e Windows	√	×
	Mining	Detectar, verificar e remover software de mineração em servidores e informar alarmes.	×	√	√	√	√	Linux e Windows	√	√

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
Exploração de vulnerabilidades	Remote code execution	Detectar e relatar alarmes sobre invasões de servidores que exploram vulnerabilidades em tempo real.	×	×	√	√	√	Linux e Windows	√	×
	Explosões de vulnerabilidade do Redis	Detectar as modificações feitas pelo processo do Redis nos principais diretórios em tempo real e relatar alarmes.	×	√	√	√	√	Linux	√	×

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
	Hadoop vulnerability exploits	Detectar as modificações feitas pelo processo de Hadoop nos principais diretórios em tempo real e relatar alarmes.	×	√	√	√	√	Linux	√	×
	MySQL vulnerability exploits	Detectar as modificações feitas pelo processo de MySQL nos principais diretórios em tempo real e relatar alarmes.	×	√	√	√	√	Linux	√	×

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
Comportamento anormal do sistema	Reverse shells	Monitorar os comportamentos do processo do usuário em tempo real para relatar alarmes e bloquear shells reversos causados por conexões inválidas. Os shells reversos podem ser detectados para protocolos, incluindo TCP, UDP e ICMP. Você pode configurar a regra de detecção de shell reverso e o bloqueio automático na regra de **Malicious File Detection** na página **Policies**. O HSS verificará se há comandos suspeitos ou executados remotamente. Você também pode configurar o bloqueio automático de shells reversos na regra de **HIPS Detection** na página **Policies**.	×	√	√	√	√	Linux	√	×
	File privilege escalations	Detectar comportamentos de escalonamento de privilégios de arquivos e gerar alarmes.	×	√	√	√	√	Linux	√	×

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
	Process privilege escalations	Detectar as operações de escalonamento de privilégios dos seguintes processos e gerar alarmes: ● Escalonamento de privilégios da raiz por meio da exploração de vulnerabilidades do programa SUID ● Escalonamento de privilégios da raiz por meio da exploração de vulnerabilidades do kernel	×	√	√	√	√	Linux	√	×
	Important file changes	Monitorar arquivos importantes do sistema (como ls, ps, login e top) em tempo real e gerar alarmes se esses arquivos forem modificados. Para obter detalhes sobre os caminhos monitorados, consulte **Caminhos de arquivos importantes monitorados**. O HSS reporta todas as alterações em arquivos importantes, independentemente de as alterações serem realizadas manualmente ou por processos.	×	√	√	√	√	Linux	√	×

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
	File/Directory changes	Monitorar arquivos e diretórios do sistema em tempo real e gerar alarmes se esses arquivos forem criados, excluídos, movidos ou se seus atributos ou conteúdo forem modificados.	×	√	√	√	√	Linux e Windows	√	×
	Abnormal process behavior	Verificar os processos em servidores, incluindo seus IDs, linhas de comando, caminhos de processo e comportamento. Enviar alarmes sobre operações de processo não autorizadas e intrusões. O seguinte comportamento anormal do processo pode ser detectado: ● Uso anormal da CPU ● Processos que acessam endereços IP maliciosos ● Aumento anormal nas conexões de processos simultâneos	×	×	√	√	√	Linux e Windows	√	x (parcialmente suportado)

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
	High-risk command executions	Você pode configurar quais comandos acionarão alarmes na regra de **High-risk Command Scan** na página **Policies**. O HSS verifica os comandos executados em tempo real e gera alarmes se forem detectados os comandos de alto risco.	×	√	√	√	√	Linux e Windows	√	×
	Abnormal shells	Detectar ações em shells anormais, incluindo mover, copiar e excluir arquivos de shell e modificar as permissões de acesso e links físicos dos arquivos. Você pode configurar a regra de detecção de shell anormal na regra de **Malicious File Detection** na página **Policies**. O HSS verificará se há comandos suspeitos ou executados remotamente.	×	√	√	√	√	Linux	√	×

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
	Suspicious crontab tasks	Verificar e listar serviços iniciados automaticamente, tarefas agendadas, bibliotecas dinâmicas pré-carregadas, chaves de registro de execução e pastas de inicialização. Você pode ser notificado imediatamente quando itens anormais de inicialização automática forem detectados e localizar rapidamente os cavalos de Troia.	×	×	×	√	√	Linux e Windows	√	×
	System protection disabling	Detectar os preparativos para a criptografia de ransomware: desativar a função de proteção em tempo real do Windows Defender por meio do registro. Uma vez que a função é desativada, um alarme é relatado imediatamente.	×	×	√	√	√	Windows	√	×

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
	Backup deletion	Excluir os preparativos para a criptografia de ransomware: excluir arquivos de backup ou arquivos na pasta **Backup**. Uma vez que a exclusão de backup é detectada, um alarme é relatado imediatamente.	×	×	√	√	√	Windows	√	×
	Suspicious registry operations	Detectar operações como desativar o firewall do sistema por meio de registro e usar o ransomware **Stop** para modificar o registro e gravar cadeias específicas no registro. Um alarme é relatado imediatamente quando essas operações são detectadas.	×	×	√	√	√	Windows	√	×

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
	System log deletions	Um alarme é gerado quando um comando ou ferramenta é usado para limpar os registros do sistema.	×	×	√	√	√	Windows	√	×
	Suspicious command executions	● Verificar se uma tarefa agendada ou uma tarefa de inicialização automatizada é criada ou excluída executando comandos ou ferramentas. ● Detectar execução de comandos remotos suspeitos.	×	×	√	√	√	Windows	√	×

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
	Suspicious process execution	Detectar e relatar alarmes em processos de aplicações não autenticados ou não autorizados.	×	×	√	√	√	Linux e Windows	√	×
	Suspicious process file access	Detectar e relatar alarmes nos processos de aplicações não autenticados ou não autorizados que acessam diretórios específicos.	×	×	√	√	√	Linux e Windows	√	×

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
Comportamento anormal do usuário	Brute-force attacks	Se hackers fizerem logon em seus servidores por meio de ataques de força bruta, eles podem obter as permissões de controle dos servidores e realizar operações maliciosas, como roubar dados do usuário; implementar ransomware, mineradores ou cavalos de Troia; criptografar dados; ou usar seus servidores como zumbis para realizar ataques DDoS. Detectar ataques de força bruta em contas SSH, RDP, FTP, SQL Server e MySQL. ● Se o número de ataques de força bruta (tentativas consecutivas de senha incorreta) de um endereço IP atingir 5 em 30 segundos, o endereço IP será bloqueado. Por padrão, os invasores SSH suspeitos são bloqueados por 12 horas. Outros tipos de invasores suspeitos são bloqueados por 24 horas. ● Você pode verificar se o endereço IP é confiável com base no seu tipo de ataque e quantas vezes ele foi bloqueado. Você pode desbloquear manualmente os endereços IP confiáveis.	√	√	√	√	√	Linux e Windows	√	×

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
	Abnormal logins	Detectar comportamento anormal de logon, como logon remoto e ataques de força bruta. Se logons anormais forem relatados, seus servidores podem ter sido invadidos por hackers. ● Verificar e lidar com logons remotos. Você pode verificar os endereços IP de logon bloqueados e quem os usou para fazer logon em qual servidor e a que horas. Se a localização de logon de um usuário não for qualquer localização de logon comum que você definiu, um alarme será acionado. ● Acionar um alarme se um usuário efetuar logon no host por meio de um ataque de força bruta.	√	√	√	√	√	Linux e Windows	√	×
	Invalid accounts	Hackers provavelmente podem quebrar contas inseguras em seus servidores e controlar os servidores. O HSS verifica contas ocultas suspeitas e contas clonadas e gera alarmes sobre elas.	×	√	√	√	√	Linux e Windows	√	×

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
	User account added	Detectar os comandos usados para criar contas ocultas. As contas ocultas não podem ser encontradas na interface de interação com o usuário nem ser consultadas por comandos.	×	×	√	√	√	Windows	√	×
	Password theft	Detectar a obtenção anormal de contas de sistema e hashes de senha em servidores e relatar alarmes.	×	×	√	√	√	Windows	√	×

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
Acesso anormal à rede	Abnormal outbound connection	Relatar alarmes sobre endereços IP suspeitos que iniciam conexões de saída.	×	√	√	√	√	Linux	√	×
	Port forwarding	Relatar alarmes sobre o encaminhamento de porta realizado usando ferramentas suspeitas.	×	√	√	√	√	Linux	√	×

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
	Suspicious download requests	Um alarme é gerado quando uma solicitação HTTP suspeita que usa ferramentas do sistema para baixar programas é detectada.	×	×	√	√	√	Windows	√	×
	Suspicious HTTP requests	Um alarme é gerado quando uma solicitação HTTP suspeita que usa uma ferramenta ou processo do sistema para executar um script de hospedagem remota é detectada.	×	×	√	√	√	Windows	√	×

Tipo de evento	Nome do alarme	Descrição	Edição básica	Edição profissional	Edição empresarial	Edição premium	Edição WTP	SO suportado	Adicionar à lista branca de alarmes	Isolar e eliminar
Reconhecimento	Port scan	Detectar verificação ou sniffing em portas especificadas e relatar alarmes.	×	×	×	√	√	Linux	×	×
	Host scan	Detectar as atividades de verificação de rede com base nas regras do servidor (incluindo ICMP, ARP e nbtscan) e informar alarmes.	×	×	×	√	√	Linux	√	×

Caminhos de arquivos importantes monitorados

Tipo	Linux
bin	/bin/ls /bin/ps /bin/bash /bin/login

Tipo	Linux
usr	/usr/bin/ls /usr/bin/ps /usr/bin/bash /usr/bin/login /usr/bin/passwd /usr/bin/top /usr/bin/killall /usr/bin/ssh /usr/bin/wget /usr/bin/curl

6.1.1.2 Visualização de alarmes de intrusão

O HSS exibe estatísticas de alarmes e eventos e seu resumo em uma única página. Você pode ter uma visão geral rápida dos alarmes, incluindo o número de alarmes urgentes, alarmes totais, servidores com alarmes, endereços IP bloqueados e arquivos isolados.

A página **Events** exibe os eventos de alarmes gerados nos últimos 30 dias. Você pode lidar manualmente com os itens alarmados.

O status de um evento manipulado muda de **Unhandled** para **Handled**.

NOTA

Os alarmes gerados pela detecção AV e detecção HIPS são exibidos em diferentes tipos de eventos.

- Os alarmes gerados pela detecção AV são exibidos apenas sob os eventos **Malware**.
- Os alarmes gerados pela detecção HIPS são exibidos em subcategorias de todos os eventos.

Restrições e limitações

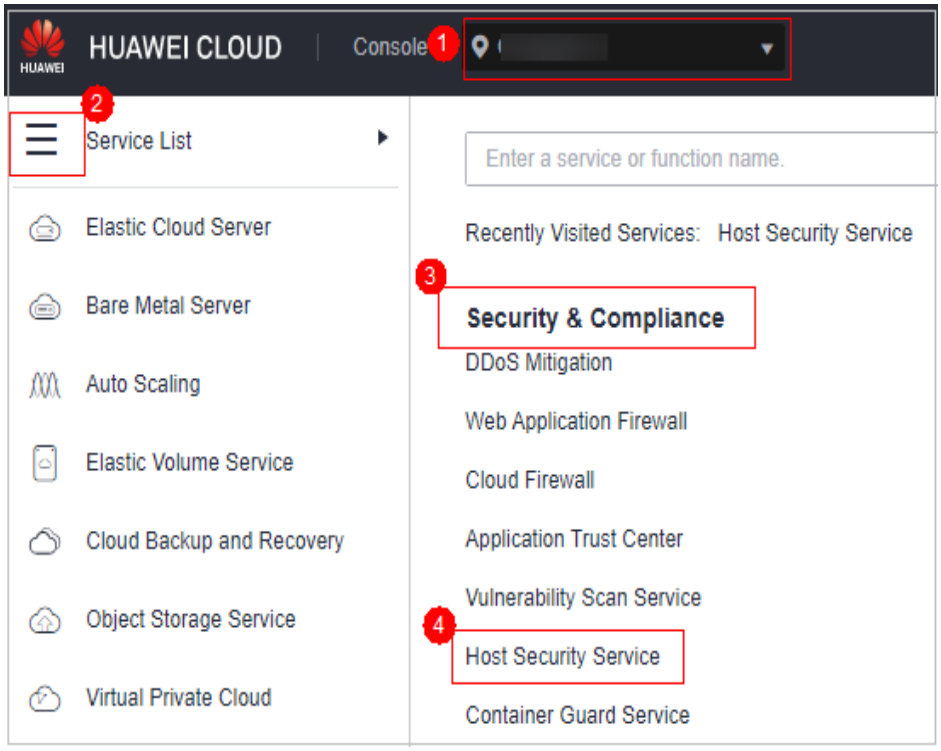
- Para ignorar as verificações de execução de comandos de alto risco, escalonamento de privilégios, shells reversos, shells anormais ou web shells, desative manualmente as políticas correspondentes nos grupos de políticas na página **Policies**. O HSS não verificará os servidores vinculados às políticas desativadas. Para obter detalhes, consulte **Visualização de um grupo de políticas**.
- Outros itens de detecção não podem ser desativados manualmente.
- Os servidores que não estão protegidos pelo HSS não suportam operações relacionadas a alarmes e eventos.

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 6-1 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Detection** > **Alarms** e clique em **Server Alarms**.

NOTA

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

Tabela 6-1 Estatísticas de alarme

Parâmetro	Descrição
Enterprise Project	Selecione um projeto empresarial e visualize os detalhes do alarme por projeto empresarial.
Time range	Você pode selecionar um período fixo ou personalizar um intervalo de tempo para procurar alarmes. Somente alarmes gerados dentro de 30 dias podem ser consultados. As opções são as seguintes: ● Last 24 hours ● Last 3 days ● Last 7 days ● Last 30 days
Urgent Alarms	Número de alarmes urgentes que precisam ser manipulados.
Total Alarms	Número total de alarmes em seus ativos.

Parâmetro	Descrição
Affected Servers	Número de servidores para os quais os alarmes são gerados. Ao verificar os alarmes gerados nas últimas 24 horas, você pode clicar no número de servidores para ir para a página **Servers & Quota** e verificar os servidores correspondentes.
Handled Alarms	Número de alarmes manipulados.
Blocked IP Addresses	Número de endereços IP bloqueados. Você pode clicar no número para verificar a lista de endereços IP bloqueados. A lista de endereços IP bloqueados exibe o nome do servidor, o endereço IP da origem do ataque, o tipo de logon, o status do bloqueio, o número de blocos, a hora de início do bloqueio e a hora de bloqueio mais recente. Se um endereço IP válido for bloqueado por engano (por exemplo, após a equipe de O&M inserir senhas incorretas várias vezes), você poderá desbloqueá-lo manualmente. Se um servidor é frequentemente atacado, é aconselhável corrigir suas vulnerabilidades em tempo hábil e eliminar os riscos. **AVISO** ● Depois que um endereço IP bloqueado for desbloqueado, o HSS não bloqueará mais as operações realizadas pelo endereço IP. ● Um máximo de 10.000 endereços IP podem ser bloqueados para cada tipo de software. Se o seu servidor do Linux não suportar ipset, um máximo de 50 endereços IP podem ser bloqueados para MySQL e vsftp. Se o seu servidor do Linux não suporta ipset ou hosts.deny, um máximo de 50 endereços IP podem ser bloqueados para SSH.
Isolated Files	O HSS pode isolar arquivos de ameaças detectados. Os arquivos que foram isolados são exibidos em um painel deslizante na página **Server Alarms**. Você pode clicar em **Isolated Files** no canto superior direito para verificá-los. Você pode recuperar arquivos isolados. Para mais detalhes, consulte **Gerenciamento de arquivos isolados**.

Passo 4 Verifique os alarmes em seus ativos.

Na área **Alarms to Be Handled**, pode selecionar um tipo de alarme e uma fase ATT&CK para ver os alarmes do tipo selecionado.

As tags de fase de ataque ATT&CK também são exibidas abaixo dos nomes dos alarmes. Para obter mais informações, consulte **Tabela 6-2**.

NOTA

Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) é uma estrutura que ajuda as organizações a entender as táticas e técnicas de adversários cibernéticos usadas pelos agentes de ameaças em todo o ciclo de vida do ataque.

Tabela 6-2 Fases ATT&CK

Fase ATT&CK	Descrição
Reconnaissance	Os atacantes buscam vulnerabilidades em seu sistema ou rede.
Initial Access	O atacante tenta entrar em seu sistema ou rede.
Execution	Os atacantes tentam executar código malicioso.
Persistence	Os atacantes tentam manter sua posição.
Privilege Escalation	Os atacantes tentam obter permissões mais altas.
Defense Evasion	Os atacantes tentam evitar serem detectados.
Credential Access	Os atacantes tentam roubar nomes e senhas de contas.
Command and Control	Os atacantes tentam se comunicar com máquinas comprometidas para controlá-las.
Impact	Os atacantes tentam manipular, interromper ou destruir seu sistema ou dados.

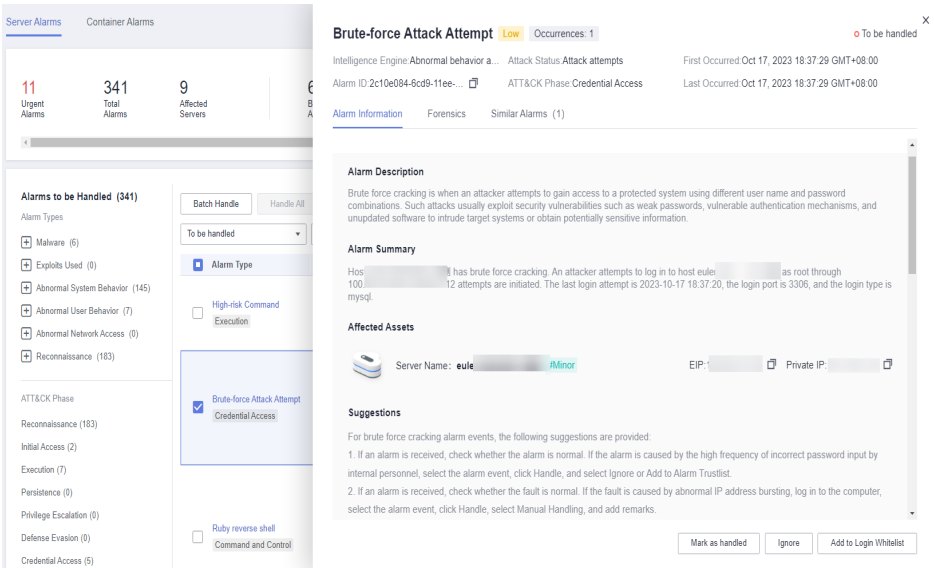
Passo 5 Clique em um nome de alarme para visualizar seus detalhes.

Você pode visualizar as descrições dos alarmes, sugestões, caminhos e endereços de alarmes na análise forense do HSS e o histórico de tratamento de alarmes semelhantes.

NOTA

Você pode baixar os arquivos de origem de alarme de determinado malware para o seu PC local para análise. A senha para descompactar os arquivos é **unlock**.

Figura 6-2 Detalhes de alarme



----Fim

6.1.1.3 Gerenciamento de arquivos isolados

O HSS pode isolar arquivos de ameaças detectados. Os arquivos que foram isolados são exibidos em um painel deslizante na página **Server Alarms**. Você pode clicar em **Isolated Files** no canto superior direito para verificá-los e pode recuperar arquivos isolados a qualquer momento.

Para detalhes sobre eventos que podem ser isolados e eliminados, veja **Alarmes do servidor**.

Restrições

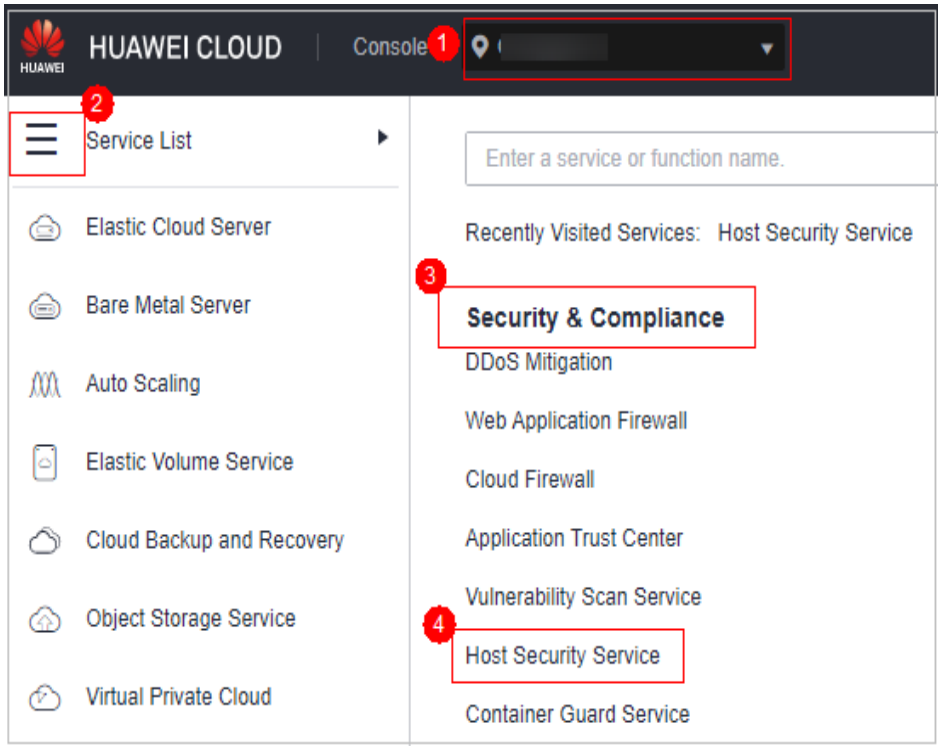
Os servidores que não estão protegidos pelo HSS não suportam operações relacionadas com alarmes.

Operações de isolamento e eliminação

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 6-3 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Detection** > **Alarms** e clique em **Server Alarms**.

NOTA

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

Tabela 6-3 Estatísticas de alarme

Parâmetro	Descrição
Enterprise Project	Selecione um projeto empresarial e visualize os detalhes do alarme por projeto empresarial.
Time range	Você pode selecionar um período fixo ou personalizar um intervalo de tempo para procurar alarmes. Somente alarmes gerados dentro de 30 dias podem ser consultados. As opções são as seguintes: ● Last 24 hours ● Last 3 days ● Last 7 days ● Last 30 days
Urgent Alarms	Número de alarmes urgentes que precisam ser manipulados.
Total Alarms	Número total de alarmes em seus ativos.
Affected Servers	Número de servidores para os quais os alarmes são gerados. Ao verificar os alarmes gerados nas últimas 24 horas, você pode clicar no número de servidores para ir para a página **Servers & Quota** e verificar os servidores correspondentes.
Handled Alarms	Número de alarmes manipulados.
Blocked IP Addresses	Número de endereços IP bloqueados. Você pode clicar no número para verificar a lista de endereços IP bloqueados. A lista de endereços IP bloqueados exibe o nome do servidor, o endereço IP da origem do ataque, o tipo de logon, o status do bloqueio, o número de blocos, a hora de início do bloqueio e a hora de bloqueio mais recente. Se um endereço IP válido for bloqueado por engano (por exemplo, após a equipe de O&M inserir senhas incorretas várias vezes), você poderá desbloqueá-lo manualmente. Se um servidor é frequentemente atacado, é aconselhável corrigir suas vulnerabilidades em tempo hábil e eliminar os riscos. **AVISO** ● Depois que um endereço IP bloqueado for desbloqueado, o HSS não bloqueará mais as operações realizadas pelo endereço IP. ● Um máximo de 10.000 endereços IP podem ser bloqueados para cada tipo de software. Se o seu servidor do Linux não suportar ipset, um máximo de 50 endereços IP podem ser bloqueados para MySQL e vsftp. Se o seu servidor do Linux não suporta ipset ou hosts.deny, um máximo de 50 endereços IP podem ser bloqueados para SSH.

Parâmetro	Descrição
Isolated Files	O HSS pode isolar arquivos de ameaças detectados. Os arquivos que foram isolados são exibidos em um painel deslizante na página **Server Alarms**. Você pode clicar em **Isolated Files** no canto superior direito para verificá-los. Você pode recuperar arquivos isolados. Para mais detalhes, consulte **Gerenciamento de arquivos isolados**.

Passo 4 Localize um evento que possa ser isolado e eliminado, clique em **Handle** na coluna **Operation** e selecione **Isolate and Kill** na caixa exibida.

NOTA

Para detalhes sobre eventos que podem ser isolados e eliminados, veja **Alarmes do servidor**.

Passo 5 Clique em **OK** para isolar e eliminar o evento de alarme de destino.

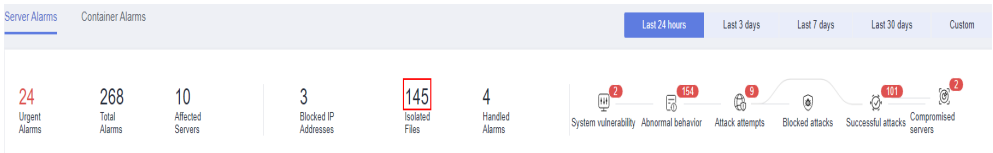
Os arquivos que foram isolados são exibidos em um painel deslizante na página **Server Alarms** e não podem danificar seus servidores. Você pode clicar em **Isolated Files** no canto superior direito para verificá-los.

----Fim

Verificar arquivos isolados

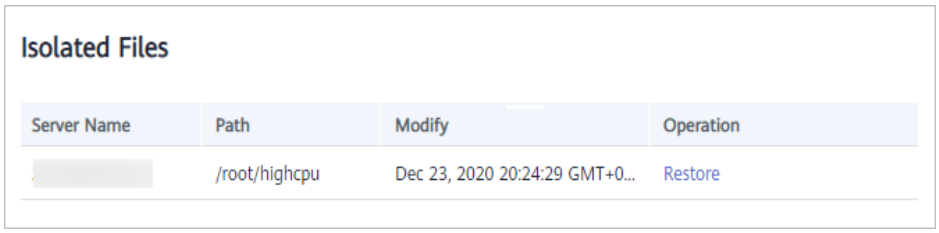
Passo 1 Na área de estatísticas de alarme na página **Server Alarms**, clique no número acima de **Isolated Files** para verificar os arquivos isolados.

Figura 6-4 Estatísticas de alarme



Passo 2 Verifique os servidores, nomes, caminhos e horário de modificação dos arquivos isolados.

Figura 6-5 Verificar arquivos isolados



----Fim

Recuperar arquivos isolados

Passo 1 Clique em **Restore** na coluna **Operation** de um arquivo isolado.

Passo 2 Clique em **OK**.

NOTA

Os arquivos recuperados não serão mais isolados. Tenha cuidado ao realizar esta operação.

----Fim

6.1.1.4 Manipulação de alarmes do servidor

O HSS exibe estatísticas de alarmes e eventos e seu resumo em uma única página. Você pode ter uma visão geral rápida dos alarmes, incluindo o número de alarmes urgentes, alarmes totais, servidores com alarmes, endereços IP bloqueados e arquivos isolados.

A página **Events** exibe os alarmes gerados nos últimos 30 dias.

O status de um alarme manipulado muda de **Unhandled** para **Handled**.

NOTA

Os alarmes gerados pela detecção AV e detecção HIPS são exibidos em diferentes tipos de eventos.

- Os alarmes gerados pela detecção AV são exibidos apenas sob os eventos **Malware**.
- Os alarmes gerados pela detecção HIPS são exibidos em subcategorias de todos os eventos.

Limitações e restrições

- Para ignorar as verificações de execução de comandos de alto risco, escalações de privilégio, shells reversos, shells anormais ou web shells, desative manualmente as políticas correspondentes nos grupos de políticas na página **Policies**. O HSS não verificará os servidores vinculados às políticas desativadas. Para obter detalhes, consulte **Verificação ou criação de um grupo de políticas**.
- Outros itens de detecção não podem ser desativados manualmente.
- Os servidores que não estão protegidos pelo HSS não suportam operações relacionadas a alarmes e eventos.

Procedimento

Esta seção descreve como você deve lidar com alarmes para melhorar a segurança do servidor.

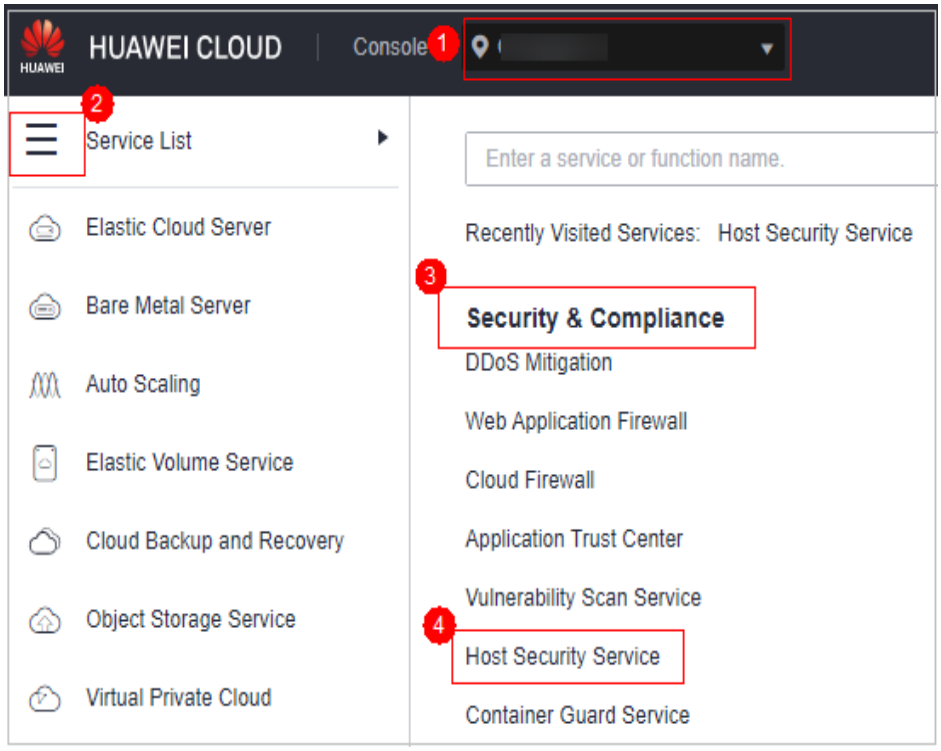
NOTA

Não confie totalmente na manipulação de alarmes para se defender contra ataques, porque nem todos os problemas podem ser detectados em tempo hábil. É aconselhável tomar mais medidas para prevenir ameaças, como verificar e corrigir vulnerabilidades e configurações inseguras.

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 6-6 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Detection** > **Alarms** e clique em **Server Alarms**.

NOTA

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

Tabela 6-4 Estatísticas de alarme

Parâmetro	Descrição
Enterprise Project	Selecione um projeto empresarial e visualize os detalhes do alarme por projeto empresarial.
Time range	Você pode selecionar um período fixo ou personalizar um intervalo de tempo para procurar alarmes. Somente alarmes gerados dentro de 30 dias podem ser consultados. As opções são as seguintes: ● Last 24 hours ● Last 3 days ● Last 7 days ● Last 30 days
Urgent Alarms	Número de alarmes urgentes que precisam ser manipulados.
Total Alarms	Número total de alarmes em seus ativos.

Parâmetro	Descrição
Affected Servers	Número de servidores para os quais os alarmes são gerados. Ao verificar os alarmes gerados nas últimas 24 horas, você pode clicar no número de servidores para ir para a página **Servers & Quota** e verificar os servidores correspondentes.
Handled Alarms	Número de alarmes manipulados.
Blocked IP Addresses	Número de endereços IP bloqueados. Você pode clicar no número para verificar a lista de endereços IP bloqueados. A lista de endereços IP bloqueados exibe o nome do servidor, o endereço IP da origem do ataque, o tipo de logon, o status do bloqueio, o número de blocos, a hora de início do bloqueio e a hora de bloqueio mais recente. Se um endereço IP válido for bloqueado por engano (por exemplo, após a equipe de O&M inserir senhas incorretas várias vezes), você poderá desbloqueá-lo manualmente. Se um servidor é frequentemente atacado, é aconselhável corrigir suas vulnerabilidades em tempo hábil e eliminar os riscos. **AVISO** ● Depois que um endereço IP bloqueado for desbloqueado, o HSS não bloqueará mais as operações realizadas pelo endereço IP. ● Um máximo de 10.000 endereços IP podem ser bloqueados para cada tipo de software. Se o seu servidor do Linux não suportar ipset, um máximo de 50 endereços IP podem ser bloqueados para MySQL e vsftp. Se o seu servidor do Linux não suporta ipset ou hosts.deny, um máximo de 50 endereços IP podem ser bloqueados para SSH.
Isolated Files	O HSS pode isolar arquivos de ameaças detectados. Os arquivos que foram isolados são exibidos em um painel deslizante na página **Server Alarms**. Você pode clicar em **Isolated Files** no canto superior direito para verificá-los. Você pode recuperar arquivos isolados. Para mais detalhes, consulte **Gerenciamento de arquivos isolados**.

Passo 4 Clique no nome de um alarme para ver os detalhes e sugestões do alarme.

Passo 5 Lide com os alarmes.

NOTA

Os alarmes são exibidos na página **Server Alarms**. Aqui você pode verificar até 30 dias de alarmes históricos.

Verifique e lide com alarmes conforme necessário. O status de um alarme manipulado muda de **Unhandled** para **Handled**. O HSS não coletará mais suas estatísticas nem as exibirá na página **Dashboard**.

- Manipulação de um único alarme

  Na coluna **Operation** de um alarme, clique em **Handle**.
- Manipulação de alarmes em lotes

  Selecione todos os alarmes e clique em **Batch Handle** acima da lista de alarmes.

- Manipulação de todos os alarmes

  Na área **Alarms to be Handled** no painel esquerdo da lista de alarmes, selecione um tipo de alarmes e clique em **Handle All** acima da lista de alarmes.

  Figura 6-7 Manipulação de todos os alarmes

Passo 6 Na caixa de diálogo **Handle Event**, selecione uma ação. Para obter detalhes sobre as ações de manipulação de alarmes, consulte **Tabela 6-5**.

Ao manipular um único evento de alarme ou manipular alarmes em lotes, é possível selecionar **Handle duplicate alarms in batches** na caixa de diálogo **Handle Event**.

Tabela 6-5 Métodos de manipulação de alarmes

Ação	Descrição
Ignore	Ignorar o alarme atual. Quaisquer novos alarmes do mesmo tipo ainda serão relatados pelo HSS.
Isolate and kill	Se um programa for isolado e eliminado, ele será encerrado imediatamente e não poderá mais 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. Você pode clicar em **Isolated Files** no canto superior direito para verificar os arquivos. Para mais detalhes, consulte **Gerenciamento de arquivos isolados**. Para detalhes sobre eventos que podem ser isolados e eliminados, veja **Alarmes do servidor**. **NOTA** Quando um programa é isolado e eliminado, o processo do programa é encerrado imediatamente. Para evitar impacto nos serviços, verifique o resultado da detecção e cancele o isolamento ou deixe de ignorar programas maliciosos reportados incorretamente (se houver).
Mark as handled	Marcar o evento como manipulado. É possível adicionar observações ao evento para registrar mais detalhes.
Add to process whitelist	Se você puder confirmar que um processo que aciona um alarme pode ser confiável, você pode adicioná-lo à lista branca do processo. O HSS não reportará mais alarmes sobre processos na lista branca.
Add to login whitelist	Adicionar itens com alarme falso dos tipos **Brute-force attack** e **Abnormal login** à lista branca de logon. O HSS não reportará mais alarmes sobre os itens da lista branca. Um evento de logon na lista branca não acionará alarmes. Os seguintes alarmes podem ser adicionados à lista branca de logon: ● Ataques de força bruta ● Logons anormais

Ação	Descrição
Add to alarm whitelist	Adicionar itens com alarme falso dos seguintes tipos à lista branca de alarmes. O HSS não reportará mais alarmes sobre os itens da lista branca. Um alarme na lista branca não acionará alarmes. Você pode clicar em **Add Rule** e configurar caminhos de arquivo, caminhos de processo ou linhas de comando de processo em regras de mascaramento de alarme. O HSS não relatará os alarmes correspondentes a essas regras. Para detalhes sobre eventos que podem ser isolados e eliminados, veja **Alarmes do servidor**.

Passo 7 Clique em **OK**.

Verifique os alarmes manipulados. Para mais detalhes, consulte **Visualização do histórico de tratamento**.

----Fim

6.1.1.5 Exportação de alarmes do servidor

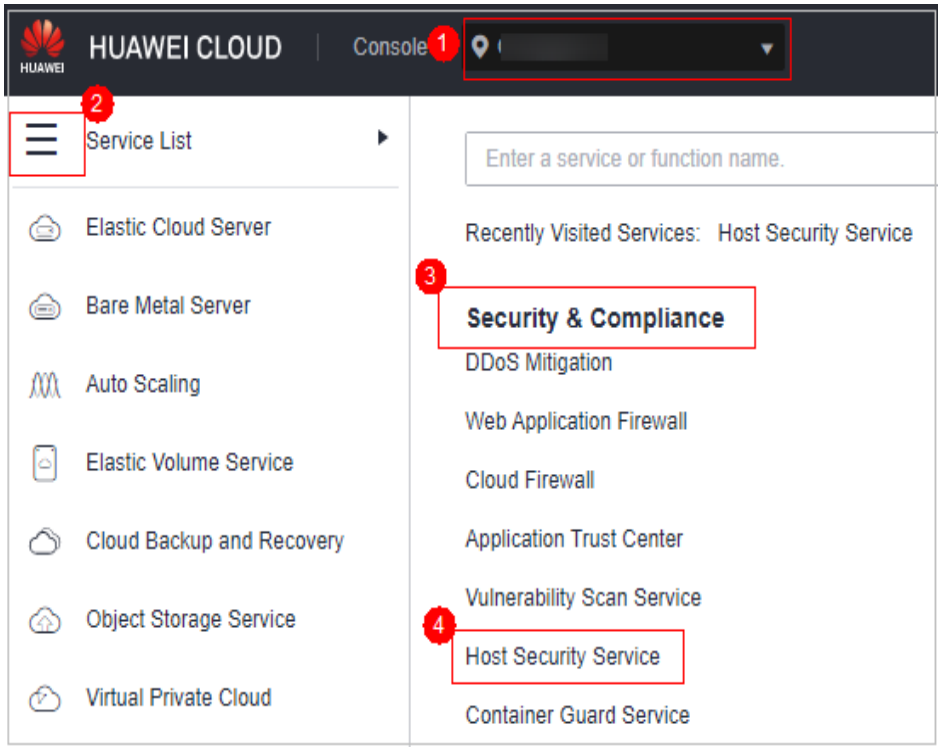
Você pode exportar alarmes e eventos do servidor para um PC local.

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 6-8 Acessar o HSS



Passo 3 No painel de navegação, escolha **Detection** > **Alarms**.

NOTA

Se os servidores forem gerenciados por projetos empresariais, você poderá selecionar o projeto empresarial de destino para visualizar ou operar as informações sobre ativos e detecção.

Passo 4 Clique na guia **Server Alarms**.

Passo 5 Clique em **Export** acima da lista de alarmes para exportar todos os eventos de segurança.

Para exportar os alarmes de um certo tipo ou fase de ataque ATT&CK, selecione o tipo ou fase na área **Alarms to Be Handled** e clique em **Export**.

----Fim

6.1.2 Alarmes de containers

6.1.2.1 Eventos de alarme de container

Depois que a proteção de nó é ativada, um agente é implementado em cada host de container para monitorar o status de execução dos containers em tempo real. Os agentes oferecem suporte à detecção de escape, chamadas de sistema de alto risco, processos anormais, arquivos anormais e detecção de ambiente de container. Você pode aprender os eventos de alarme de forma abrangente na página **Container Alarms** e excluir os riscos de segurança em seus ativos em tempo hábil.

Restrições

- Somente a edição de container do HSS suporta a função de alarme de segurança do container. Para obter detalhes sobre como comprar e atualizar o HSS, consulte **Compra de uma cota de HSS** e **Atualização de sua edição**.
- A função de alarme de segurança de container suporta detecção de intrusão e relatórios de alarme para os seguintes componentes de tempo de execução de container do Linux:
  - Containerd
  - Docker

Tipos de alarmes de containers

Tipo de evento	Nome do alarme	Mecanismo
Malware	Malware não classificado	Verificar malware, como web shells, cavalos de Troia, software de mineração, worms e outros vírus e variantes. O malware é encontrado e removido pela análise das características e comportamentos do programa, algoritmos de impressão digital de imagem de IA e verificação e eliminação na nuvem.
	Ransomware	Verificar se há ransomware em páginas da Web, software, e-mails e mídia de armazenamento. O ransomware pode criptografar e controlar seus ativos de dados, como documentos, e-mails, bancos de dados, código-fonte, imagens e arquivos compactados, para aproveitar a extorsão da vítima.
	Web shells	Verificar se os arquivos (frequentemente arquivos PHP e JSP) nos diretórios da Web em containers são web shells.
	Ferramentas de hackers	Relatar alarmes sobre os comportamentos maliciosos que exploram vulnerabilidades ou são realizados usando ferramentas de hackers.
Explorações de vulnerabilidades	Escapes de vulnerabilidade	O HSS relata um alarme se detectar o comportamento do processo de container que corresponda ao comportamento de vulnerabilidades conhecidas (como Dirty COW, ataque de força bruta, runC e shocker).
	Escapes de arquivo	O HSS relata um alarme se detectar que um processo de container acessa um diretório de arquivos de chave (por exemplo, **/etc/shadow** ou **/etc/crontab**). Diretórios que atendem às regras de mapeamento de diretório de container também podem acionar esses alarmes.

Tipo de evento	Nome do alarme	Mecanismo
Comportamentos anormais do sistema	Shells reversos	Monitorar os comportamentos do processo do usuário em tempo real para relatar alarmes e bloquear shells reversos causados por conexões inválidas. Os shells reversos podem ser detectados para protocolos, incluindo TCP, UDP e ICMP. Você pode configurar a regra de detecção de shell reverso e o bloqueio automático na regra de **Malicious File Detection** na página **Policies**. O HSS verificará se há comandos suspeitos ou executados remotamente. Você também pode configurar o bloqueio automático de shells reversos na regra de **HIPS Detection** na página **Policies**.
	Escalonamentos de privilégio de arquivo	Relatar alarmes sobre escalações de privilégios raiz que exploram vulnerabilidades de programas SUID e SGID.
	Escalonamentos de privilégio do processo	Depois que os hackers invadirem os containers, eles tentarão explorar as vulnerabilidades para conceder a si mesmos as permissões raiz ou adicionar permissões para arquivos. Dessa forma, eles podem criar contas do sistema ilegalmente, modificar permissões de conta e adulterar arquivos. O HSS pode detectar as seguintes operações de escalonamento de privilégios anormais: ● Escalonamento de privilégio raiz explorando vulnerabilidades do programa SUID ● Escalonamento de privilégios raiz explorando vulnerabilidades do kernel ● Escalonamento de privilégio de arquivo
	Mudanças de arquivo importante	Monitorar arquivos importantes do sistema (como ls, ps, login e top) em tempo real e gerar alarmes se esses arquivos forem modificados. Para obter mais informações, consulte **Caminhos de arquivos importantes monitorados**. O HSS reporta todas as alterações em arquivos importantes, independentemente de as alterações serem realizadas manualmente ou por processos.

Tipo de evento	Nome do alarme	Mecanismo
	Comportamentos anormais do processo	Verificar os processos em servidores, incluindo seus IDs, linhas de comando, caminhos de processo e comportamento. Enviar alarmes sobre operações de processo não autorizadas e intrusões. O seguinte comportamento anormal do processo pode ser detectado: ● Uso anormal da CPU ● Processos que acessam endereços IP maliciosos ● Aumento anormal nas conexões de processos simultâneos
	Chamadas de sistema de alto risco	O CGS relata um alarme se detecta uma chamada de alto risco, como **open_by_handle_at**, **ptrace**, **setns** ou **reboot**.
	Execuções de comando de alto risco	Verificar os comandos executados nos containers e gerar alarmes se os comandos de alto risco forem detectados.
	Processos de container anormal	● Programa de container malicioso O HSS monitora o comportamento do processo do container e processa as impressões digitais do arquivo. Ele informa um alarme se detectar um processo cujas características de comportamento correspondam às de um programa malicioso predefinido. ● Processos anormais Se tiver a certeza de que apenas processos específicos são executados em um container, pode colocar na lista branca os processos na página **Policy Groups** e vincular a política ao container. O HSS relata um alarme se detectar que um processo que não está na lista branca está sendo executado no container.
	Acesso a arquivos sensíveis	O HSS monitora os arquivos de imagem de container vinculados às políticas de proteção de arquivos e relata um alarme se os arquivos forem modificados.

Tipo de evento	Nome do alarme	Mecanismo
	Inicializações anormais de containers	O HSS monitora as inicializações de container e relata um alarme se detectar que um container com muitas permissões foi iniciado. Este alarme não indica um ataque real. Os ataques que exploram esse risco acionarão outros alarmes de containers do HSS. Os itens de verificação do container do HSS incluem: ● Inicialização de container privilegiada (**privileged:true**) Os alarmes são acionados pelos containers iniciados com as permissões máximas. As configurações que podem acionar tais alarmes incluem o parâmetro **–privileged=true** no comando **docker run** e **privileged: true** em **securityContext** do container em um pod do Kubernetes. Se o nome do alarme for **Container Security Options** e o conteúdo do alarme contiver **privileged:true**, isso indicará que o container foi iniciado no modo de container privilegiado. ● Muitos recursos de containers (**capability:[xxx]**) Nos SOs de Linux, as permissões do sistema são divididas em grupos antes de serem atribuídas aos containers. Um container tem apenas um número limitado de permissões e o escopo de impacto desse container é limitado no caso de um incidente. No entanto, usuários maliciosos podem conceder todas as permissões do sistema a um container modificando suas configurações de inicialização. Se o nome do alarme for **Container Security Options** e o conteúdo do alarme contiver **capabilities:[xxx]**, isso indicará que o container foi iniciado com um conjunto de capacidades excessivamente grande, o que representa riscos. ● Seccomp não habilitado (**seccomp=unconfined**) O modo de computação segura (seccomp) é um recurso do kernel do Linux. Ele pode restringir as chamadas do sistema invocadas por processos para reduzir a superfície de ataque do kernel. Se **seccomp=unconfined** for configurado quando um container for iniciado, as chamadas do sistema não serão restritas para o container. Se o nome do alarme for **Container Security Options** e o conteúdo do alarme contiver **seccomp=unconfined**, isso indica que o container foi iniciado sem seccomp, o que representa riscos. **NOTA** Se seccomp estiver habilitado, as permissões serão verificadas para cada chamada do sistema. As verificações provavelmente afetarão os serviços se as chamadas do sistema forem frequentes. Antes de decidir se deseja habilitar o seccomp, é aconselhável habilitá-lo e analisar o impacto em seus serviços. ● Escalonamento de privilégios de container (**no-new-privileges:false**)

Tipo de evento	Nome do alarme	Mecanismo
		O CGS relata um alarme se detectar que um processo tenta escalonar permissões executando o comando **sudo** e usando o bit SUID ou SGID. Se **–no-new-privileges=false** for especificado quando um container for iniciado, o container poderá escalar privilégios. Se o nome do alarme for **Container Security Options** e o conteúdo do alarme contiver **no-new-privileges:false**, isso indica que a restrição de escalonamento de privilégio está desabilitada para o container, o que representa riscos. ● Mapeamento de diretório de alto risco (**mounts:[...]**) Para fins de conveniência, quando um container é iniciado em um servidor, os diretórios do servidor podem ser mapeados para o container. Dessa forma, os serviços no container podem ler e gravar recursos diretamente no servidor. No entanto, esse mapeamento incorre em riscos de segurança. Se qualquer diretório crítico no SO do servidor for mapeado para o container, operações incorretas no container provavelmente danificarão o SO do servidor. O HSS reporta um alarme se detectar que um caminho crítico do servidor (**/boot**, **/dev**, **/etc**, **/sys**, **/var/run**) está montado durante a inicialização do container. Se o nome do alarme for **Container Mount Point** e o conteúdo do alarme contiver **mounts: [{"source":"xxx","destination":"yyy"...]**, isso indica que um caminho de arquivo mapeado para o container não é seguro. Nesse caso, verifique se há mapeamentos de diretório arriscados. Você pode configurar os caminhos de montagem que são considerados seguros na política de coleta de informações de container. **NOTA** Alarmes não serão acionados para os arquivos que precisam ser acessados com frequência por containers do Docker, como **/etc/hosts** e **/etc/resolv.conf**. ● Inicialização de containers no namespace de **host** O namespace de um container deve ser isolado do namespace de um servidor. Se um container e um servidor usarem o mesmo namespace, o container poderá acessar e modificar o conteúdo no servidor, o que acarreta riscos de escape do container. Para evitar esses problemas, o HSS verifica o PID do container, a rede e se o namespace do container é **host**. Se o nome do alarme for **Container Namespace** e o conteúdo do alarme contiver **Container PID Namespace Mode**, **Container IPC Namespace Mode** ou **Container Network Namespace Mode**, isso indicará que um container cujo namespace é **host** foi iniciado. Nesse caso, verifique as opções de inicialização do container com base nas

Tipo de evento	Nome do alarme	Mecanismo
		informações de alarme. Se tiver certeza de que o container pode ser confiável, você pode ignorar o alarme.
	Bloqueio de imagem do container	Se um container contiver imagens inseguras especificadas em **Comportamentos suspeitos de imagem**, antes que o container seja iniciado, um alarme será gerado para as imagens inseguras. **NOTA** Você precisa **instalar o plug-in do Docker**.
	Execuções de comandos suspeitos	● Verificar se uma tarefa agendada ou uma tarefa de inicialização automatizada é criada ou excluída executando comandos ou ferramentas. ● Detectar execução de comandos remotos suspeitos.
Comportamentos anormais do usuário	Contas inválidas	Os hackers provavelmente podem quebrar contas inseguras em seus containers e controlar os containers. O HSS verifica se há contas ocultas suspeitas e contas clonadas e gera alarmes sobre elas.
	Ataques de força bruta	Detectar e relatar alarmes para comportamentos de ataque de força bruta, como tentativas de ataque de força bruta e ataques de força bruta bem-sucedidos, em containers. Detectar ataques de força bruta SSH, Web e Enumdb em containers. **NOTA** Atualmente, os ataques de força bruta podem ser detectados apenas no tempo de execução do Docker.
	Roubos de senhas	Relatar alarmes sobre roubo de chave do usuário.
Acesso anormal à rede	Conexões de saída anormais	Relatar alarmes sobre endereços IP suspeitos que iniciam conexões de saída.
	Encaminhamento de porta	Relatar alarmes no encaminhamento de porta usando ferramentas suspeitas.
Comportamentos anormais do cluster	Comportamentos anormais do pod	Detectar operações anormais, como a criação de pods privilegiados, pods estáticos e pods sensíveis em um cluster e operações anormais realizadas em pods existentes e relatar alarmes.
	Enumerações de informações do usuário	Detectar as operações de enumerar as permissões e a lista de operações executáveis dos usuários do cluster e relatar alarmes.

Tipo de evento	Nome do alarme	Mecanismo
	Vinculação de funções de cluster	Detectar operações como vinculação ou criação de uma função de cluster de alto privilégio ou conta de serviço e relatar alarmes.
	Exclusões de eventos do Kubernetes	Detectar a exclusão de eventos do Kubernetes e relatar alarmes.

Caminhos de arquivos importantes monitorados

Tipo	Linux
bin	/bin/ls /bin/ps /bin/bash /bin/login
usr	/usr/bin/ls /usr/bin/ps /usr/bin/bash /usr/bin/login /usr/bin/passwd /usr/bin/top /usr/bin/killall /usr/bin/ssh /usr/bin/wget /usr/bin/curl

6.1.2.2 Visualização de alarmes de container

O HSS exibe estatísticas de alarmes e eventos e seu resumo em uma única página. Você pode ter uma visão geral rápida dos alarmes, incluindo o número de alarmes urgentes, alarmes totais, containers com alarmes e alarmes manipulados.

A página **Events** exibe os eventos de alarme gerados nos últimos 30 dias.

O status de um evento manipulado muda de **Unhandled** para **Handled**.

Restrições

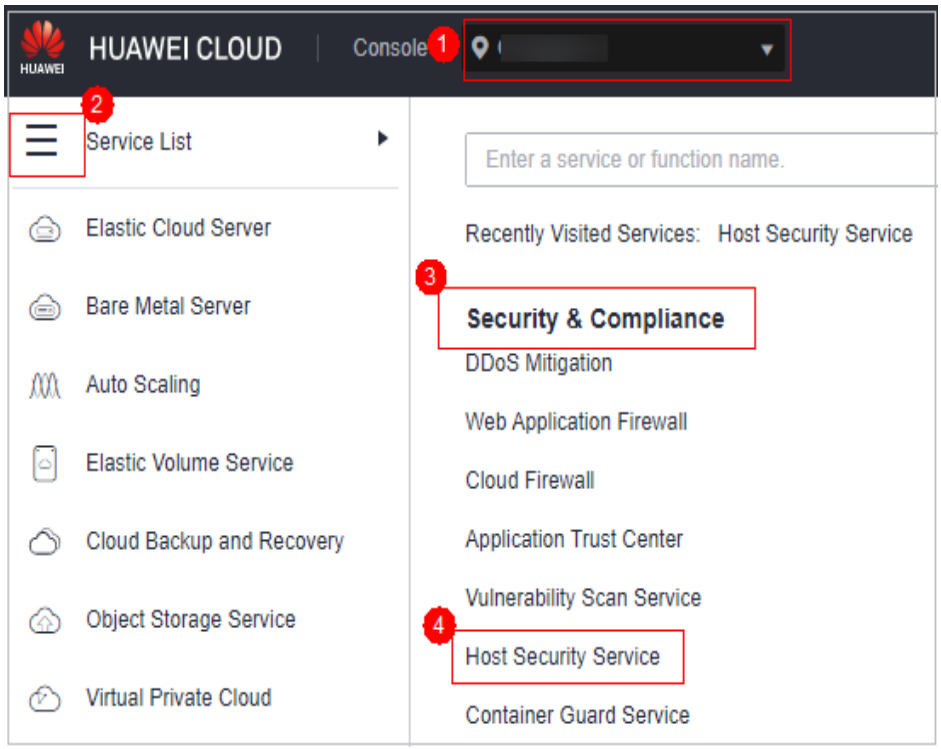
Os servidores que não estão protegidos pelo HSS não suportam operações relacionadas a alarmes e eventos.

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 6-9 Acessar o HSS



Passo 3 No painel de navegação, escolha **Detection** > **Alarms** e clique na guia **Container Alarms** para visualizar os alarmes e eventos do container.

- Visualize a visão geral dos alarmes e eventos do container.
  - **Urgent Alarms**: número de alarmes urgentes que precisam ser manipulados. Você pode clicar no número para ver a lista de alarmes.
  - **Total Alarms**: número total de alarmes relatados em seus ativos. Você pode clicar no número para ver todos os alarmes.
  - **Containers with Alarms**: número de containers com alarmes.
  - **Handled Alarms**: número de alarmes manipulados.
- Visualize os alarmes de um determinado tipo ou fase ATT&CK.

  Na área **Alarms to Be Handled**, selecione um tipo de alarme ou fase att&ck.

  As tags de fase de ataque ATT&CK também são exibidas abaixo dos nomes dos alarmes. Para obter mais informações, consulte **Tabela 6-6**.

  NOTA

  Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) é uma estrutura que ajuda as organizações a entender as táticas e técnicas de adversário cibernético usadas pelos atores de ameaças em todo o ciclo de vida do ataque.

Tabela 6-6 Fases ATT&CK

Fase ATT&CK	Descrição
Reconnaissance	Os atacantes buscam vulnerabilidades em seu sistema ou rede.
Initial Access	Os atacantes tentam entrar em seu sistema ou rede.
Execution	Os atacantes tentam executar código malicioso.
Persistence	Os atacantes tentam manter sua posição.
Privilege Escalation	Os atacantes tentam obter permissões mais altas.
Defense Evasion	Os atacantes tentam evitar serem detectados.
Credential Access	Os atacantes tentam roubar nomes e senhas de contas.
Command and Control	Os atacantes tentam se comunicar com máquinas comprometidas para controlá-las.
Impact	Os atacantes tentam manipular, interromper ou destruir seu sistema ou dados.

- Visualize detalhes sobre alarmes e eventos de container.

  Clique em um nome de alarme para ir para sua página de detalhes. Você pode visualizar a descrição do alarme, a sugestão, o caminho e o endereço do alarme na análise forense do HSS e o histórico de manipulação de alarmes semelhantes.

  NOTA

  Você pode baixar os arquivos de origem de alarme de determinado malware para o seu PC local para análise. A senha para descompactar os arquivos é **unlock**.

- Visualize os detalhes do pod do evento de alarme do container.

  Clique no nome do pod do evento de alarme de destino para visualizar os detalhes do pod, incluindo o endereço IP do nó, namespace, endereço IP do pod, rótulo do pod e lista de containers.

----Fim

6.1.2.3 Manipulação de alarmes de container

O HSS exibe estatísticas de alarme e eventos e seu resumo em uma única página. Você pode ter uma visão geral rápida dos alarmes, incluindo o número de alarmes urgentes, alarmes totais, containers com alarmes e alarmes manipulados.

A página **Events** exibe os alarmes gerados nos últimos 30 dias.

O status de um alarme manipulado muda de **Unhandled** para **Handled**.

Restrições

Os servidores que não estão protegidos pelo HSS não suportam operações relacionadas a alarmes e eventos.

Procedimento

Esta seção descreve como você deve lidar com alarmes para melhorar a segurança do servidor.

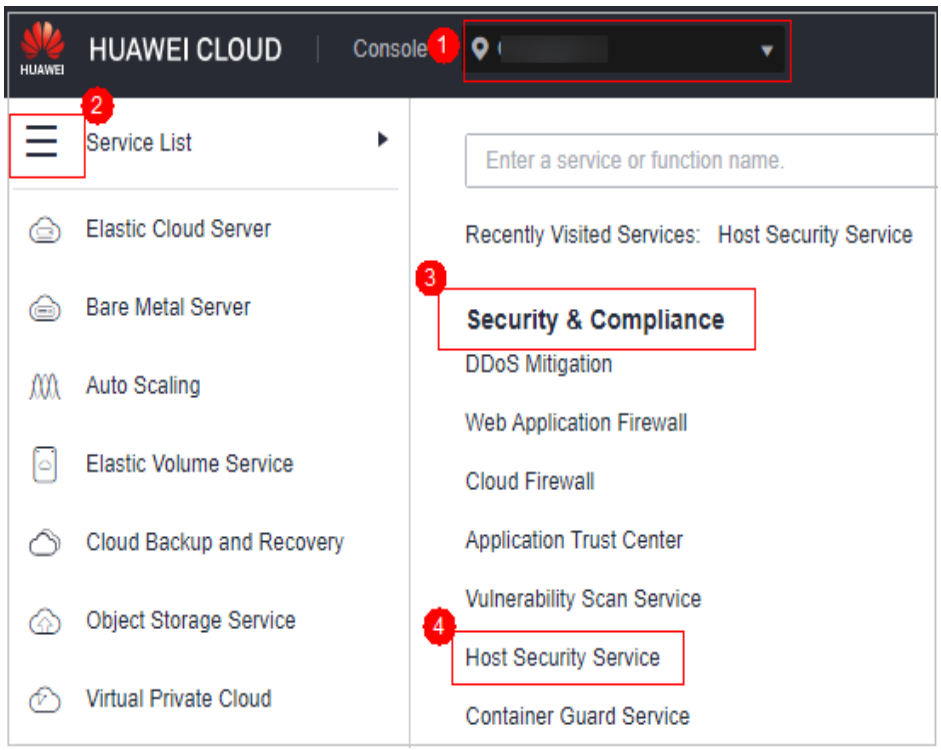
NOTA

Não confie totalmente na manipulação de alarmes para se defender contra ataques, porque nem todos os problemas podem ser detectados em tempo hábil. Recomendamos que você tome mais medidas para evitar ameaças, como verificar e corrigir vulnerabilidades e configurações inseguras.

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 6-10 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Detection** > **Alarms** e clique em **Container Alarms**.

Figura 6-11 Alarmes de container

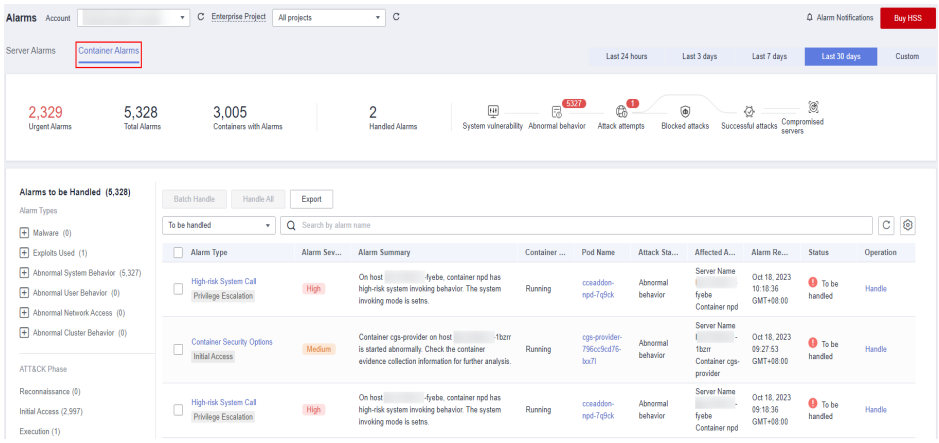


Tabela 6-7 Estatísticas de alarme

Evento de alarme	Descrição
Alarmes urgentes	Número de alarmes urgentes que precisam ser manipulados.
Alarmes totais	Número total de alarmes em seus ativos.
Containers com alarmes	Número de containers para os quais os alarmes são gerados.
Alarmes manipulados	Número de alarmes manipulados.

Passo 4 Clique no nome de um alarme para ver os detalhes e sugestões do alarme.

Passo 5 Manipule os alarmes.

NOTA

Os alarmes são exibidos na página **Container Alarms**. Aqui você pode verificar até 30 dias de alarmes históricos.

Verifique e manuseie alarmes conforme necessário. O status de um alarme manipulado muda de **Unhandled** para **Handled**. O HSS não coletará mais suas estatísticas.

- Manipulação de um único alarme

  Na coluna **Operation** de um alarme, clique em **Handle**.

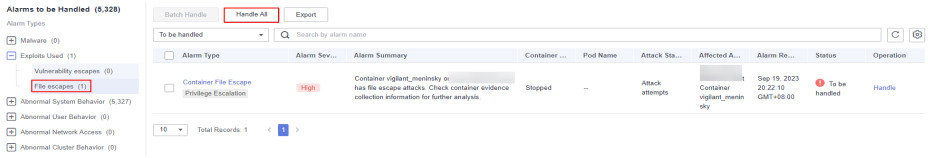
- Manipulação de alarmes em lotes

  Selecione todos os alarmes e clique em **Batch Handle** acima da lista de alarmes.

- Manipulação de todos os alarmes

  Na área **Alarms to be Handled**, no painel esquerdo da lista de alarmes, selecione um tipo de alarme e clique em **Handle All**, acima da lista de alarmes.

Figura 6-12 Manipulação de todos os alarmes



Passo 6 Na caixa de diálogo **Handle Event**, selecione uma ação. Para obter detalhes sobre os modos de processamento, consulte **Tabela 6-8**.

Ao manipular um único evento de alarme ou manipular alarmes em lotes, é possível selecionar **Handle duplicate alarms in batches** na caixa de diálogo **Handle Event**.

Tabela 6-8 Métodos de tratamento de alarmes

Ação	Descrição
Ignorar	Ignorar o alarme atual. Quaisquer novos alarmes do mesmo tipo ainda serão relatados pelo HSS.
Marcar como manipulado	Marcar o evento como manipulado. É possível adicionar observações ao evento para registrar mais detalhes.
Adicionar à lista branca de logon	Adicionar itens de alarmes falsos do **Brute-force attack** e tipos de **Abnormal login** à lista branca de logon. O HSS não relatará mais alarmes sobre os itens da lista branca. Um evento de logon na lista branca não acionará alarmes. Os seguintes alarmes podem ser adicionados à lista branca de logon: ● Ataques de força bruta ● Logons anormais
Adicionar à lista branca do processo	Se você puder confirmar que um processo que aciona um alarme pode ser confiável, você pode adicioná-lo à lista branca do processo.
Adicionar à lista branca do alarme	Adicionar itens com alarme falso à lista branca de logon. O HSS não relatará mais alarmes sobre os itens da lista branca. Um alarme na lista branca não acionará alarmes. Você pode clicar em **Add Rule** e configurar caminhos de arquivo, caminhos de processo ou linhas de comando de processo em regras de mascaramento de alarme. O HSS não relatará os alarmes correspondentes a essas regras. Para detalhes sobre eventos que podem ser isolados e eliminados, veja **Eventos de alarme de container**.

Passo 7 Clique em **OK**.

Verifique os alarmes manuseados. Para obter detalhes, consulte **Registros históricos**.

----Fim

6.1.2.4 Exportação de alarmes de container

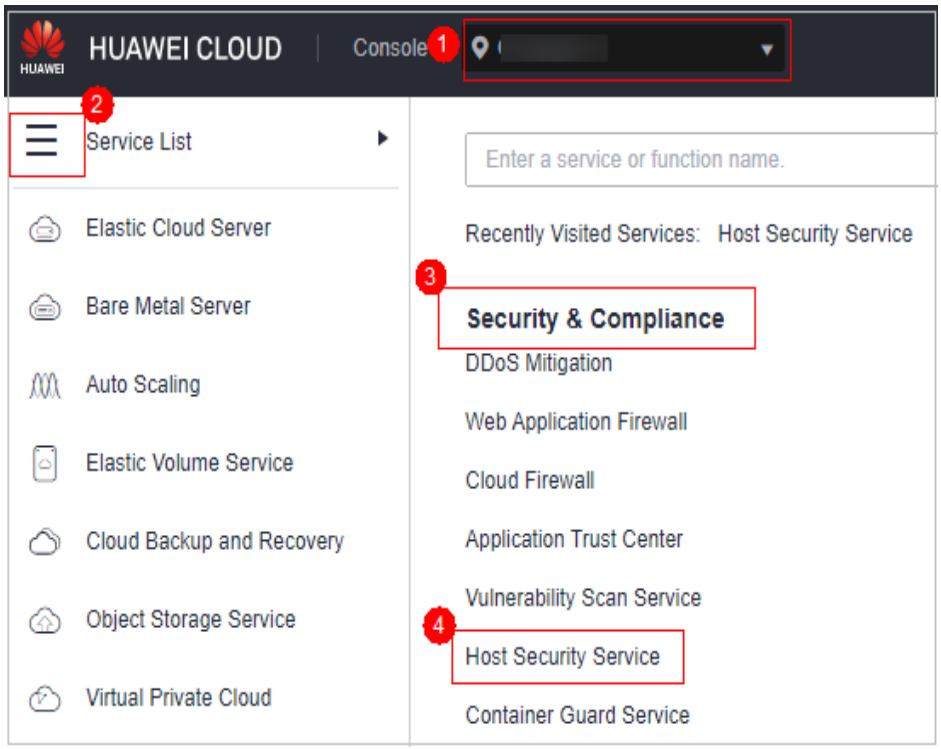
Você pode exportar alarmes e eventos do container para um PC local.

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 6-13 Acessar o HSS



Passo 3 No painel de navegação, escolha **Detection** > **Alarms**.

NOTA

Se os servidores forem gerenciados por projetos empresariais, você poderá selecionar o projeto empresarial de destino para visualizar ou operar as informações sobre ativos e detecção.

Passo 4 Clique na guia **Container Alarms**.

Passo 5 Clique em **Export** acima da lista de alarmes para exportar todos os eventos de segurança.

Para exportar os alarmes de um determinado tipo ou fase de ataque ATT&CK, selecione o tipo ou fase na área **Alarms to Be Handled** e clique em **to export**.

----Fim

6.2 Gerenciamento da lista branca

6.2.1 Configuração da lista branca de logon

Você pode configurar os endereços IP dos servidores de destino, endereços IP de logon, nomes de usuário de logon e comportamentos de usuário na lista branca.

NOTA

- Se o endereço IP do servidor de destino, o endereço IP de logon e o nome de usuário de um logon estiverem todos na lista branca, esse logon será permitido sem verificação.
- Depois que um endereço IP é adicionado a uma lista branca seguindo as instruções em **Adição de informações de logon à lista branca de logon**, os alarmes (se houver) que foram gerados para o endereço IP não serão automaticamente apagados. Manuseie os alarmes referindo-se a **Visualização de alarmes de intrusão**.

Você pode adicionar informações de logon à lista branca de logon das seguintes maneiras:

- Adicione-as à lista branca ao lidar com alarmes falsos dos tipos de **Brute-force attack** e **Abnormal login**. Para mais detalhes, consulte **Visualização de alarmes de intrusão**.
- Adicione-as à lista branca de logon na guia **Login Whitelist**.

Restrições

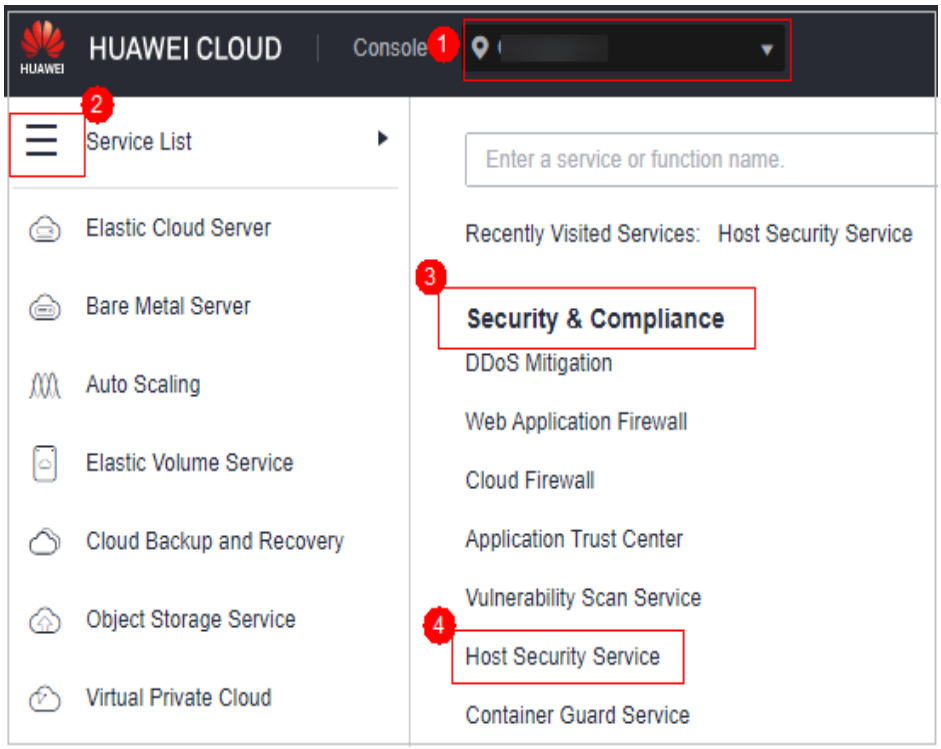
Qualquer uma das edições premium, WTP ou CGS deve estar habilitada.

Adição de informações de logon à lista branca de logon

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 6-14 Acessar o HSS

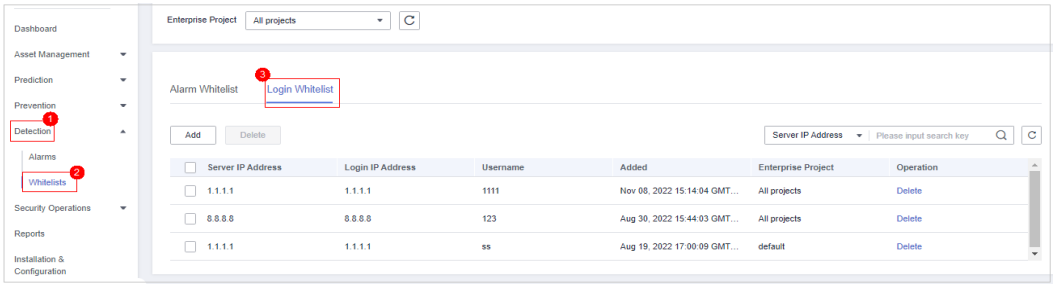


Passo 3 Escolha **Detection** > **Whitelists** > **Login Whitelist** para acessar a página **Whitelists** e clique em **Add**.

NOTA

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

Figura 6-15 Adição de uma lista branca de logon



Passo 4 Na página exibida, insira o endereço IP do servidor, o endereço IP de logon e o nome de usuário de logon.

Tabela 6-9 Parâmetros da lista branca de segurança de logon

Parâmetro	Descrição	Exemplo de valor
Server IP Address	● Endereços IPv4 são suportados ● Endereços IP únicos, segmentos de endereços IP e máscaras são suportados. Use vírgulas (,) para separá-los.	● 192.168.1.1 ● 192.168.2.1-192.168.6.1 ● 192.168.7.0/24
Login IP Address		
Login Username	Nome de usuário de logon atual	hss_test
Remarks	Descrição da lista branca personalizada	Test

Passo 5 Clique em **OK**.

----Fim

Outras operações

Remover informações de logon da lista branca de logon

Para excluir uma parte das informações de logon da lista branca, selecione-a e clique em **Delete** ou clique em **Delete** na coluna **Operation**.

NOTA

Tenha cuidado ao executar a operação de exclusão porque ela não pode ser revertida.

6.2.2 Gerenciamento da lista branca de alarmes

Você pode configurar a lista branca de alarmes para reduzir alarmes falsos. Os eventos podem ser excluídos da lista branca.

Os eventos na lista branca não acionarão alarmes.

Na página **Alarms**, você pode adicionar alarmes falsamente relatados à lista branca de alarmes. Depois que um alarme é adicionado à lista branca, o HSS não gerará alarmes nem coletará estatísticas sobre ele.

Restrições

Qualquer uma das edições premium, WTP ou CGS deve estar ativada.

Adicionar eventos à lista branca de alarmes

Tabela 6-10 Configurar a lista branca de alarmes

Método	Descrição
Adicionar à lista branca de alarmes	Escolha adicionar o alarme à lista branca ao lidar com ele. Os seguintes tipos de eventos podem ser adicionados à lista branca de alarmes: ● Shells reversos ● Ransomware ● Programas maliciosos ● Web shell ● Comportamentos anormais do processo ● Escalonamentos de privilégio do processo ● Escalonamentos de privilégio de arquivo ● Execuções de comando de alto risco ● Programas maliciosos ● Alterações de arquivo importante ● Alterações de arquivo/diretório ● Shells anormais ● Tarefas suspeitas de crontab ● Contas inválidas ● Explosões comuns de vulnerabilidades ● Explosões de vulnerabilidade do Redis ● Explosões de vulnerabilidade de Hadoop ● Explorações de vulnerabilidade do MySQL

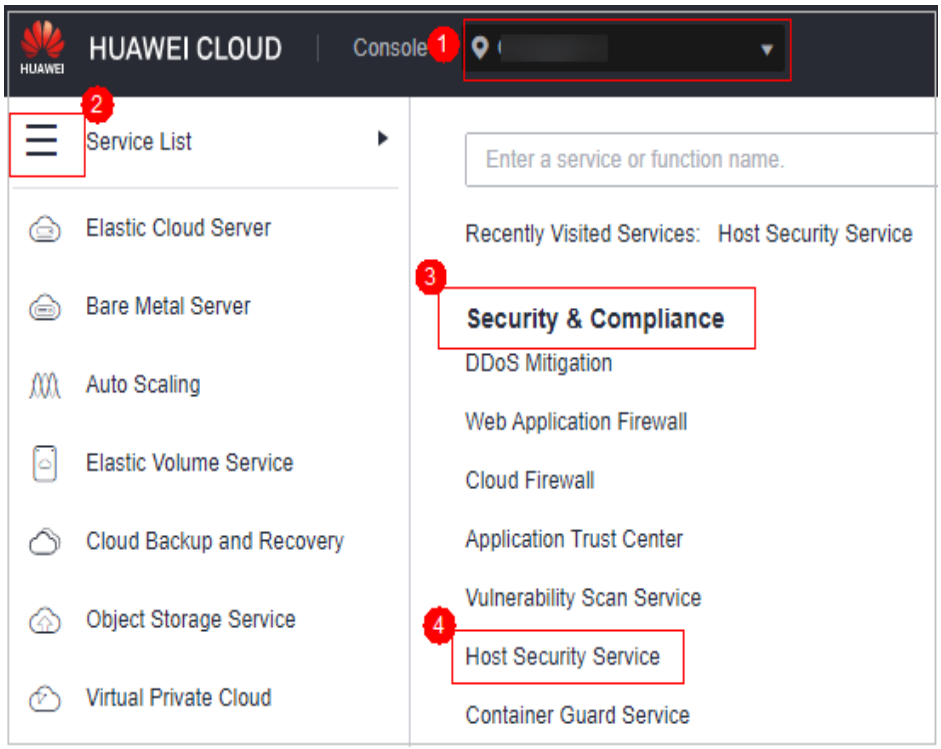
Verificação da lista branca de alarmes

Execute as seguintes etapas para verificar a lista branca do alarme:

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 6-16 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Detection** > **Whitelists**.

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 Clique em **Alarm Whitelist** para visualizar a lista branca de alarmes adicionada. Para obter mais informações, consulte **Tabela 6-11**.

Figura 6-17 Lista branca do alarme

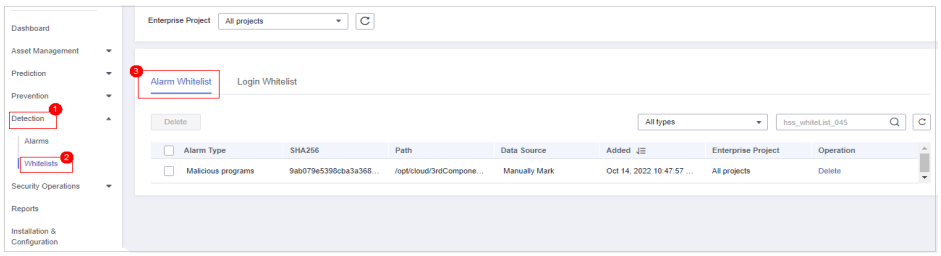


Tabela 6-11 Descrição do parâmetro

Nome do parâmetro	Descrição
Alarm Type	Nome do tipo de lista branca de alarmes.
SHA256	Valor de hash do arquivo de destino.
Path	Caminho que armazena o arquivo do servidor.
Data Source	Fonte da lista branca de destino.
Added	Hora em que um alarme é adicionado à lista branca.
Enterprise Project	Projeto empresarial

----Fim

Procedimento de acompanhamento

Remover alarmes da lista branca

Para remover um alarme da lista branca, selecione-o e clique em **Delete**.

NOTA

- Tenha cuidado ao realizar esta operação. Os alarmes da lista branca não podem ser restaurados após a remoção e serão relatados quando acionados.
- Depois que um alarme é excluído da lista branca, o status de manipulação dos eventos vinculados ao alarme não é atualizado. Para alterar o status, escolha **Detection** > **Alarms**, clique em **Handle** na coluna **Operation** de um evento e selecione **Remove from whitelist**.

6.2.3 Configuração da lista branca de usuários do sistema

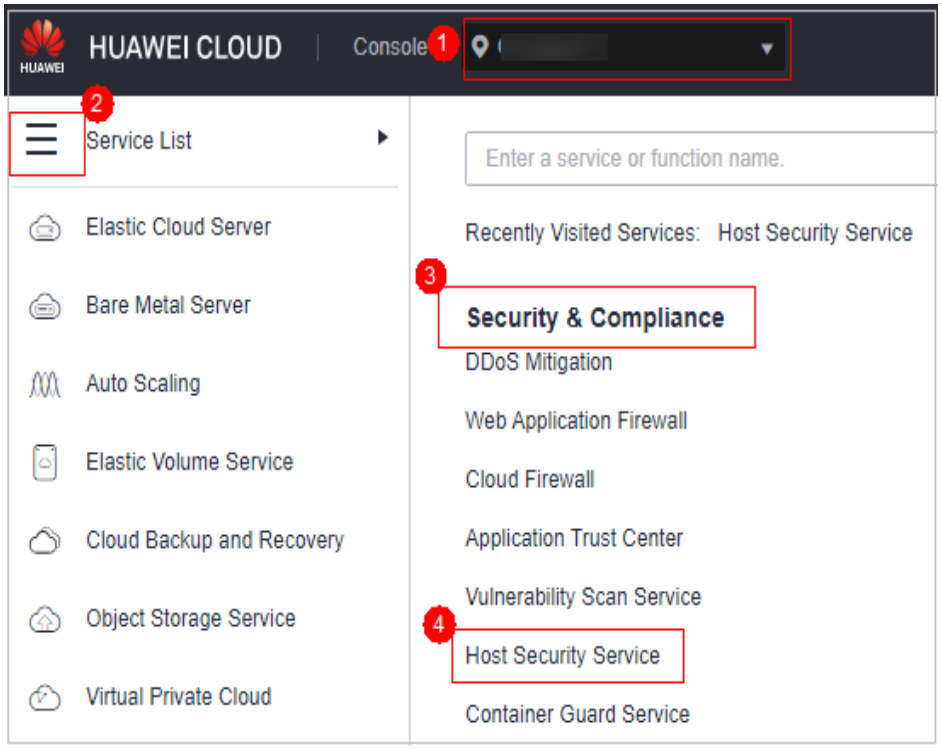
O HSS gera alarmes de conta arriscada quando usuários não raiz são adicionados ao grupo de usuários raiz. Você pode adicionar os usuários não raiz confiáveis à lista branca de usuários do sistema. O HSS não gera alarmes de conta arriscada para usuários na lista branca de usuários do sistema.

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 6-18 Acessar o HSS



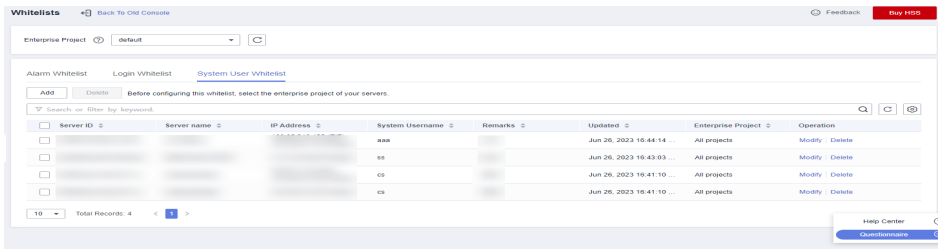
Passo 3 No painel de navegação à esquerda, escolha **Detection** > **Whitelists**. A página **Whitelists** é exibida.

Passo 4 (Opcional) No canto superior esquerdo da página **Whitelists**, selecione o projeto empresarial ao qual o servidor pertence ou **All projects** para **Enterprise Project**.

Se você não ativou a função de projeto empresarial, ignore esta etapa.

Passo 5 Clique na guia **System User Whitelist** e clique em **Add**.

Figura 6-19 Configuração da lista branca do usuário do sistema



Passo 6 Na caixa de diálogo **Add to System User Whitelist**, digite o ID do servidor, o nome de usuário do sistema e as observações.

Passo 7 Clique em **OK**.

----Fim

Operações relacionadas

Modificar uma lista branca de usuários do sistema

Passo 1 (Opcional) No canto superior esquerdo da página **Whitelists**, selecione o projeto empresarial ao qual o servidor pertence ou **All projects** para **Enterprise Project**.

Se você não ativou a função de projeto empresarial, ignore esta etapa.

Passo 2 Na linha da lista branca do usuário do sistema de destino, clique em **Modify** na coluna **Operation**.

Passo 3 Na caixa de diálogo **Modify System User Whitelist**, modifique as informações e clique em **OK**.

----Fim

Excluir uma lista branca de usuários do sistema

Passo 1 (Opcional) No canto superior esquerdo da página **Whitelists**, selecione o projeto empresarial ao qual o servidor pertence ou **All projects** para **Enterprise Project**.

Se você não ativou a função de projeto empresarial, ignore esta etapa.

Passo 2 Na linha da lista branca de usuários do sistema de destino, clique em **Delete** na coluna **Operation**.

Você também pode selecionar várias listas brancas de usuários do sistema e clicar em **Delete** no canto superior esquerdo da lista branca de usuários do sistema.

Passo 3 Na caixa de diálogo exibida, clique em **OK**.

----Fim

7 Operações de segurança

7.1 Gerenciamento de políticas

7.1.1 Visualização de um grupo de políticas

Você pode agrupar políticas e servidores para aplicar políticas em lote a servidores e containers, adaptando-se facilmente a cenários de negócios.

Restrições

A edição profissional, empresarial, premium, WTP ou de container está ativada.

Antes de começar

- Quando você ativa a edição empresarial, o grupo de políticas do lado do locatário desta edição (incluindo senha fraca e políticas de detecção de shell de site) entra em vigor em todos os seus servidores.
- Quando você ativa a edição premium separadamente ou ativa a edição premium incluída na edição WTP, o grupo de políticas do lado do locatário desta edição entra em vigor.

  Para criar seu próprio grupo de políticas, você pode copiar o grupo de políticas do lado do locatário e adicionar ou remover políticas na cópia.

Lista de políticas

Nome da política	Ação	SO suportado	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição CGS
Asset Discovery	Verificar e exibir todos os softwares em um só lugar, incluindo o nome do software, o caminho e as principais aplicações, ajudando a identificar ativos anormais.	Linux e Windows	×	×	√	√	√
AV Detection	Verificar os ativos do servidor e informar, isolar e eliminar os vírus detectados. Os alarmes gerados são exibidos em **Detection** > **Alarms** > **Server Alarms** > **Event Types** > **Malware**. Depois que a detecção AV é ativada, o uso de recursos é o seguinte: O uso da CPU não excede 40% de uma única vCPU. O uso real da CPU depende do status do servidor. Para obter detalhes, consulte **Quantos recursos de CPU e memória estão ocupados pelo agente quando ele executa verificações?**	Windows	√	√	√	√	×
Configuration Check	Verificar as configurações inseguras de Tomcat, Nginx e logon SSH encontradas pelo HSS.	Linux e Windows	×	×	√	√	√
Container Information Collection	Coletar informações sobre todos os containers em um servidor, incluindo portas e diretórios, e relatar alarmes para informações arriscadas.	Linux	×	×	×	×	√

Nome da política	Ação	SO suportado	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição CGS
Weak Password Detection	Alterar as senhas fracas por outras mais fortes com base nos resultados e sugestões da verificação do HSS.	Linux	√	√	√	√	√
Cluster Intrusion Detection	Detectar alterações de alto privilégio de container, criação de informações importantes e invasão de vírus.	Linux	×	×	×	×	√
Container escape	Verificar e gerar alarmes em escapes de containers.	Linux	×	×	×	×	√
Web Shell Detection	Verificar os diretórios da Web em servidores em busca de web shells.	Linux e Windows	√	√	√	√	√
Container File Monitoring	Detectar o acesso a arquivo que viola as políticas de segurança. O pessoal de O&M de segurança pode verificar se os hackers estão intrometendo e adulterando arquivos confidenciais.	Linux	×	×	×	×	√
Container Process Whitelist	Verifique se há inicializações de processos que violam as políticas de segurança.	Linux	×	×	×	×	√
Suspicious Image Behaviors	Configurar a lista negra e a lista branca e personalizar as permissões para ignorar comportamentos anormais ou relatar alarmes.	Linux	×	×	×	×	√
HIPS Detection	Verificar registros, arquivos e processos e relatar alarmes para operações como alterações anormais.	Linux e Windows	×	√	√	√	√

Nome da política	Ação	SO suportado	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição CGS
File Protection	Verificar os arquivos no SO Linux, aplicações e outros componentes para detectar adulteração.	Linux	√	√	√	√	√
Login Security Check	Detectar ataques de força bruta em contas SSH, FTP e MySQL. Se o número de ataques de força bruta (tentativas consecutivas de senha incorreta) de um endereço IP atingir 5 em 30 segundos, o endereço IP será bloqueado. Por padrão, os invasores SSH suspeitos são bloqueados por 12 horas. Outros tipos de invasores suspeitos são bloqueados por 24 horas. Você pode verificar se o endereço IP é confiável com base no seu tipo de ataque e quantas vezes ele foi bloqueado. Você pode desbloquear manualmente os endereços IP confiáveis.	Linux e Windows	√	√	√	√	√
Malicious File Detection	● Shell reverso: monitorar o comportamento do processo do usuário em tempo real para detectar shells reversos causados por conexões inválidas. ● Detectar ações em shells anormais, incluindo mover, copiar e excluir arquivos de shell e modificar as permissões de acesso e links físicos dos arquivos.	Linux	√	√	√	√	√

Nome da política	Ação	SO suportado	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição CGS
Port Scan Detection	Detectar verificação ou farejamento em portas especificadas e relatar alarmes.	Linux	×	×	√	√	√
Abnormal process behaviors	Todos os processos em execução em todos os seus servidores são monitorados para você. Você pode criar uma lista branca de processos para ignorar alarmes em processos confiáveis e pode receber alarmes sobre comportamentos e invasões de processos não autorizados.	Linux	√	×	√	√	√
Root privilege escalation	Detectar o escalonamento de privilégios de raiz para arquivos no sistema atual.	Linux	√	√	√	√	√
Real-time Process	Monitorar os comandos executados em tempo real e gerar alarmes se forem detectados comandos de alto risco.	Linux e Windows	√	√	√	√	√
Rootkit Detection	Detectar ativos do servidor e relatar alarmes para módulos, arquivos e pastas do kernel suspeitos.	Linux	√	√	√	√	√

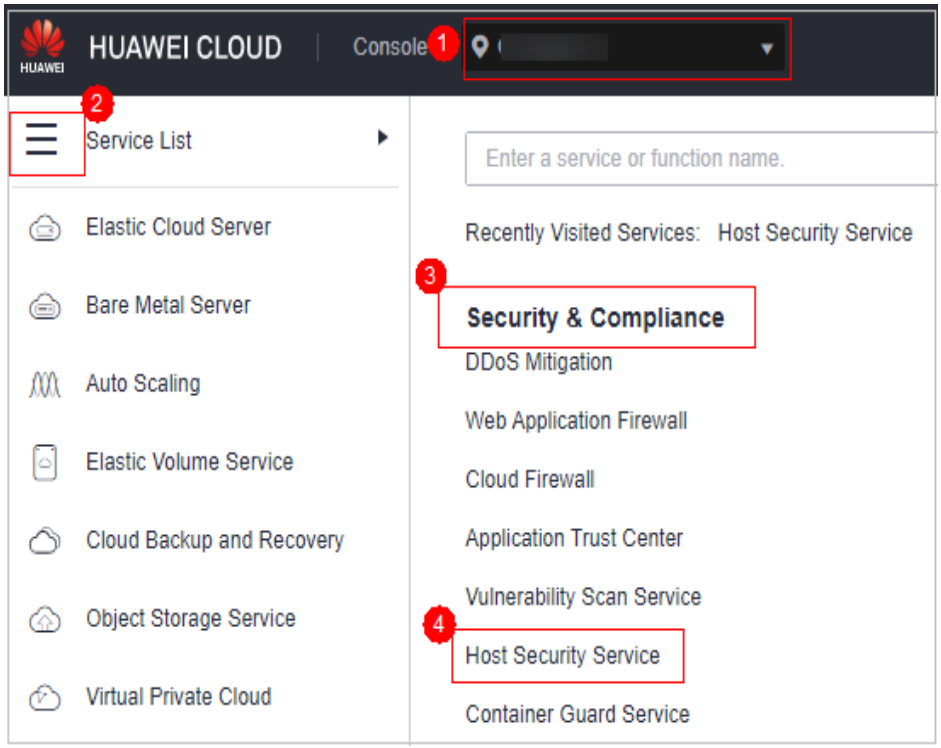
Nome da política	Ação	SO suportado	Edição profissional	Edição empresarial	Edição premium	Edição WTP	Edição CGS
Self-protection	Proteger arquivos, processos e softwares do HSS contra programas maliciosos, que podem desinstalar agentes do HSS, adulterar arquivos do HSS ou interromper processos do HSS. ● 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. ● 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. – Os processos do HSS não podem ser encerrados. – 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).	Windows	×	×	√	√	×

Checking the Policy Group List

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 7-1 Acessar o HSS



Passo 3 Na árvore de navegação à esquerda, escolha **Security Operations** > **Policies** para verificar os grupos de políticas exibidos. Para obter mais informações, consulte **Tabela 7-1**.

NOTA

- **tenant_linux_advanced_default_policy_group**: política predefinida da edição profissional do Linux, que só pode ser visualizada, mas não pode ser copiada ou excluída.
- **tenant_windows_advanced_default_policy_group**: política de predefinição da edição profissional do Windows, que só pode ser visualizada, mas não pode ser copiada ou excluída.
- **tenant_linux_container_default_policy_group** é o grupo de políticas padrão do Linux da edição de container. Este grupo de políticas só pode ser visualizado e não pode ser copiado ou excluído.
- **tenant_linux_enterprise_default_policy_group** é o grupo de políticas padrão do Linux da edição empresarial. Este grupo de políticas só pode ser visualizado e não pode ser copiado ou excluído.
- **tenant_windows_enterprise_default_policy_group** é o grupo de políticas do Windows padrão da edição empresarial. Este grupo de políticas só pode ser visualizado e não pode ser copiado ou excluído.
- **tenant_linux_premium_default_policy_group** é o grupo de políticas padrão do Linux da edição premium. Você pode criar um grupo de políticas copiando esse grupo padrão e modificar a cópia.
- **tenant_windows_premium_default_policy_group** é o grupo de políticas padrão do Windows da edição premium. Você pode criar um grupo de políticas copiando esse grupo padrão e modificar a cópia.
- **wtp**_*ServerName* é um grupo de políticas de edição WTP. Ele é gerado por padrão quando a WTP está ativada para um servidor.

- Para atualizar a lista, clique em  no canto superior direito.
- Para visualizar detalhes sobre os servidores vinculados a um grupo de políticas, clique no número na coluna **Servers** do grupo.

Tabela 7-1 Parâmetros do grupo de políticas

Parâmetro	Descrição
Policy Group	Nome de um grupo de políticas
ID	ID exclusivo de um grupo de políticas
Description	Descrição de um grupo de políticas
Supported Version	Edição do HSS suportada por um grupo de políticas
OS	SO suportado pela política.
Servers	Número de servidores vinculados à política

Passo 4 Clique no nome de um grupo de políticas para verificar os detalhes da política, incluindo os nomes, status, categorias de função, tipo de SO das políticas.

NOTA

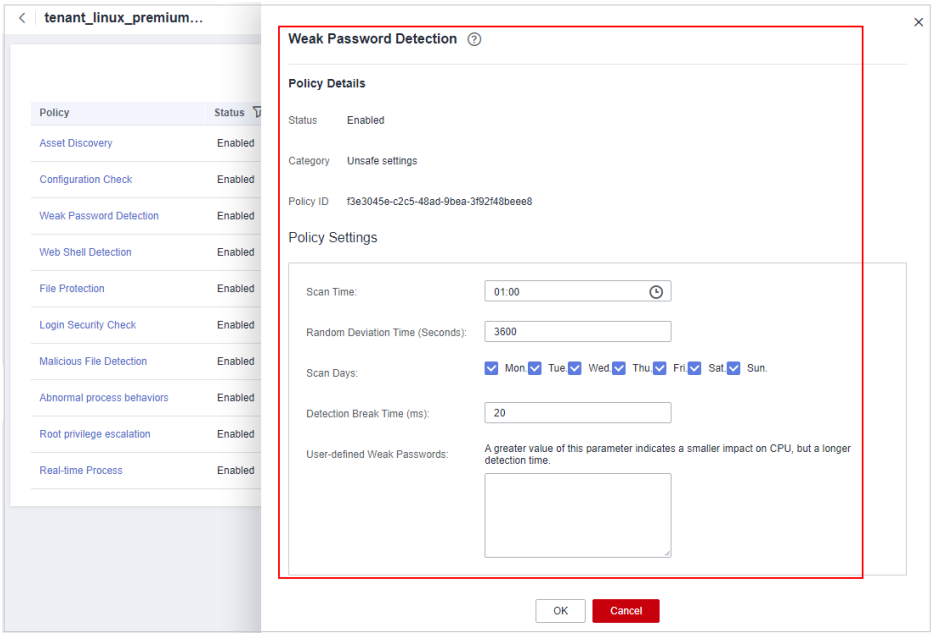
- Todas as políticas no grupo **tenant_enterprise_policy_group** são ativadas por padrão.
- Você pode clicar em **Enable** ou **Disable** na coluna **Operation** de uma política para controlar o que verificar.

Passo 5 Para visualizar as informações detalhadas sobre uma política, clique no nome da política.

NOTA

Para obter detalhes sobre como modificar uma política, consulte **Modificação de uma política**.

Figura 7-2 Exemplo de detalhes de política de senha fraca



----Fim

7.1.2 Criação de um grupo de políticas

Você pode criar um grupo de políticas para executar uma verificação específica e detalhada em determinados servidores.

Pré-requisito

A edição premium foi ativada.

NOTA

Até agora, você pode criar um grupo de políticas somente na edição premium. Se a edição premium não estiver ativada para um servidor, o grupo de políticas criado para ele não terá efeito.

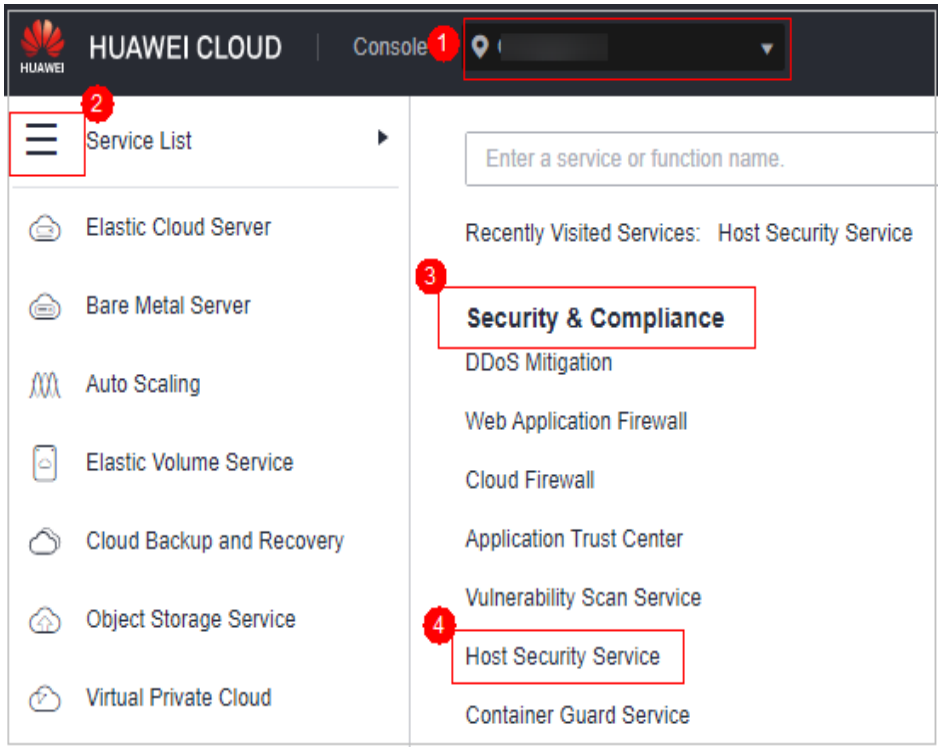
Criação de um grupo de políticas

O seguinte usa uma política de servidor de Linux na edição premium como um exemplo:

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 7-3 Acessar o HSS



Passo 3 Na árvore de navegação à esquerda, escolha **Security Operations** > **Policies** para verificar os grupos de políticas exibidos. Para obter mais informações, consulte **Tabela 7-2**.

NOTA

- **tenant_linux_advanced_default_policy_group**: política predefinida da edição profissional do Linux, que só pode ser visualizada, mas não pode ser copiada ou excluída.
- **tenant_windows_advanced_default_policy_group**: política de predefinição da edição profissional do Windows, que só pode ser visualizada, mas não pode ser copiada ou excluída.
- **tenant_linux_container_default_policy_group** é o grupo de políticas padrão do Linux da edição de container. Este grupo de políticas só pode ser visualizado e não pode ser copiado ou excluído.
- **tenant_linux_enterprise_default_policy_group** é o grupo de políticas padrão do Linux da edição empresarial. Este grupo de políticas só pode ser visualizado e não pode ser copiado ou excluído.
- **tenant_windows_enterprise_default_policy_group** é o grupo de políticas do Windows padrão da edição empresarial. Este grupo de políticas só pode ser visualizado e não pode ser copiado ou excluído.
- **tenant_linux_premium_default_policy_group** é o grupo de políticas padrão do Linux da edição premium. Você pode criar um grupo de políticas copiando esse grupo padrão e modificar a cópia.
- **tenant_windows_premium_default_policy_group** é o grupo de políticas padrão do Windows da edição premium. Você pode criar um grupo de políticas copiando esse grupo padrão e modificar a cópia.
- **wtp_***ServerName* é um grupo de políticas de edição WTP. Ele é gerado por padrão quando a WTP está ativada para um servidor.
- Para atualizar a lista, clique em no canto superior direito.
- Para visualizar detalhes sobre os servidores vinculados a um grupo de políticas, clique no número na coluna **Servers** do grupo.

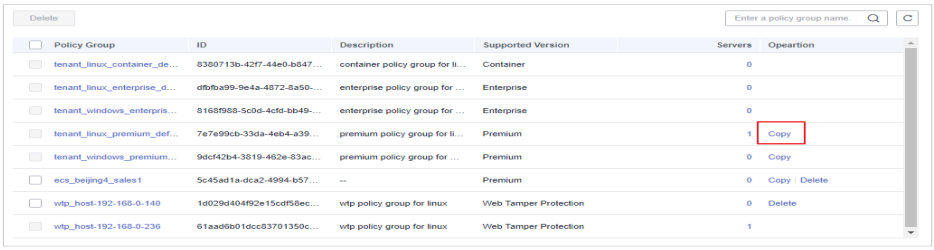
Tabela 7-2 Parâmetros do grupo de políticas

Parâmetro	Descrição
Policy Group	Nome de um grupo de políticas
ID	ID exclusivo de um grupo de políticas
Description	Descrição de um grupo de políticas
Supported Version	Edição do HSS suportada por um grupo de políticas
OS	SO suportado pela política.
Servers	Número de servidores vinculados à política

Passo 4 Localize o grupo de políticas **tenant_linux_premium_default_policy_group** ou **tenant_windows_premium_default_policy_group** e clique em **Copy** na coluna **Operation** do grupo de políticas.

O seguinte usa um grupo de políticas do Linux como exemplo.

Figura 7-4 Copiar um grupo de política

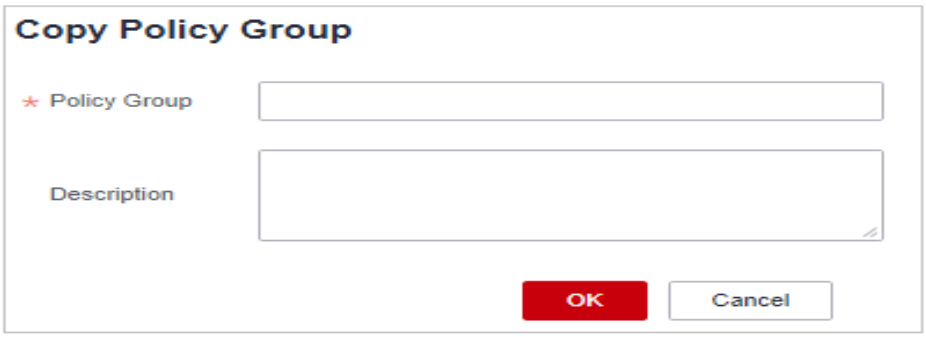


Passo 5 Na caixa de diálogo exibida, insira um nome e uma descrição do grupo de políticas e clique em **OK**.

NOTA

- O nome de um grupo de políticas deve ser exclusivo, ou o grupo não será criado.
- O nome do grupo de políticas e sua descrição podem conter apenas letras, dígitos, sublinhados (_), hifens (-) e espaços e não podem começar ou terminar com um espaço.

Figura 7-5 Criar um grupo de políticas



Passo 6 Clique em **OK**.

Passo 7 Clique no nome do grupo de políticas que acabou de criar. As políticas no grupo serão exibidas.

Passo 8 Clique em um nome de política e modifique suas configurações conforme necessário. Para mais detalhes, consulte **Modificação de uma política**.

Passo 9 Ative ou desative a política clicando no botão correspondente na coluna **Operation**.

----Fim

Operações de acompanhamento

Excluir um grupo de políticas

Depois que um grupo de políticas for excluído, a coluna **Policy Group** dos servidores vinculados ao grupo ficará em branco.

Passo 1 Vá para a lista de políticas. Exclua uma ou várias políticas.

Figura 7-6 Exclusão de grupos de políticas

Policy	Status	Category	OS	Opeartion
Asset Discovery	Enabled	Asset management	Linux	Disabled
Configuration Check	Enabled	Unsafe settings	Linux	Disabled
Weak Password Detection	Enabled	Unsafe settings	Linux	Disabled
Web Shell Detection	Enabled	Intrusion detection	Linux	Disabled
File Protection	Enabled	Intrusion detection	Linux	Disabled
Login Security Check	Enabled	Intrusion detection	Linux	Disabled
Malicious File Detection	Enabled	Intrusion detection	Linux	Disabled
Abnormal process behaviors	Enabled	Intrusion detection	Linux	Disabled
Root privilege escalation	Enabled	Intrusion detection	Linux	Disabled
Real-time Process	Enabled	Intrusion detection	Linux	Disabled

NOTA

Você pode clicar em **Delete** na coluna **Operation** de um grupo de políticas para excluí-lo.

Você também pode selecionar vários grupos de políticas e clicar em **Delete** acima da lista para excluí-los em lotes.

Passo 2 Na caixa de diálogo exibida, clique em **OK**.

----Fim

7.1.3 Modificação de uma política

Esta seção descreve como modificar políticas em um grupo de políticas.

AVISO

- Modificações em uma política entram em vigor somente no grupo ao qual ela pertence.
- Para os grupos de políticas padrão, é aconselhável manter suas configurações padrão.

Restrições

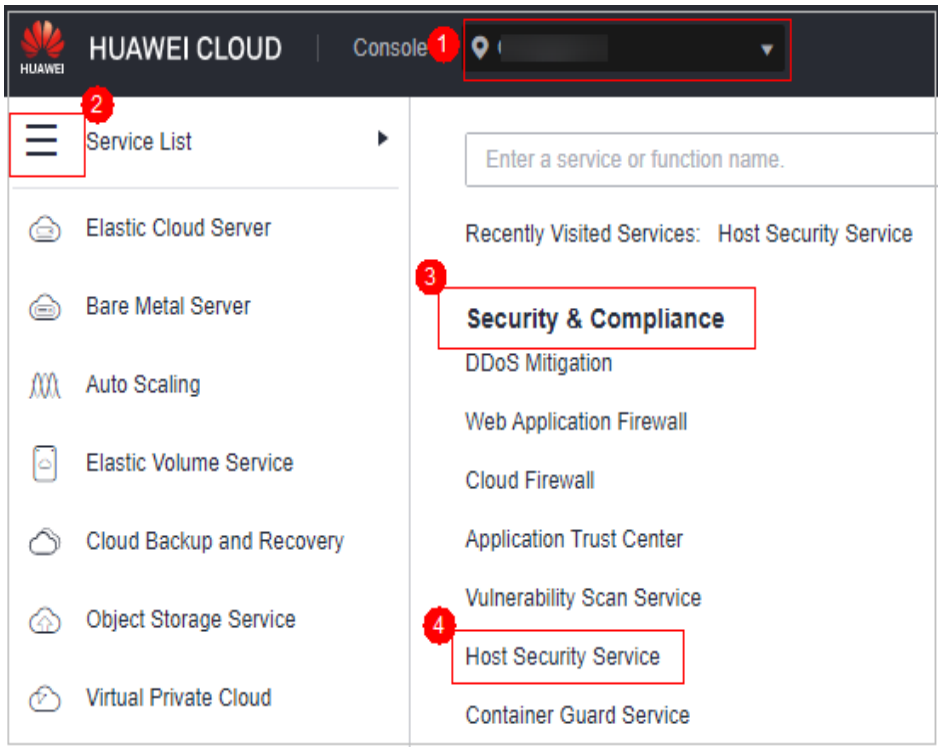
A edição profissional, empresarial, premium, WTP ou de container está ativada.

Acessar a página de políticas

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 7-7 Acessar o HSS



Passo 3 Na árvore de navegação à esquerda, escolha **Security Operations** > **Policies** para verificar os grupos de políticas exibidos. Para obter mais informações, consulte **Tabela 7-3**.

NOTA

- **tenant_linux_advanced_default_policy_group**: política predefinida da edição profissional do Linux, que só pode ser visualizada, mas não pode ser copiada ou excluída.
- **tenant_windows_advanced_default_policy_group**: política de predefinição da edição profissional do Windows, que só pode ser visualizada, mas não pode ser copiada ou excluída.
- **tenant_linux_container_default_policy_group** é o grupo de políticas padrão do Linux da edição de container. Este grupo de políticas só pode ser visualizado e não pode ser copiado ou excluído.
- **tenant_linux_enterprise_default_policy_group** é o grupo de políticas padrão do Linux da edição empresarial. Este grupo de políticas só pode ser visualizado e não pode ser copiado ou excluído.
- **tenant_windows_enterprise_default_policy_group** é o grupo de políticas do Windows padrão da edição empresarial. Este grupo de políticas só pode ser visualizado e não pode ser copiado ou excluído.
- **tenant_linux_premium_default_policy_group** é o grupo de políticas padrão do Linux da edição premium. Você pode criar um grupo de políticas copiando esse grupo padrão e modificar a cópia.
- **tenant_windows_premium_default_policy_group** é o grupo de políticas padrão do Windows da edição premium. Você pode criar um grupo de políticas copiando esse grupo padrão e modificar a cópia.
- **wtp**_*ServerName* é um grupo de políticas de edição WTP. Ele é gerado por padrão quando a WTP está ativada para um servidor.
- Para atualizar a lista, clique em  no canto superior direito.
- Para visualizar detalhes sobre os servidores vinculados a um grupo de políticas, clique no número na coluna **Servers** do grupo.

Tabela 7-3 Parâmetros do grupo de políticas

Parâmetro	Descrição
Policy Group	Nome de um grupo de políticas
ID	ID exclusivo de um grupo de políticas
Description	Descrição de um grupo de políticas
Supported Version	Edição do HSS suportada por um grupo de políticas
OS	SO suportado pela política.
Servers	Número de servidores vinculados à política

Passo 4 Clique no nome do grupo de políticas para acessar a lista de detalhes da política. Você pode modificar a política clicando em seu nome.

----Fim

Descoberta de ativos

Passo 1 Clique em **Asset Discovery**.

Passo 2 Na página exibida, modifique as configurações conforme necessário. Para obter mais informações, consulte **Tabela 7-4**.

Tabela 7-4 Descrição do parâmetro

Parâmetro	Descrição
Scan Time	Tempo fixo para verificação automática de ativos. O tempo de verificação pode ser personalizado para middleware, estruturas da Web, módulos do kernel, aplicações Web, sites, serviços da Web e bancos de dados. O tempo de deslocamento é o ajuste automático antes ou depois do tempo de verificação especificado. ● Contas: as contas do Linux são verificadas automaticamente a cada hora e as contas do Windows são verificadas em tempo real. ● As portas abertas são verificadas automaticamente a cada 30 segundos. ● Os processos são verificados automaticamente a cada hora. ● O software instalado é verificado automaticamente uma vez por dia. ● Os itens de inicialização automática são verificados automaticamente a cada hora. ● Middleware/estrutura da Web: você pode selecionar a data e a hora da verificação juntos. ● Módulos do kernel: você pode definir a data e a hora da verificação conforme necessário. ● Aplicações Web/sites/serviços Web/bancos de dados: você pode selecionar a data e a hora da verificação juntos.
Software Scanned	● Nome do software. Um nome pode conter um máximo de 5.000 caracteres sem nenhum espaço. Use vírgulas (,) para separar nomes de software. ● Se esse parâmetro não for especificado, as informações sobre todos os softwares instalados serão recuperadas como seu valor.
Software Scanned	Caminho para pesquisa de software. Este parâmetro não é necessário para servidores do Windows.
Web Directory to Be Scanned	Especifica um diretório Web a ser verificado.
Web Directory Scan Depth	Especifica o nível de profundidade para verificação de diretórios Web.

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Verificação de senha fraca

Senhas fracas não são atribuídas a um certo tipo de vulnerabilidade, mas elas não trazem menos riscos de segurança do que qualquer tipo de vulnerabilidade. Dados e programas se tornarão inseguros se suas senhas forem quebradas.

O HSS detecta proativamente as contas usando senhas fracas e gera alarmes para as contas. Você também pode adicionar uma senha que pode ter sido vazada à lista de senhas fracas para impedir que as contas do servidor usem a senha.

Passo 1 Clique em **Weak Password Detection**.

Passo 2 Na área **Policy Settings**, modifique as configurações conforme necessário. Para obter mais informações, consulte **Tabela 7-5**.

Figura 7-8 Modificar a política de detecção de senha fraca

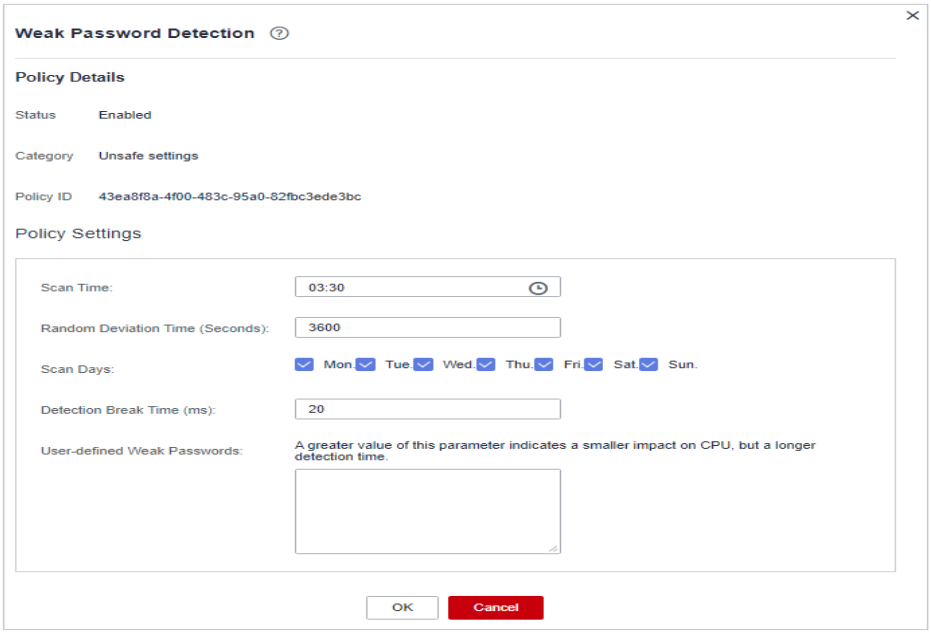


Tabela 7-5 Descrição do parâmetro

Parâmetro	Descrição
Scan Time	Momento em que as detecções são realizadas. Pode ser preciso ao minuto.
Random Deviation Time (s)	Tempo de desvio aleatório da senha fraca com base em **Scan Time**. O intervalo de valores é de 0 a 7200s.
Scan Days	Dias em uma semana em que as senhas fracas são verificadas. Você pode selecionar um ou mais dias.
Detection Break Time (ms)	Intervalo entre as verificações de duas contas. O intervalo de valores é de 0 a 2.000. Por exemplo, se esse parâmetro for definido como **50**, o sistema verificará **/bin/ls** a cada 50 milissegundos.

Parâmetro	Descrição
User-defined Weak Passwords	Você pode adicionar uma senha que pode ter sido vazada a essa caixa de texto de senha fraca para impedir que as contas do servidor usem a senha. Digite apenas uma senha fraca por linha. Até 300 senhas fracas podem ser adicionadas.

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Verificação de configuração

Passo 1 Clique em **Configuration Check**.

Passo 2 Em **Configure Check**, modifique a política.

Figura 7-9 Modificar a política de verificação de configuração

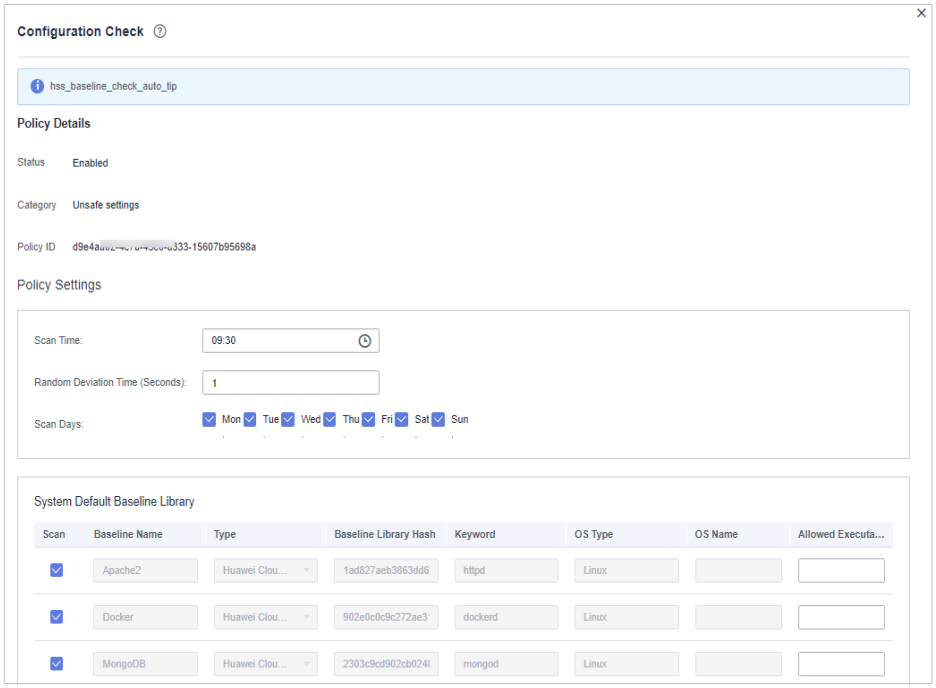


Tabela 7-6 Descrição do parâmetro

Parâmetro	Descrição
Scan Time	Momento em que as detecções são realizadas. Pode ser preciso ao minuto.
Random Deviation Time (Seconds)	Tempo de desvio aleatório da detecção do sistema. O valor varia de 0 a 7200s.

Parâmetro	Descrição
Scan Days	Dia em uma semana em que uma detecção é realizada. Você pode selecionar qualquer dia de segunda a domingo.

Passo 3 Selecione a linha de base a ser detectada ou personalize uma linha de base.

NOTA

Para verificar se o seu sistema atende aos requisitos de conformidade, selecione **DJCP MLPS** na área **Type**.

Passo 4 Confirme as informações e clique em **OK**.

----Fim

Detecção de web shell

Se **User-defined Scan Paths** não for especificado, os caminhos do site em seus ativos serão verificados por padrão. Se **User-defined Scan Paths** for especificado, somente os caminhos especificados serão verificados.

Passo 1 Clique em **Web Shell Detection**.

Passo 2 Na página **Web Shell Detection**, modifique as configurações conforme necessário. Para obter mais informações, consulte **Tabela 7-7**.

Figura 7-10 Modificar a política de detecção de web shell

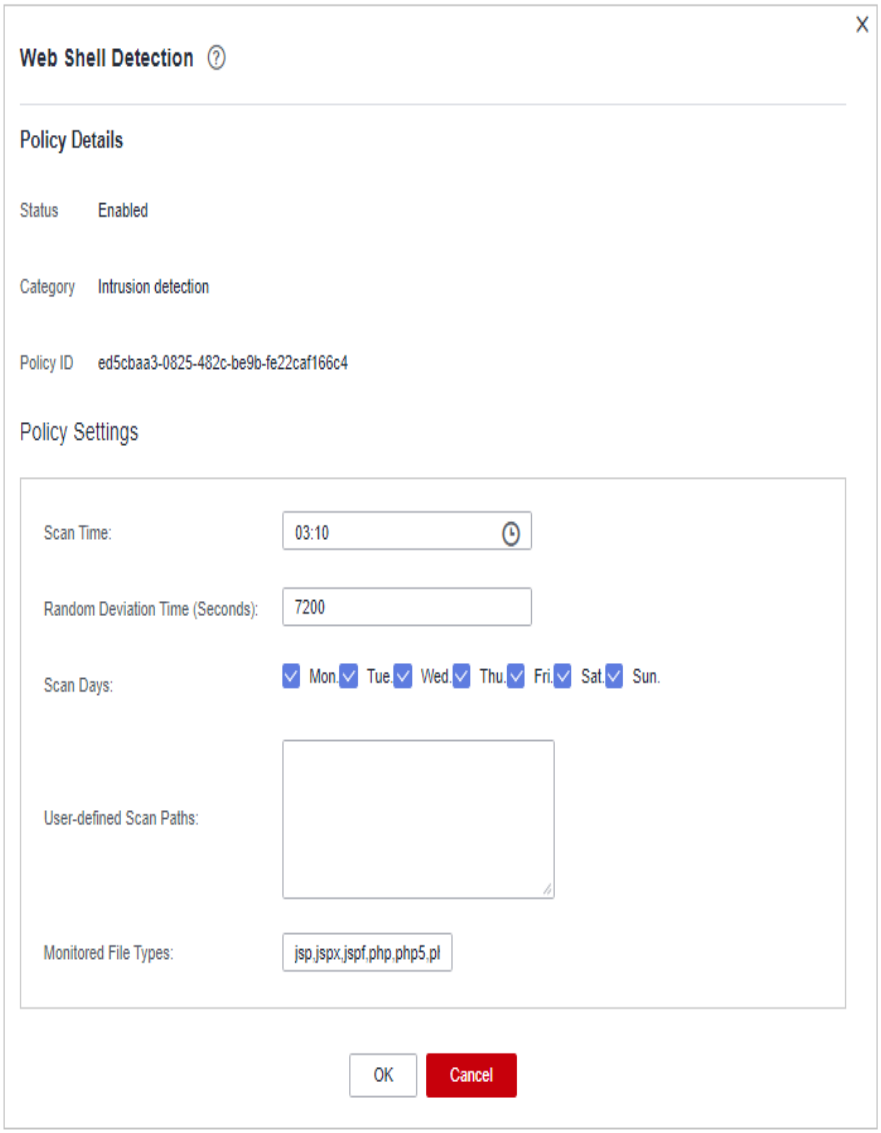


Tabela 7-7 Descrição do parâmetro

Parâmetro	Descrição
Scan Time	Momento em que as detecções são realizadas. Pode ser preciso ao minuto.
Random Deviation Time (Seconds)	Tempo de desvio aleatório. O valor varia de 0 a 7200s.
Scan Days	Dias em uma semana em que os web shells são verificados. Você pode selecionar um ou mais dias.
User-defined Scan Paths	Caminhos da Web a serem verificados. Um caminho de arquivo deve: ● Começar com uma barra (/) e terminar sem barras (/). ● Ocupar uma linha separada e não pode conter espaços.

Parâmetro	Descrição
Monitored Files Types	Extensões de arquivos a serem verificadas. Os valores válidos incluem **jsp**, **jspx**, **jspf**, **php**, **php5**, **php4**.

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Proteção de arquivos

Passo 1 Clique em **File Protection**.

Passo 2 Na página **File Protection**, modifique a política. Para obter mais informações, consulte **Tabela 7-8**.

Figura 7-11 Proteção de arquivos

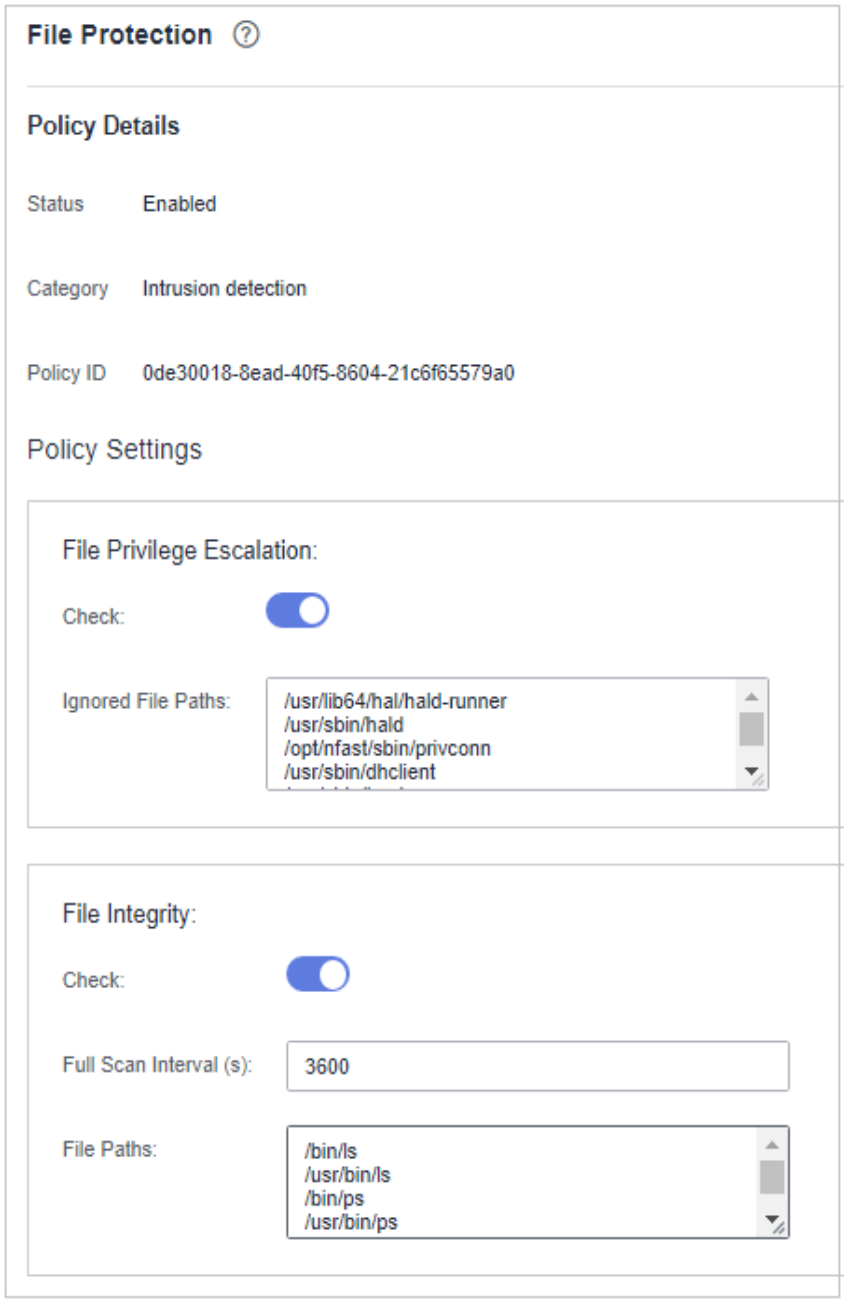


Tabela 7-8 Descrição do parâmetro

Parâmetro	Descrição
File Privilege Escalation	● Detecta escalonamento de privilégios. –  : ativar –  : desativar ● **Ignored File Path**: arquivos a serem ignorados. Comece o caminho com uma barra (/) e não termine com uma barra (/). Cada caminho ocupa uma linha. Não são permitidos espaços entre os nomes dos caminhos.
File Integrity	● Detecta a integridade dos arquivos principais. –  : ativar –  : desativar ● **File Paths**: configure os caminhos dos arquivos.
Important File Directory Change	● Detecta a alteração de diretório dos arquivos principais. –  : ativar –  : desativar ● **Enable Audit**: ativa a função de detecção de auditoria. Se a função estiver ativada e o uso de inotify exceder o limite, algumas alterações no diretório de arquivos não poderão ser detectadas. –  : ativar –  : desativar ● **Session IP Whitelist**: se o processo de arquivo pertencer às sessões dos endereços IP listados, nenhuma auditoria será aplicada. ● **Unmonitored File Types**: tipos de arquivos que não precisam ser monitorados. ● **Unmonitored File Paths**: caminhos de arquivo que não precisam ser monitorados. ● **Monitoring Login Keys**: ativa a função de monitorar chaves de logon. –  : ativar –  : desativar

Parâmetro	Descrição
Directory Monitoring Mode	● Modo de monitoramento de diretório. ● **File or Directory Path**: alguns caminhos de monitoramento de arquivos ou diretórios são predefinidos no sistema. Você pode modificar o tipo de alteração de arquivo a ser detectado e adicionar os caminhos de arquivos ou diretórios a serem monitorados.

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Detecção de HIPS

Passo 1 Clique em **HIPS Detection**.

Passo 2 Modifique o conteúdo da política. Para obter mais informações, consulte **Tabela 7-9**.

Figura 7-12 Modificar a política de detecção de HIPS

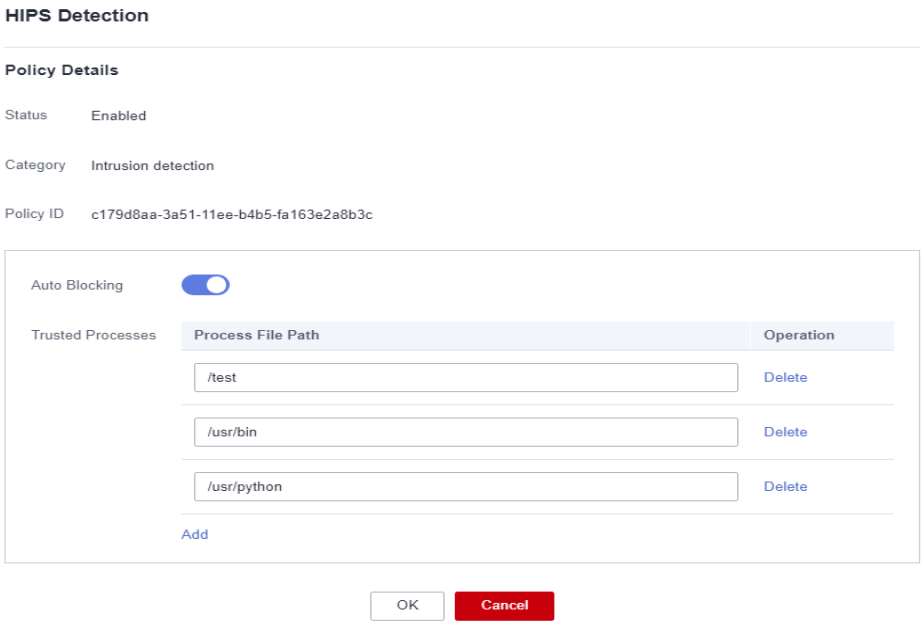


Tabela 7-9 Parâmetros de política de detecção de HIPS

Parâmetro	Descrição
Auto Blocking	Se esta função estiver ativada, alterações anormais em registros, arquivos e processos serão automaticamente bloqueadas para evitar shells reversos e comandos de alto risco. ●  : ativar ●  : desativar

Parâmetro	Descrição
Trusted Processes	Caminhos de processos confiáveis. Você pode clicar em **Add** para adicionar um caminho e clicar em **Delete** para excluí-lo.

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Verificação de segurança de logon

Passo 1 Clique em **Login Security Check**.

Passo 2 Na página **Login Security Check** exibida, modifique o conteúdo da política. **Tabela 7-10** descreve os parâmetros.

Figura 7-13 Modificar a política de verificação de segurança

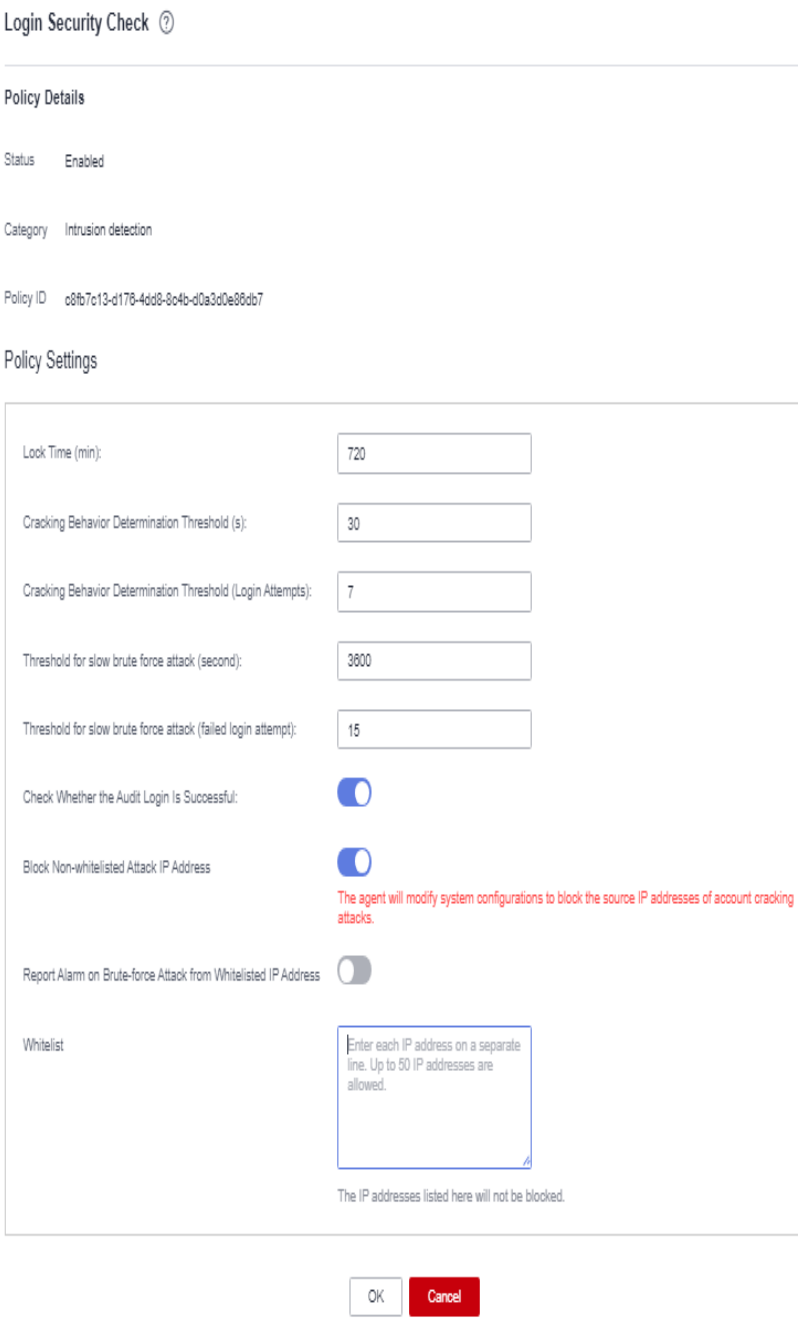


Tabela 7-10 Descrição do parâmetro

Parâmetro	Descrição
Lock Time (min)	Esse parâmetro é usado para determinar quantos minutos os endereços IP que enviam ataques são bloqueados. O intervalo de valores é de 1 a 43.200. O logon não é permitido durante o período de bloqueio.

Parâmetro	Descrição
Cracking Behavior Determination Threshold (s)	Este parâmetro é usado junto com **Cracking Behavior Determination Threshold (Login Attempts)**. O intervalo de valores é de 5 a 3.600. Por exemplo, se esse parâmetro for definido como **30** e **Cracking Behavior Determination Threshold (Login Attempts)** for definido como **5**, o sistema determinará que uma conta será quebrada quando o mesmo endereço IP falhar ao efetuar logon no sistema por cinco vezes dentro de 30 segundos.
Cracking Behavior Determination Threshold (Login Attempts)	Este parâmetro é usado em conjunto com **Cracking Behavior Determination Threshold**. O intervalo de valores é de 1 a 36.000.
Threshold for slow brute force attack (second)	Esse parâmetro é usado junto com **Threshold for slow brute force attack (failed login attempt)**. O intervalo de valores é de 600 a 86.400s. Por exemplo, se este parâmetro for definido como **3600** e **Threshold for slow brute force attack (failed login attempt)** for definido como **15**, o sistema determina que uma conta foi quebrada quando o mesmo endereço IP falha ao fazer logon no sistema por quinze vezes dentro de 3.600 segundos.
Threshold for slow brute-force attack (failed login attempt)	Este parâmetro é usado em conjunto com **Threshold for slow brute force attack (second)**. O intervalo de valores é de 6 a 100.
Check Whether the Audit Login Is Successful	● Depois que essa função é ativada, o HSS relata logs de sucesso de logon. –  : ativar –  : desativar
Block Non-whitelisted Attack IP Address	Depois que essa função é ativada, o HSS bloqueia o logon de endereços IP de força bruta (endereços IP não incluídos na lista branca).
Report Alarm on Brute-force Attack from Whitelisted IP Address	Depois que essa função é ativada, o HSS gera alarmes para ataques de força bruta a partir de endereços IP na lista branca. ●  : ativar ●  : desativar
Whitelist	Depois que um endereço IP é adicionado à lista branca, o HSS não bloqueia ataques de força bruta do endereço IP na lista branca. Um máximo de 50 endereços IP ou segmentos de rede podem ser adicionados à lista branca. Ambos os endereços IPv4 e IPv6 são suportados.

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Detecção de arquivos maliciosos

Passo 1 Clique em **Malicious File Detection**.

Passo 2 Na página exibida, modifique a política. Para obter mais informações, consulte **Tabela 7-11**.

Figura 7-14 Modificar a política de detecção de arquivos maliciosos

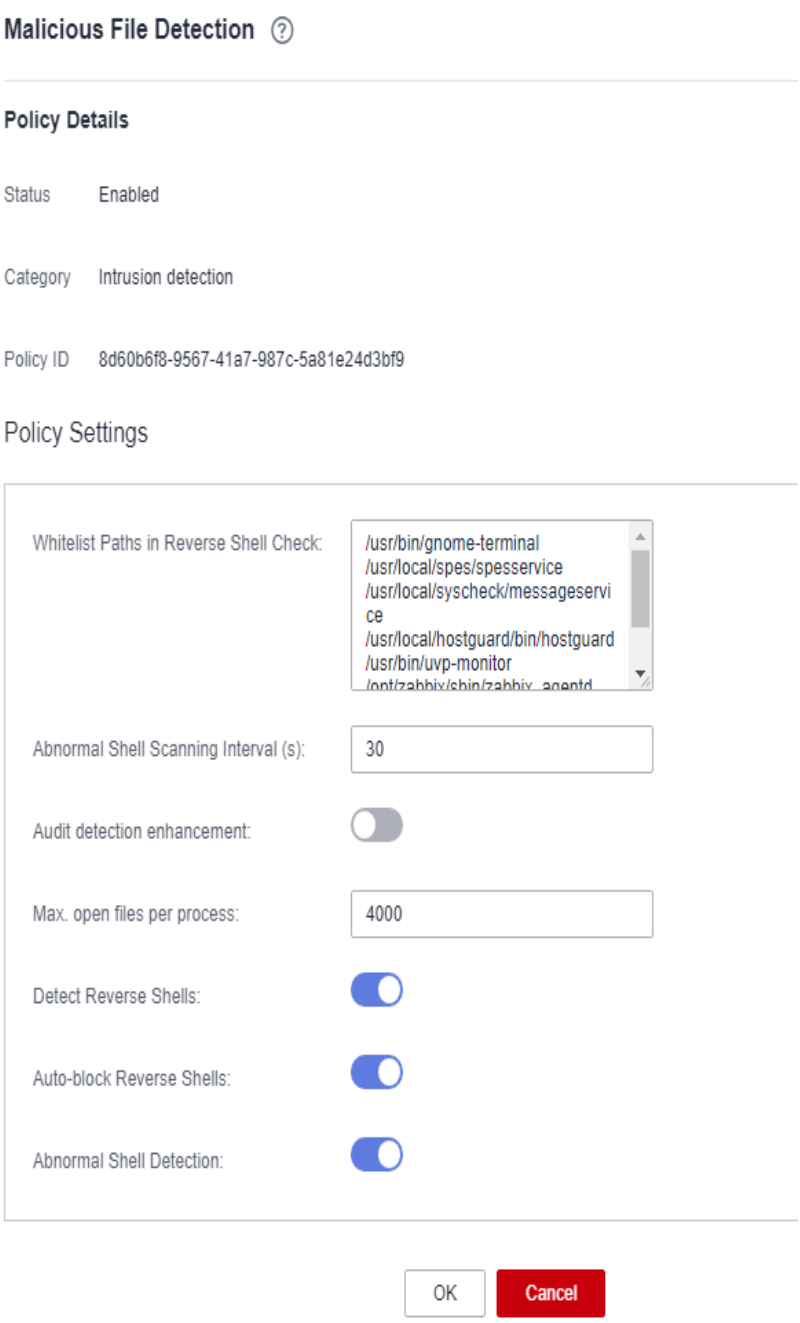


Tabela 7-11 Descrição do parâmetro

Parâmetro	Descrição
Whitelist Paths in Reverse Shell Check	Caminho do arquivo do processo a ser ignorado na detecção de shell reverso Começar com uma barra (/) e terminar sem barras (/). Ocupar uma linha separada e não pode conter espaços.
Reverse Shell Scanning Interval (s)	Período de verificação reversa do shell. O intervalo de valores é de 30 a 86.400.
Audit detection enhancement	● Seja para melhorar a detecção de auditoria. É aconselhável ativar esta função. –  : ativar –  : desativar
Max. open files per process	Número máximo de arquivos que podem ser abertos por um processo. O intervalo de valores é de 10 a 300.000.
Detect Reverse Shells	● Detecta shells reversos. Você é aconselhado a ativá-lo. –  : ativar –  : desativar
Auto-block Reverse Shells	Especifica se deve ser ativado o bloqueio automático de shells reversos. É aconselhável ativar esta função. ●  : ativar ●  : desativar **NOTA** Este parâmetro entra em vigor após a função de **Isolamento e eliminação de programas maliciosos** estar ativada.
Abnormal Shell Detection	● Detecta shells anormais. Você é aconselhado a ativá-lo. –  : ativar –  : desativar

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Comportamento anormal do processo

Passo 1 Clique em **Abnormal process behaviors**.

Passo 2 Na área exibida, modifique as configurações conforme necessário. Para obter mais informações, consulte **Tabela 7-12**.

Tabela 7-12 Descrição do parâmetro

Parâmetro	Descrição	Exemplo de valor
Detection and Scanning Cycle (Seconds)	Intervalo para verificar os programas em execução no host. O intervalo de valores é de 30 a 1.800.	1800
Detection Mode	Selecione o método para detecção de comportamento anormal do processo. ● **Sensitive**: detecção e verificação profunda e completa são realizadas em todos os processos, o que pode causar falsos positivos. Adequado para simulações de proteção cibernética e simulações de garantia de eventos importantes. ● **Balanced**: todos os processos são detectados e verificados. A precisão do resultado da detecção e a taxa de detecção anormal do processo são balanceadas. Adequado para proteção de rotina. ● **Conservative**: todos os processos são detectados e verificados. Este modo fornece alta precisão de resultados de detecção e baixos falsos positivos. Adequado para cenários com um grande número de falsos positivos.	Balanced

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Detecção de escalonamento de privilégios raiz

Passo 1 Clique em **Root privilege escalation**.

Passo 2 Na área exibida, modifique as configurações conforme necessário. Para obter mais informações, consulte **Tabela 7-13**.

Figura 7-15 Modificar a política de escalonamento de privilégio raiz

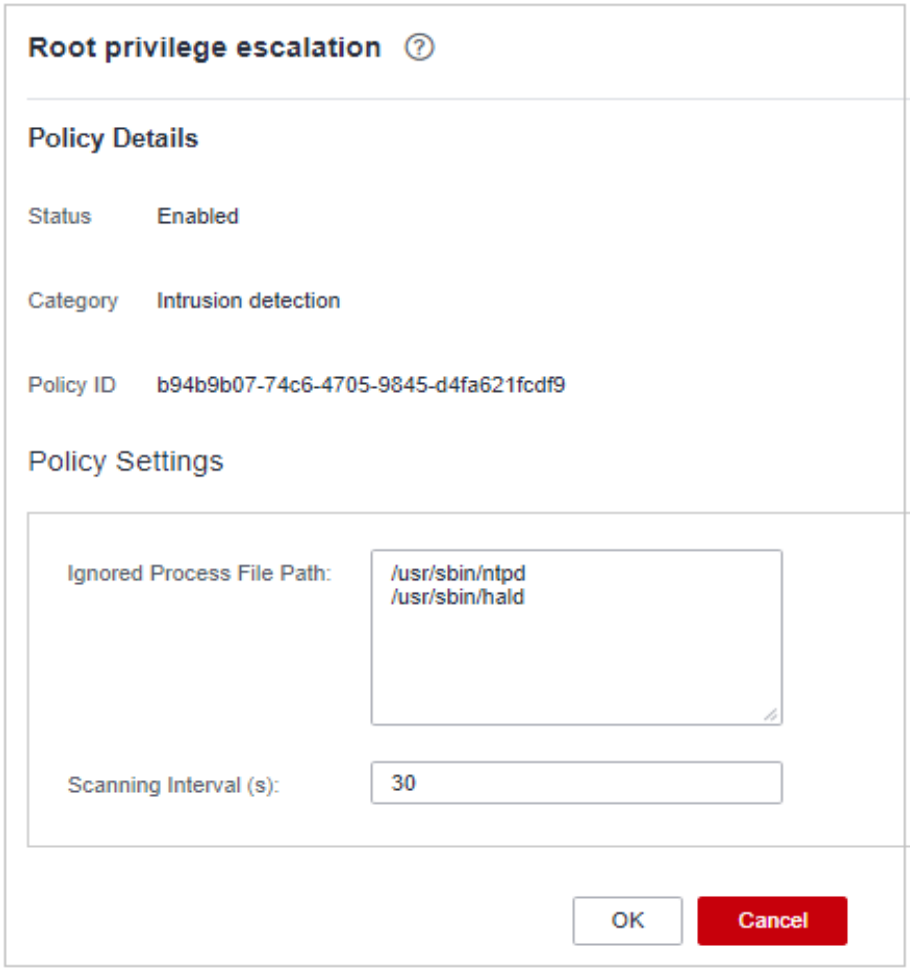


Tabela 7-13 Descrição do parâmetro

Parâmetro	Descrição
Ignored Process File Path	Caminho do arquivo de processo ignorado Começar com uma barra (/) e terminar sem barras (/). Ocupar uma linha separada e não pode conter espaços.
Scanning Interval (s)	Intervalo para verificar os arquivos do processo. O intervalo de valores é de 5 a 3.600.

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Processo em tempo real

Passo 1 Clique em **Real-time Process**.

Passo 2 Na página exibida, modifique as configurações conforme necessário. Para obter mais informações, consulte **Tabela 7-14**.

Figura 7-16 Modificar a política de processos em tempo real

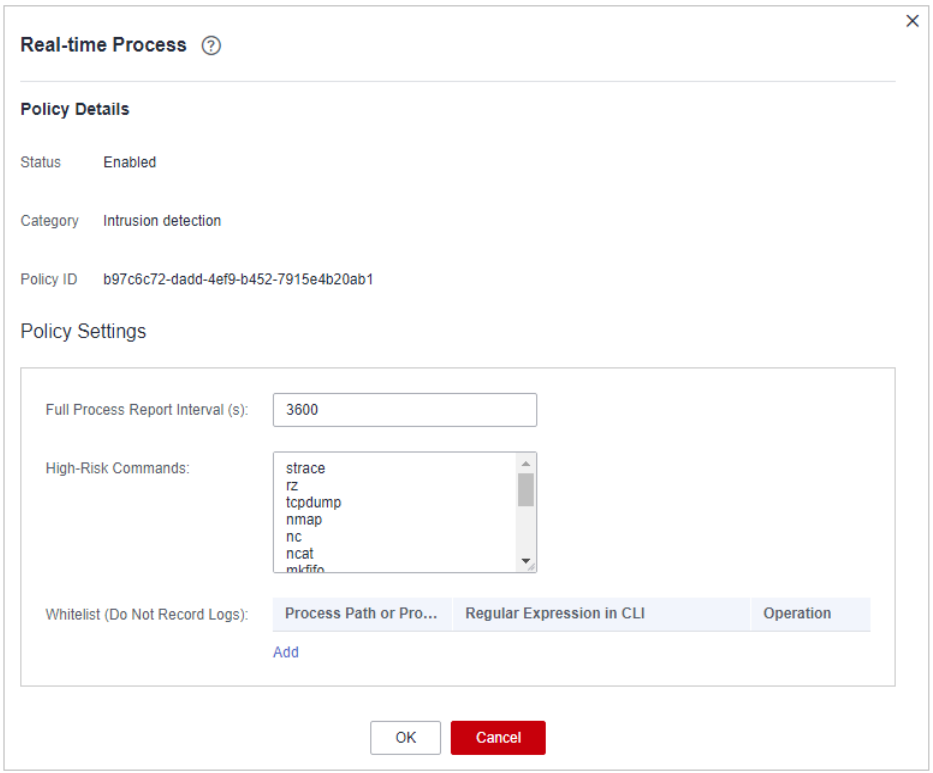


Tabela 7-14 Parâmetros para configurações de política de processo em tempo real

Parâmetro	Descrição
Full Process Report Interval (s)	Intervalo para reportar o processo completo. O intervalo de valores é de 3.600 a 86.400.
High-Risk Commands	Comandos de alto risco que contêm palavras-chave durante a detecção.
Whitelist (Do Not Record Logs)	Adicione caminhos ou nomes de programas que são permitidos ou ignorados durante a detecção.

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Detecção de rootkit

Passo 1 Clique em **Rootkit Detection**.

Passo 2 Na página de detecção de rootkit, modifique o conteúdo da política.

Figura 7-17 Modificar a política de detecção de rootkit

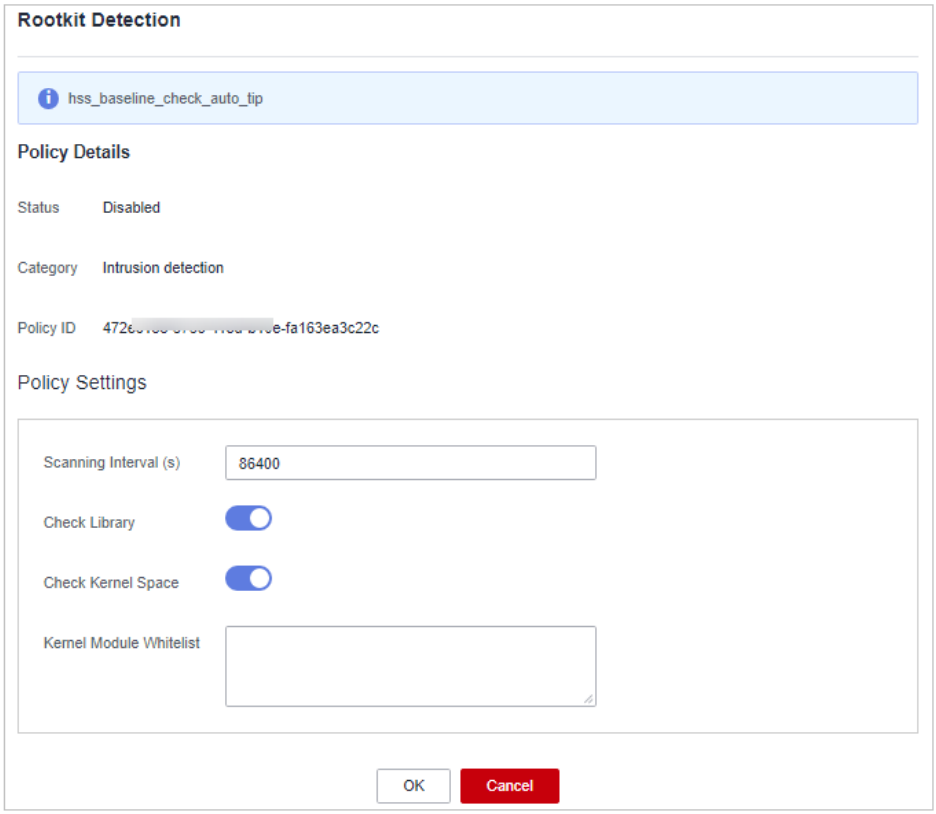


Tabela 7-15 Descrição do parâmetro

Parâmetro	Descrição	Exemplo de valor
Scanning Interval (s)	Intervalo para execução da política de verificação. O valor varia de 60 a 86400.	86400
Check Library	Verificar os arquivos e pastas nas bibliotecas existentes. É aconselhável ativar esta função. ● : ativar ● : desativar	
Check Kernel Space	Executar a verificação pelos módulos do kernel. Todos os módulos do kernel serão verificados. É aconselhável ativar esta função. ● : ativar ● : desativar	
Kernel Module Whitelist	Adicionar os módulos do kernel que podem ser ignorados durante a detecção. Até 10 módulos do kernel podem ser adicionados. Cada módulo ocupa uma linha.	xt_conntrack virtio_scsi tun

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Detecção AV

Passo 1 Clique em **AV Detection**.

Passo 2 No painel deslizante **AV Detection** que é exibido, modifique as configurações conforme necessário. Para mais detalhes, consulte **Tabela 7-16**.

Tabela 7-16 Parâmetros de política de detecção AV

Parâmetro	Descrição	Exemplo de valor
Real-Time Protection	Depois que essa função é ativada, a detecção AV é realizada em tempo real quando a política atual é executada. É aconselhável ativar esta função. ●  : ativar ●  : desativar	
Protected File Type	Tipo dos arquivos a serem verificados em tempo real. ● **All**: selecione todos os tipos de arquivo. ● **Executable**: tipos de arquivos executáveis, como EXE, DLL e SYS. ● **Compressed**: tipos de arquivos compactados, como ZIP, RAR e JAR. ● **Text**: tipos de arquivos de texto como PHP, JSP, HTML e Bash. ● **OLE**: tipos de arquivos compostos, como arquivos do Microsoft Office (PPT e DOC) e arquivos de e-mail salvos (MSG). ● **Other**: tipos de arquivo, exceto os tipos anteriores.	All
Action	Método de manipulação para os alarmes de detecção de objetos. ● **Automated handling**: isolar arquivos de vírus de alto risco por padrão. Relatar outros arquivos de vírus, mas não os isolar. ● **Manual handling**: relatar todos os arquivos de vírus detectados, mas não os isolar. Você precisa lidar com eles manualmente.	Automated handling

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Coleta de informações de container

Passo 1 Clique em **Container Information Collection**.

Passo 2 No painel deslizante **Container Information Collection** exibido, modifique **Policy Settings**. Para obter detalhes sobre os parâmetros, consulte **Tabela 7-17**.

NOTA

A lista branca tem uma prioridade mais alta do que a lista negra. Se um diretório for especificado tanto na lista branca quanto na lista negra, ele será considerado um item na lista branca.

Tabela 7-17 Parâmetros de política de coleta de informações de container

Parâmetro	Descrição	Exemplo de valor
Mount Path Whitelist	Digite o diretório que pode ser montado.	/test/docker or /root/* Observação: se um diretório termina com um asterisco (*), ele indica todos os subdiretórios sob o diretório (excluindo o diretório principal). Por exemplo, se **/var/test/*** for especificado na lista branca, todos os subdiretórios em **/var/test/** serão colocados na lista branca, excluindo o diretório **test**.
Mount Path Blacklist	Insira os diretórios que não podem ser montados. Por exemplo, **user** e **bin**, os diretórios dos principais arquivos de informações do host, não são aconselhados a serem montados. Caso contrário, informações importantes podem ser expostas.	

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Detecção de intrusão de cluster

Passo 1 Clique em **Cluster Intrusion Detection**.

Passo 2 No painel deslizante **Cluster Intrusion Detection** que é exibido, modifique **Policy Settings**. Para obter detalhes sobre os parâmetros, consulte **Tabela 7-18**.

Tabela 7-18 Parâmetros de política de detecção de intrusão de cluster

Parâmetro	Descrição	Exemplo de valor
Basic Detection Cases	Selecione itens de verificação básica conforme necessário.	Selecionar tudo

Parâmetro	Descrição	Exemplo de valor
Whitelist	Você pode personalizar os tipos e valores que precisam ser ignorados durante a detecção. Você pode adicionar e excluir tipos e valores conforme necessário. Os seguintes tipos são suportados: ● Filtro de endereço IP ● Filtro de nome de pod ● Filtro de nome de imagem ● Filtro de usuário ● Filtro de tags de pod ● Filtro de namespace **NOTA** Cada tipo pode ser usado apenas uma vez.	Tipo: IP address filtering Valor: 192.168.x.x

NOTA

Depois que essa política for configurada, você precisará ativar a função de auditoria de logs e implementar o agente do HSS no nó de gerenciamento (nó onde o APIServer está localizado) do cluster para que a política entre em vigor.

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Monitoramento de arquivos de containers

AVISO

Se um caminho de arquivo monitorado estiver sob o caminho de montagem em vez da camada gravável do container no servidor, as alterações no arquivo não poderão acionar alarmes de modificação do arquivo do container. Para proteger esses arquivos, configure uma **política de proteção de arquivos**.

Passo 1 Clique em **Container File Monitoring**.

Passo 2 No painel deslizante **Container File Monitoring** que é exibido, modifique **Policy Settings**. Para obter detalhes sobre os parâmetros, consulte **Tabela 7-19**.

Tabela 7-19 Parâmetros de política de monitoramento de arquivos de container

Parâmetro	Descrição	Exemplo de valor
Fuzzy match	Indica se deve ser ativada a correspondência difusa para o arquivo de destino. É aconselhável selecionar esta opção.	Selecionado
Block New Executable	Monitorar o comportamento da adição de arquivos executáveis. Se esta opção estiver selecionada, a adição de arquivos executáveis é proibida. É aconselhável selecionar esta opção.	Selecionado
Image Name	Nome da imagem de destino a ser verificada	test_bj4
Image ID	ID da imagem de destino a ser verificada	-
File	Nome do arquivo na imagem de destino a ser verificada	/tmp/testw.txt

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Lista branca de processos de containers

Passo 1 Clique em **Container Process Whitelist**.

Passo 2 No painel deslizante **Container Process Whitelist** exibido, modifique **Policy Settings**. Para obter detalhes sobre os parâmetros, consulte **Tabela 7-20**.

Tabela 7-20 Parâmetros de política da lista branca do processo de container

Parâmetro	Descrição	Exemplo de valor
Fuzzy Match	Indica se deve ser ativada a correspondência difusa para o arquivo de destino. É aconselhável selecionar esta opção.	Selecionado
Image Name	Nome da imagem de destino a ser detectada	test_bj4
Image ID	ID da imagem de destino a ser verificada	-
Process	Caminho do arquivo na imagem de destino a ser verificado	/tmp/testw

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Comportamentos suspeitos de imagem

Passo 1 Clique em **Suspicious Image Behaviors**.

Passo 2 No painel deslizante **Suspicious Image Behaviors** exibido, modifique **Policy Settings**. Para obter detalhes sobre os parâmetros, consulte **Tabela 7-21**.

Tabela 7-21 Parâmetros de política de comportamentos de imagem suspeitos

Parâmetro	Descrição	Exemplo de valor
Rule Name	Nome de uma regra	-
Description	Breve descrição de uma regra	-
Template	● Configure modelos com base em regras diferentes. As regras suportadas são as seguintes: – Image whitelist – Image blacklist – Image tag whitelist – Image tag blacklist – Create container whitelist – Create container blacklist – Container mount proc whitelist – Container seccomp unconfined – Container privilege whitelist – Container capability whitelist ● Os parâmetros são descritos a seguir: – **Exact match**: digite os nomes das imagens que você deseja verificar. Use ponto-e-vírgula (;) para separar vários nomes. No máximo 20 nomes podem ser inseridos. – **RegEx match**: use expressões regulares para combinar imagens. Use ponto-e-vírgula (;) para separar várias expressões. Um máximo de 20 expressões podem ser inseridas. – **Prefix match**: digite os prefixos das imagens que você deseja verificar. Vários prefixos são separados por ponto e vírgula (;). Um máximo de 20 prefixos podem ser inseridos. – **Tag Name**: digite a tag e o valor das imagens que você deseja verificar. Um máximo de 20 tags podem ser adicionadas. – **Permission Type**: especifique as permissões a serem verificadas ou ignoradas. Para obter detalhes sobre permissões, consulte **Tabela 7-22**.	-

Tabela 7-22 Permissões de imagens anormais

Nome de permissões	Descrição
AUDIT_WRITE	Gravar registros no log de auditoria do kernel.
CHOWN	Fazer alterações arbitrárias nos UIDs e GIDs de arquivos.
DAC_OVERRIDE	Ignorar a leitura, gravação e execução de verificações de permissão de arquivo.
FOWNER	Ignorar verificações de permissão em operações que normalmente exigem que o UID do sistema de arquivos do processo corresponda ao UID do arquivo.
FSETID	Não limpar os bits de permissões set-user-ID e set-group-ID quando um arquivo for modificado.
KILL	Ignorar verificações de permissão para enviar sinais
MKNOD	Criar arquivos especiais usando mknod.
NET_BIND_SERVICE	Vincular um soquete a portas privilegiadas de domínio da Internet (números de porta inferiores a 1024).
NET_RAW	Usar soquetes RAW e PACKET.
SETFCAP	Definir as capacidades do arquivo.
SETGID	Fazer manipulações arbitrárias de GIDs de processo e lista de GIDs suplementares.
SETPCAP	Modificar as capacidades do processo.
SETUID	Fazer manipulações arbitrárias de UIDs de processo.
SYS_CHROOT	Usar chroot para alterar o diretório raiz.
AUDIT_CONTROL	Ativar e desativar a auditoria do kernel; alterar regras de filtragem de auditoria; recuperar status de auditoria e regras de filtragem.
AUDIT_READ	Permitir a leitura de logs de auditoria via soquete de netlink multicast.
BLOCK_SUSPEND	Permitir a prevenção da suspensão.
BPF	Permitir a criação de mapas BPF, carregar dados de BPF Type Format (BTF), recuperar código JITed de programas BPF e muito mais.
CHECKPOINT_RESTORE	Permitir operações relacionadas a pontos de verificação e restauração.
DAC_READ_SEARCH	Ignorar verificações de permissão de leitura de arquivos e verificações de permissão de leitura e execução de diretórios.
IPC_LOCK	Bloquear memória (como mlock, mlockall, mmap e shmctl).

Nome de permissões	Descrição
IPC_OWNER	Ignorar verificações de permissão para operações em objetos de System V IPC.
LEASE	Estabelecer locações em arquivos arbitrários
LINUX_IMMUTABLE	Definir os sinalizadores de i-node FS_APPEND_FL e FS_IMMUTABLE_FL.
MAC_ADMIN	Permitir mudanças de configuração ou estado do MAC.
MAC_OVERRIDE	Substituir o Controle de acesso obrigatório (MAC).
NET_ADMIN	Executar várias operações relacionadas à rede.
NET_BROADCAST	Fazer transmissões de soquete e ouvir multicasts.
PERFMON	Permitir operações privilegiadas de desempenho e observabilidade do sistema usando perf_events, i915_perf e outros subsistemas do kernel.
SYS_ADMIN	Executar uma série de operações de administração do sistema.
SYS_BOOT	Usar reinicialização e kexec_load. Reinicializar e carregar um novo kernel para execução posterior.
SYS_MODULE	Carregar e descarregar módulos do kernel.
SYS_NICE	Aumentar o valor nice do processo (nice, definir prioridade) e alterar o valor nice para processos arbitrários.
SYS_PACCT	Ativar ou desativar a contabilidade do processo.
SYS_PTRACE	Rastrear processos arbitrários usando ptrace.
SYS_RAWIO	Executar operações de porta I/O (ipl e ioperm).
SYS_RESOURCE	Substituir limites de recursos.
SYS_TIME	Ajustar o relógio do sistema (settimeofday, stime e adjtimex) e o relógio em tempo real (hardware).
SYS_TTY_CONFIG	Usar o vhangup. Empregar várias operações ioctl privilegiadas em terminais virtuais.
SYSLOG	Executar operações de syslog privilegiadas.
WAKE_ALARM	Acionar algo que despertará o sistema.

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Detecção de verificação de porta

Passo 1 Clique em **Port Scan Detection**.

Passo 2 No painel deslizante **Port Scan Detection** exibido, modifique **Policy Settings**. Para obter detalhes sobre os parâmetros, consulte **Tabela 7-23**.

Tabela 7-23 Parâmetros de política de detecção de verificação de porta

Parâmetro	Descrição	Exemplo de valor
Process Information Collection Interval (s):	Intervalo para obtenção de processos	Selecionado
Source IP Address Whitelist	Insira a lista branca de endereços IP. Separe vários endereços IP com ponto e vírgula (;).	test_bj4
Packet Quantity Threshold	-	-
Ports to Scan	Detalhes sobre o número da porta e o tipo de protocolo a ser detectado	-

Passo 3 Confirme as informações e clique em **OK**.

----Fim

Autoproteção

A política de autoproteção protege o software, os processos e os arquivos do HSS de serem danificados por programas maliciosos. Não é possível personalizar o conteúdo da política.

7.2 Visualização do histórico de tratamento

Você pode verificar o histórico de tratamento de vulnerabilidades e alarmes, incluindo seus manipuladores e tempo de tratamento.

Restrições

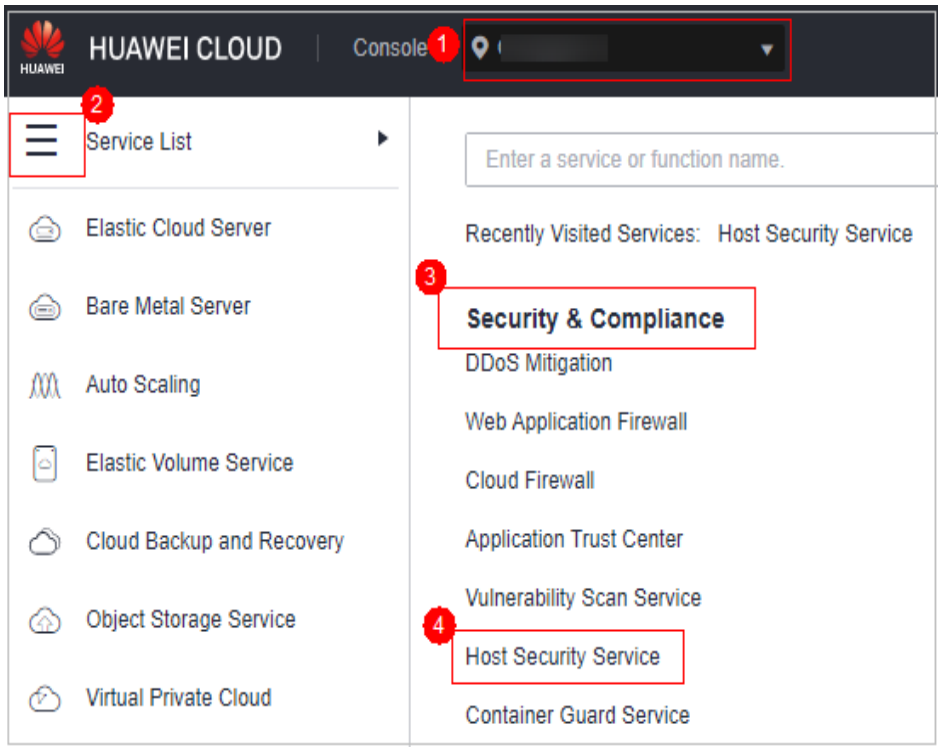
A edição básica não suporta esta função. Para obter detalhes sobre como comprar e atualizar o HSS, consulte **Compra de uma cota do HSS** e **Atualização de sua edição**.

Visualização do histórico de tratamento de todas as 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 7-18 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Security Operations** > **Handling History**. A página **Handling History** é exibida.

Passo 4 Na página de guia **Vulnerabilities** exibida, visualize o histórico de tratamento de todas as vulnerabilidades.

- Visualização do histórico de tratamento de vulnerabilidades de um projeto empresarial especificado

  No canto superior esquerdo da página **Handling History**, selecione um projeto empresarial para **Enterprise Project** para visualizar o histórico de tratamento de vulnerabilidades do servidor no projeto empresarial.

- Visualização do histórico de tratamento de vulnerabilidades de uma propriedade especificada

  Na caixa de pesquisa acima da lista de histórico de tratamento de vulnerabilidades, digite um tipo de vulnerabilidade, nome de vulnerabilidade ou endereço IP do servidor e clique em para visualizar o histórico de tratamento de vulnerabilidades de uma propriedade especificada.

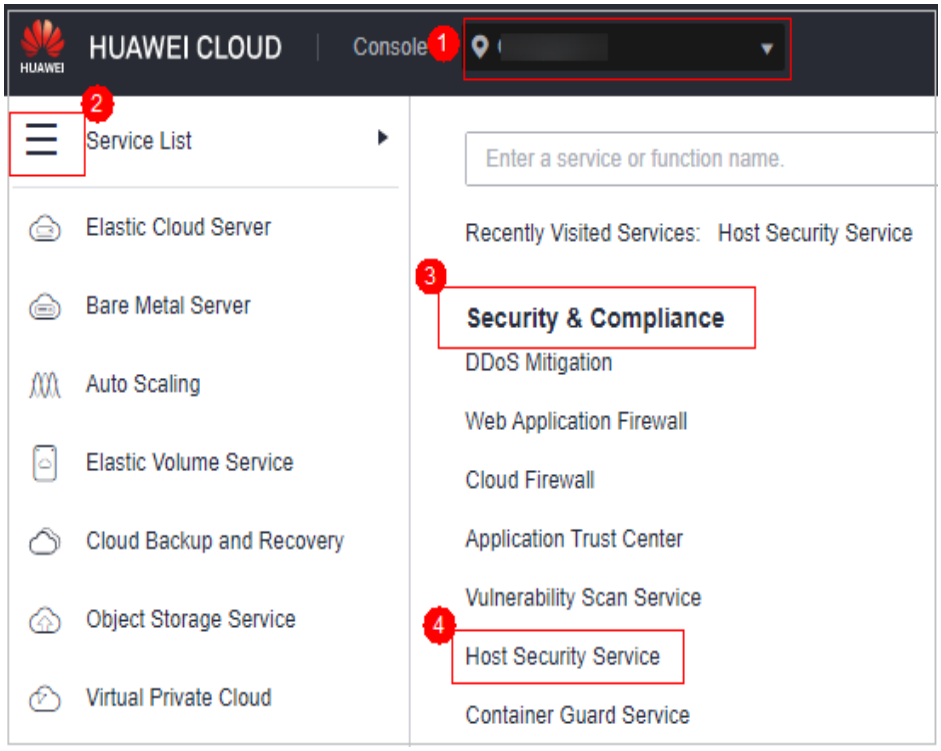
----Fim

Verificação do histórico de tratamento de alarmes

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 7-19 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Security Operations** > **Handling History**.

Passo 4 Clique na guia **Alarms** e visualize o histórico de tratamento de alarmes.

- Verificação do histórico de tratamento de alarmes em um projeto empresarial

  No canto superior esquerdo da página **Handling History**, selecione um projeto empresarial e verifique o histórico de tratamento de alarmes do servidor no projeto.
- Verificação do histórico de tratamento de alarmes com atributos especificados

  Na caixa de pesquisa acima da lista de alarmes, digite um nome de alarme, gravidade do alarme e ID de ataque e clique em para procurar os alarmes que atendam aos critérios especificados.

----Fim

8 Relatório de segurança

8.1 Relatório de segurança

8.1.1 Verificação de um relatório de segurança

Você pode assinar relatórios **diários**, semanais, mensais e **personalizados**, que são armazenados por seis meses. Os relatórios mostram as tendências de segurança do servidor e os principais eventos e riscos de segurança.

NOTA

- Se você habilitou a função de projeto empresarial, pode selecionar seu projeto empresarial na lista suspensa **Enterprise project** e assinar o relatório de segurança do projeto. Você também pode selecionar **All projects** e assinar o relatório de segurança dos servidores em todos os projetos dessa região.
- Depois de assinar um relatório, ele estará disponível para revisão e download no dia seguinte.

Restrições

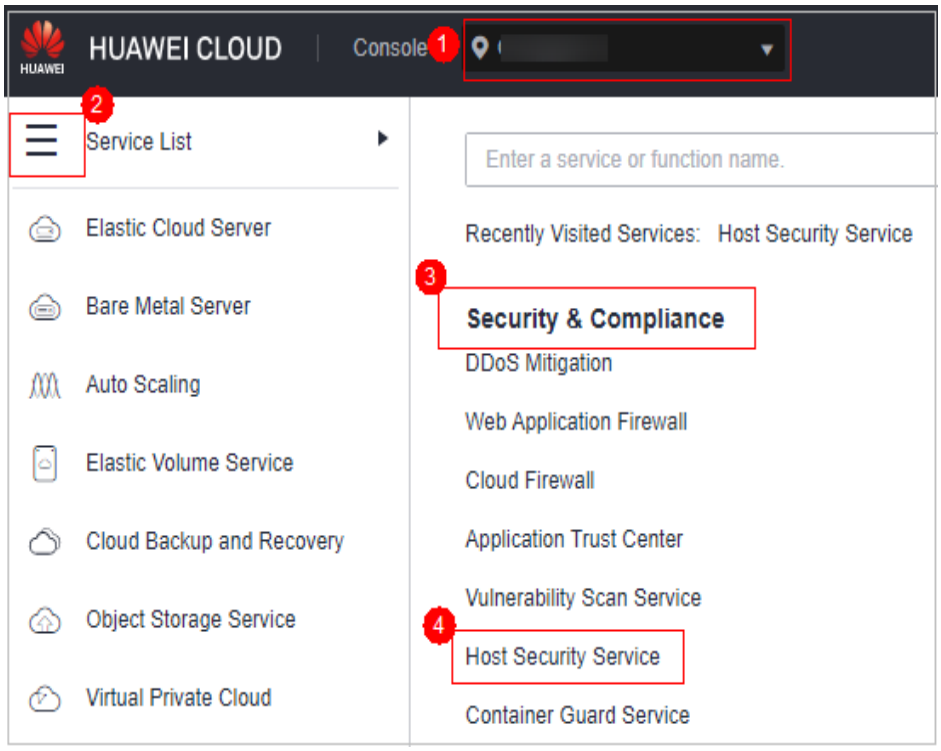
A edição empresarial e as edições superiores suportam operações relacionadas a relatórios de segurança.

Visão geral do relatório de segurança

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



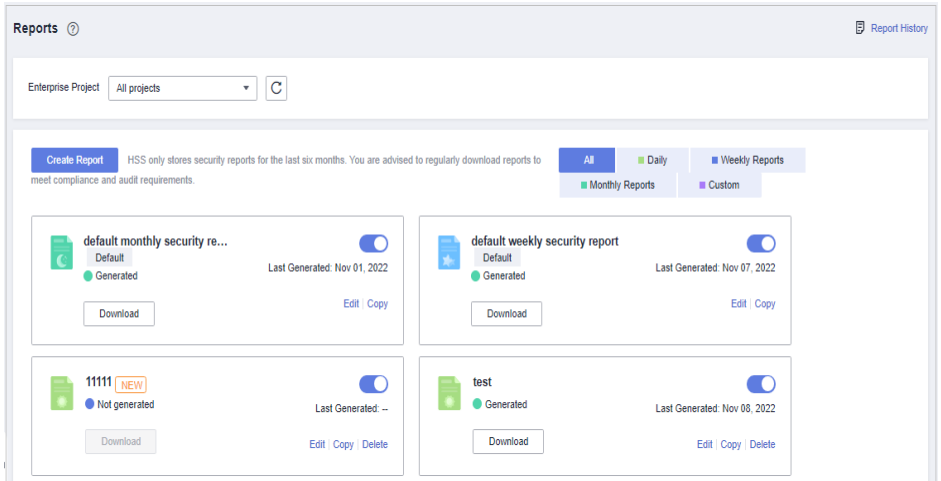
Passo 3 No painel de navegação à esquerda, escolha **Reports**. A página de visão geral do relatório de segurança é exibida.

Você pode usar os modelos de relatório de segurança padrão diretamente, que são **default monthly security report** e **default weekly security report**.

NOTA

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

Figura 8-2 Verificação de um relatório de segurança



Passo 4 Clique em **Download** para ir para a página de visualização. Você pode verificar as informações do relatório de destino e baixá-lo ou enviá-lo.

Figura 8-3 Visualização de um relatório

----Fim

Verificação do histórico do relatório

O histórico do relatório armazena os detalhes de envio do relatório.

Passo 1 No canto superior direito da página de visão geral do relatório de segurança, clique em **Report History** para verificar os registros de envio de relatórios.

Passo 2 Verifique o histórico do relatório na página exibida, como mostrado na figura a seguir. Para obter mais informações, consulte **Tabela 8-1**.

Figura 8-4 Detalhes de envio de relatórios

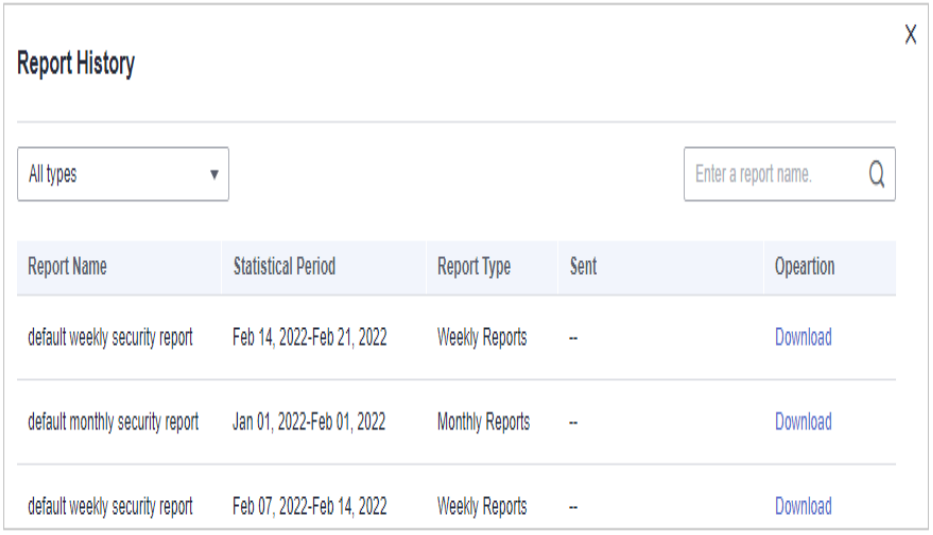


Tabela 8-1 Descrição do parâmetro

Parâmetro	Descrição
Report Name	Nome de um relatório enviado.

Parâmetro	Descrição
Statistical Period	Período estatístico de um relatório enviado.
Report Type	Tipo de período estatístico de um relatório enviado. ● Relatórios semanais ● Relatórios mensais ● Relatórios diários ● Relatórios personalizados
Sent	Hora em que o relatório é enviado.

Passo 3 Clique em **Download** na coluna **Operation** para verificar os relatórios históricos. Você também pode visualizar e baixar os relatórios.

----Fim

8.1.2 Assinatura de um relatório de segurança

Esta seção fornece orientação para você assinar rapidamente relatórios de segurança semanais ou mensais usando modelos predefinidos no console. Para obter detalhes sobre como personalizar um relatório de segurança, consulte **Criação de um relatório de segurança**.

Restrições

A edição empresarial e as edições superiores suportam operações relacionadas a relatórios de segurança.

Precaução

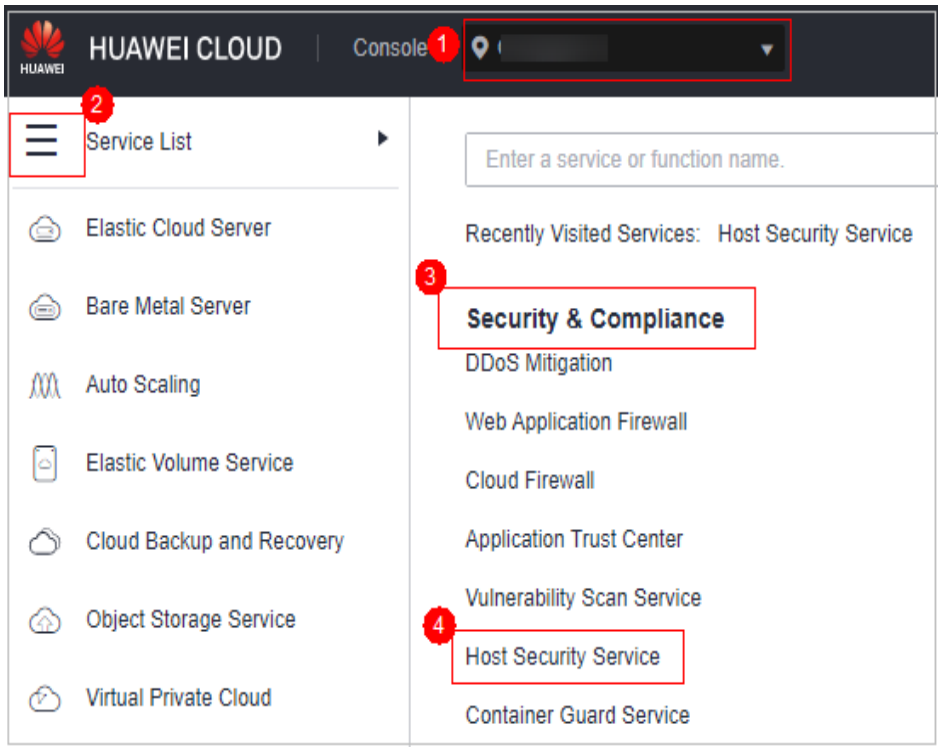
- Um relatório de segurança é gerado para todos os servidores protegidos. Não é possível especificar um servidor e gerar um relatório de segurança para ele.
- A assinatura de relatórios de segurança é gratuita, mas o conteúdo do relatório varia dependendo da edição de cota que você usa.

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 8-5 Acessar o HSS



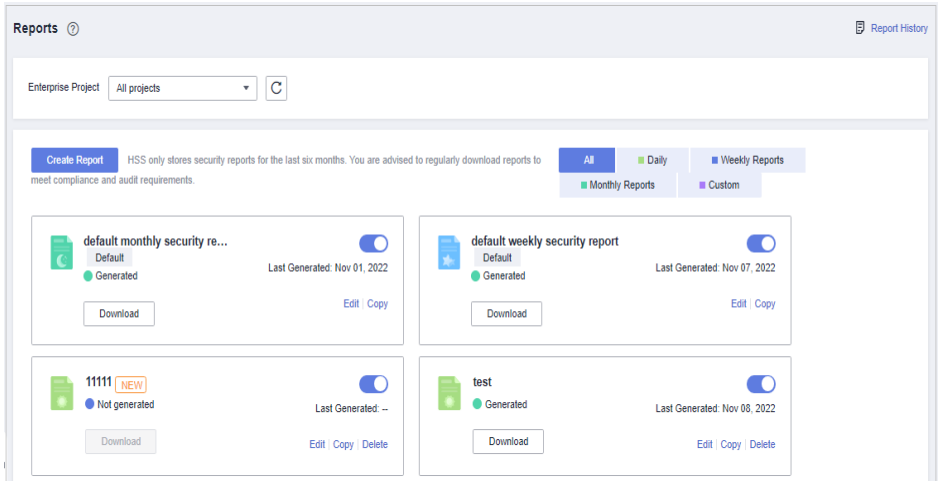
Passo 3 No painel de navegação à esquerda, escolha **Reports**. A página de visão geral do relatório de segurança é exibida.

Você pode usar os modelos de relatório de segurança padrão diretamente, que são **default monthly security report** e **default weekly security report**.

NOTA

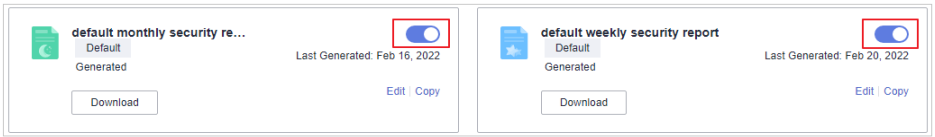
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figura 8-6 Verificação de um relatório de segurança



Passo 4 Você pode assinar relatórios de segurança mensais ou semanais. Para obter detalhes sobre como editar um relatório, consulte **Editar um relatório**.

Figura 8-7 Ativar relatórios de segurança



----Fim

8.1.3 Criação de um relatório de segurança

Se o tipo e o conteúdo do modelo de relatório existente não puderem atender aos seus requisitos, você poderá personalizar um relatório.

Restrições

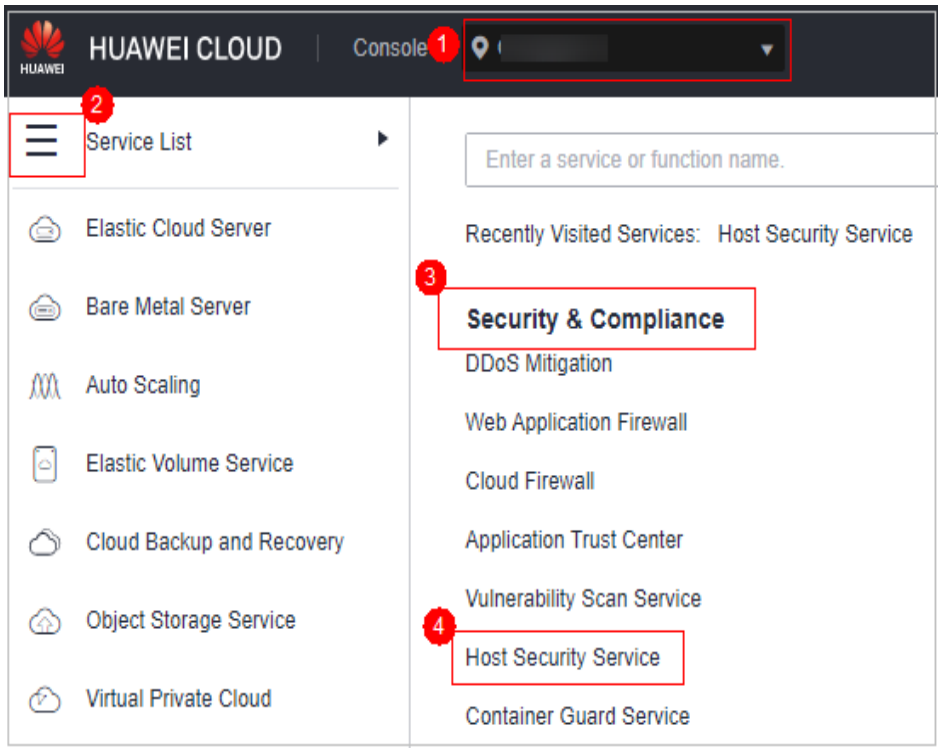
A edição empresarial e as edições superiores suportam operações relacionadas a relatórios de segurança.

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 8-8 Acessar o HSS



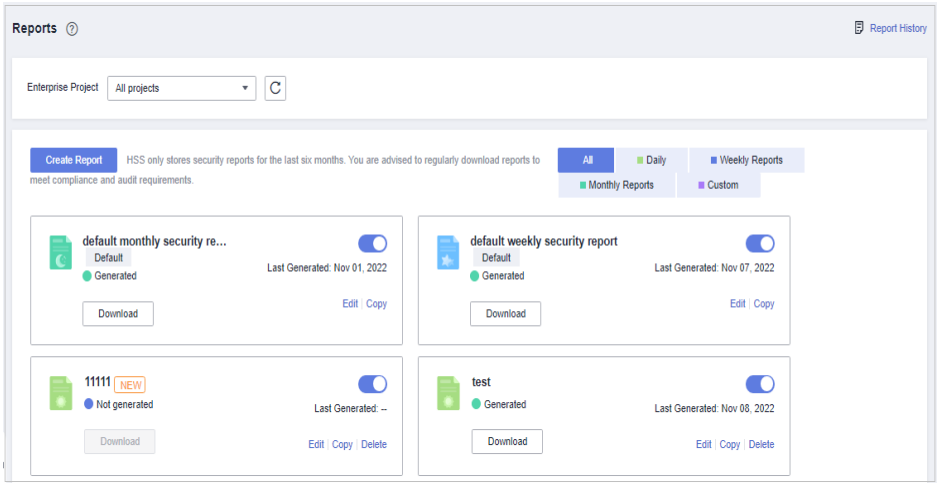
Passo 3 No painel de navegação à esquerda, escolha **Reports**. A página de visão geral do relatório de segurança é exibida.

Você pode usar os modelos de relatório de segurança padrão diretamente, que são **default monthly security report** e **default weekly security report**.

NOTA

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

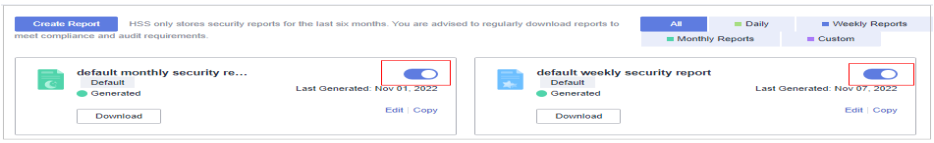
Figura 8-9 Verificação de um relatório de segurança



Passo 4 Crie um relatório.

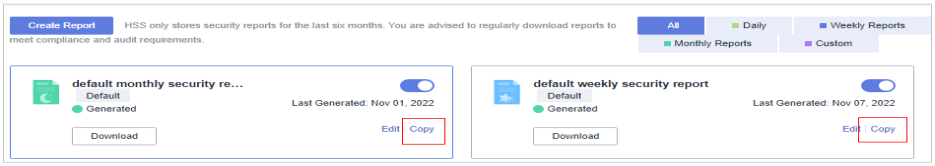
- Crie um relatório de segurança mensal ou semanal com base em modelos.
  - Clique em **Copy** no boletim semanal ou mensal para acessar a página de configuração de informações básicas.

Figura 8-10 Criação de um relatório com base em um modelo



- Você também pode personalizar o período do relatório.
  - Clique em **Create Report** para acessar a página de configuração de informações básicas.

Figura 8-11 Personalizar um relatório



Passo 5 Edite informações básicas de um relatório. Para obter mais informações, consulte **Tabela 8-2**.

Figura 8-12 Editar informações básicas de um relatório

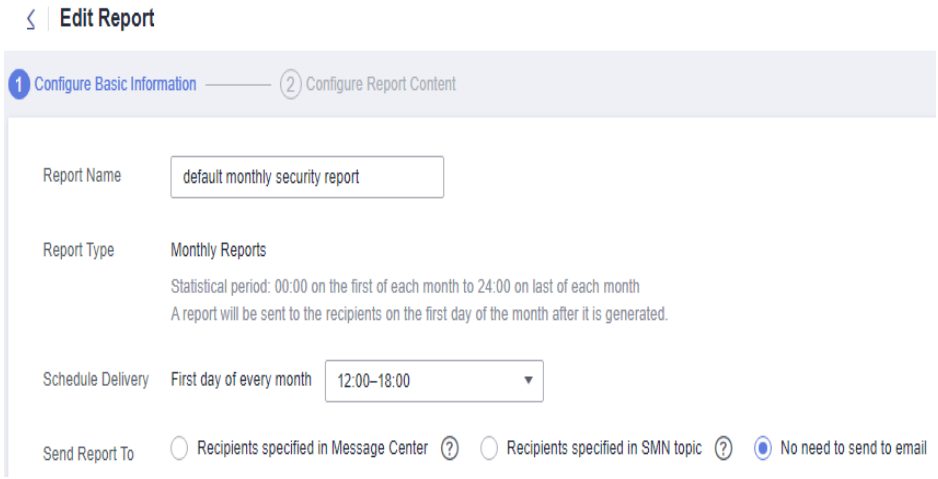


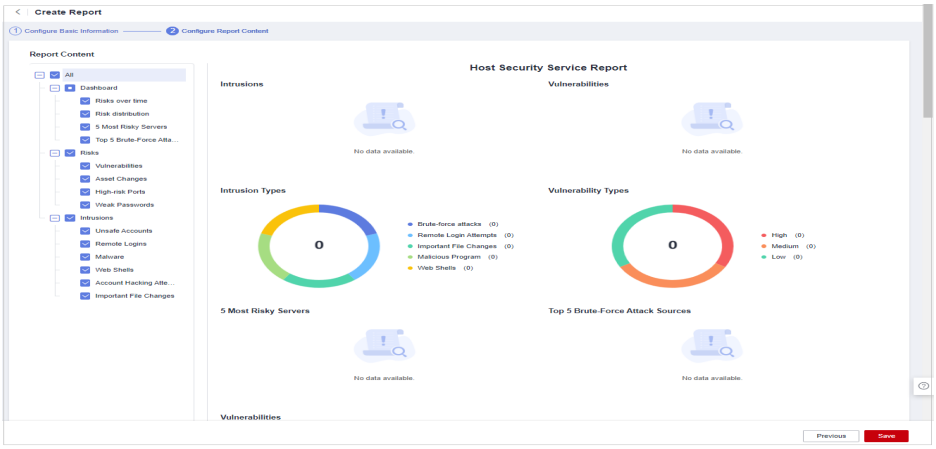
Tabela 8-2 Descrição do parâmetro

Parâmetro	Descrição	Exemplo de valor
Report Name	Nome padrão do relatório	ecs security report
Report Type	Tipo de período estatístico de um relatório: ● **Daily**: 00:00 às 24:00 todos os dias ● **Weekly Reports**: 00:00 de segunda-feira a 24:00 de domingo ● **Monthly Reports**: 00:00 do primeiro dia às 24:00 do último dia de cada mês ● **Custom**: período estatístico personalizado, que varia de um dia a três meses ● Todos os tipos de relatórios serão enviados aos destinatários no dia seguinte à sua geração.	Monthly Reports
Schedule Delivery	Hora em que um relatório é enviado automaticamente	-

Parâmetro	Descrição	Exemplo de valor
Send Report To	Destinatários do relatório de segurança. ● **Recipients specified in Message Center**: se você usar as configurações de Central de mensagens, as notificações de alarme serão enviadas aos destinatários especificados no tipo de mensagem de **Security events**. Você precisa fazer logon no console e verificar a caixa de correio no canto superior direito. ● **Recipients specified in SMN topic**: se você usar as configurações de tópico do SMN, poderá criar um tópico e especificar destinatários para o HSS. ● **No need to send to email**: o relatório não é enviado para o endereço de e-mail especificado.	Recipients specified in SMN topic

Passo 6 Depois de confirmar que as informações estão corretas, clique em **Next** no canto inferior direito da página para configurar o relatório.

Figura 8-13 Configurar um relatório



Passo 7 Selecione os itens de relatório a serem gerados no painel esquerdo. Você pode visualizar os itens de relatório no painel direito. Depois de confirmar os itens do relatório, clique em **Save** e habilite a assinatura do relatório de segurança.

----Fim

8.1.4 Gerenciamento de um relatório de segurança

Esta seção descreve como modificar, cancelar ou desativar um relatório assinado.

Restrições

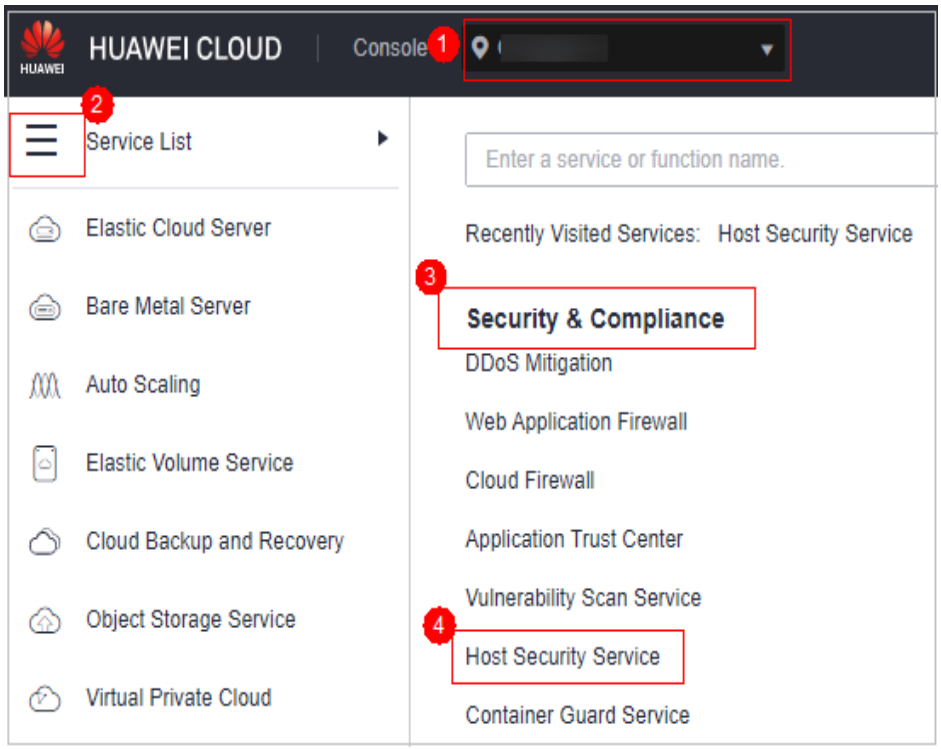
A edição empresarial e as edições superiores suportam operações relacionadas a relatórios de segurança.

Editar um relatório

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 8-14 Acessar o HSS



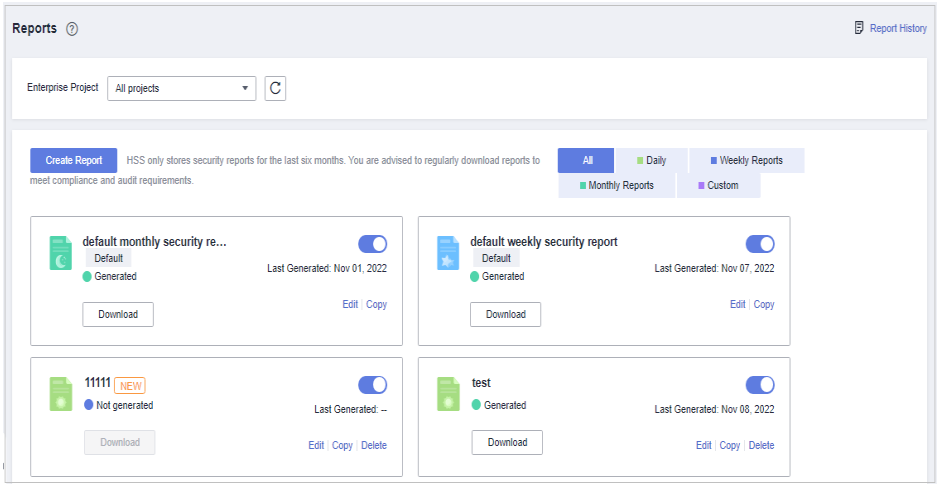
Passo 3 No painel de navegação à esquerda, escolha **Reports**. A página de visão geral do relatório de segurança é exibida.

Você pode usar os modelos de relatório de segurança padrão diretamente, que são **default monthly security report** e **default weekly security report**.

NOTA

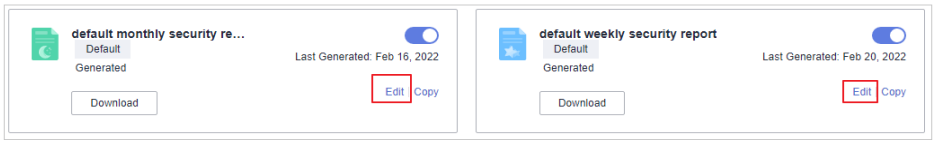
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figura 8-15 Verificação de um relatório de segurança



Passo 4 Clique em **Edit** no canto inferior direito do relatório de destino.

Figura 8-16 Editar um relatório



Passo 5 Edite informações básicas de um relatório. Para obter mais informações, consulte **Tabela 8-3**.

Figura 8-17 Editar informações básicas de um relatório

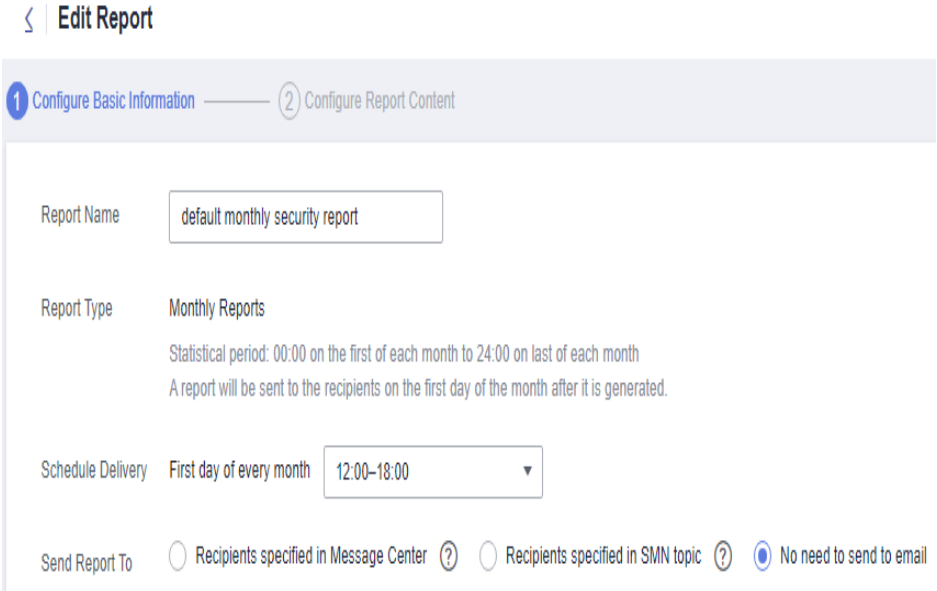
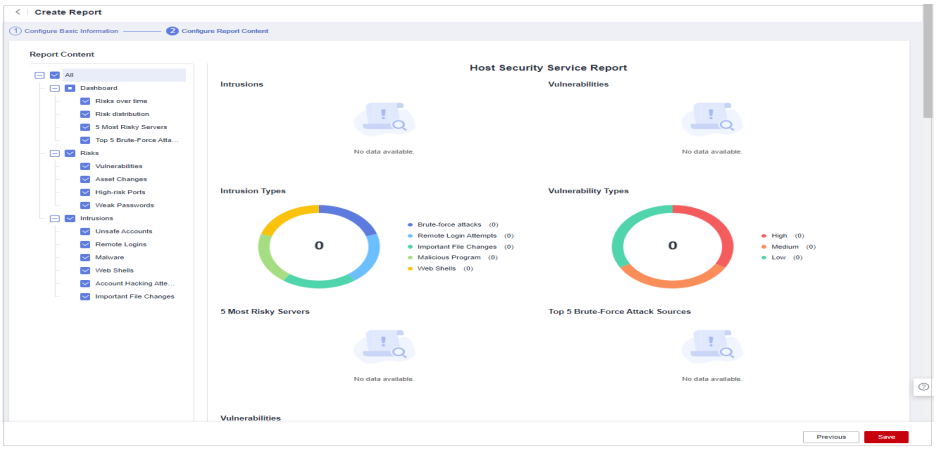


Tabela 8-3 Descrição do parâmetro

Parâmetro	Descrição	Exemplo de valor
Report Name	Nome do relatório padrão.	**default monthly security report**
Report Type	Nome do tipo de período estatístico de um relatório, que não pode ser editado.	**Monthly Reports**
Schedule Delivery	Hora em que um relatório é enviado automaticamente.	-
Send Report To	Modo para enviar os relatórios de segurança gerados: ● **Recipients specified in Message Center**: se você usar as configurações de Central de mensagens, as notificações de alarme serão enviadas aos destinatários especificados no tipo de mensagem de **Security events**. Você precisa fazer logon no console e verificar a caixa de correio no canto superior direito. ● **Recipients specified in SMN topic**: se você usar as configurações de tópico do SMN, poderá criar um tópico e especificar destinatários para o HSS. ● **No need to send to email**: o relatório não é enviado para o endereço de e-mail especificado.	Recipients specified in SMN topic

Passo 6 Confirme as informações e clique em **Next** no canto inferior direito da página para configurar o relatório.

Figura 8-18 Configurar um relatório



Passo 7 Selecione ou desmarque os itens de relatório no painel à esquerda. Você pode visualizar os itens do relatório à direita. Depois de confirmar os itens do relatório, clique em **Save**. O relatório foi alterado com sucesso.

----Fim

Cancelamento da assinatura de um relatório

Passo 1 Faça logon no console de gerenciamento do HSS.

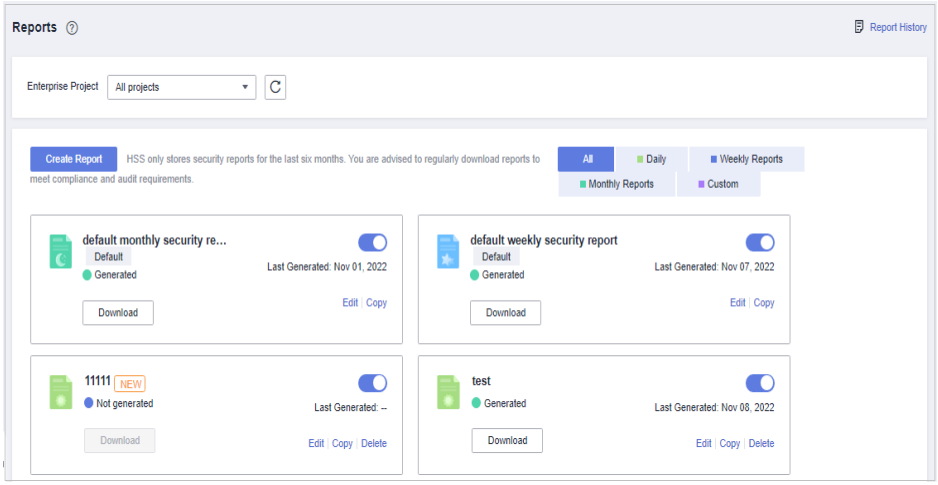
Passo 2 No painel de navegação à esquerda, escolha **Reports**. A página de visão geral do relatório de segurança é exibida.

Você pode usar os modelos de relatório de segurança padrão diretamente, que são **default monthly security report** e **default weekly security report**.

NOTA

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

Figura 8-19 Verificação de um relatório de segurança



Passo 3 Desative o relatório de destino ( ).

----Fim

Excluir um relatório

NOTA

Modelos de relatório de segurança padrão **default monthly security report** e **default weekly security report** não podem ser excluídos.

Passo 1 Faça logon no console de gerenciamento do HSS.

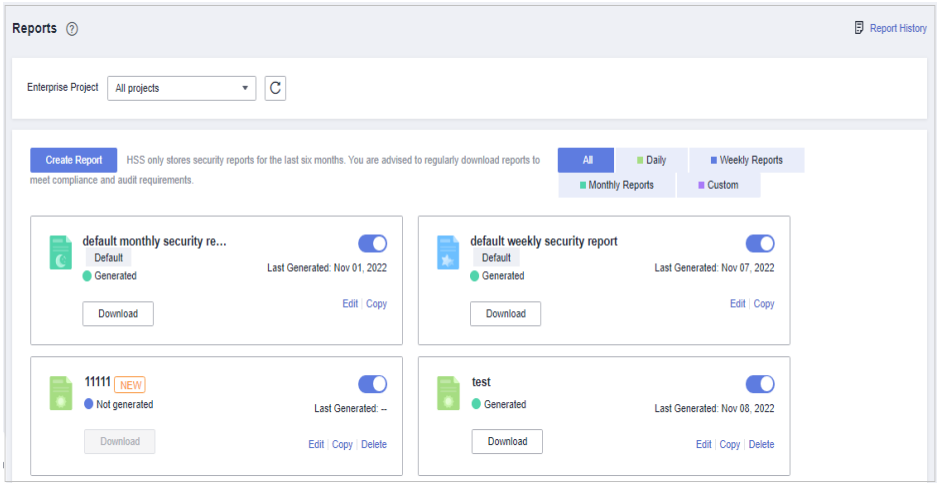
Passo 2 No painel de navegação à esquerda, escolha **Reports**. A página de visão geral do relatório de segurança é exibida.

Você pode usar os modelos de relatório de segurança padrão diretamente, que são **default monthly security report** e **default weekly security report**.

NOTA

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

Figura 8-20 Verificação de um relatório de segurança



Passo 3 Clique em **Delete** no canto inferior direito do relatório de destino.

----Fim

8.2 Verificação gratuita em servidores desprotegidos

Os servidores que não são protegidos pelo HSS são verificados gratuitamente. Um relatório de segurança sobre suas vulnerabilidades, senhas inseguras e riscos de ativos será gerado.

Se você precisar executar verificação de linha de base, proteção de aplicações, proteção contra adulteração na Web, proteção contra ransomware, detecção de intrusões, gerenciamento de políticas, detecção de integridade de arquivos e isolamento e eliminação, você pode **ativar o HSS**.

Verificação gratuita

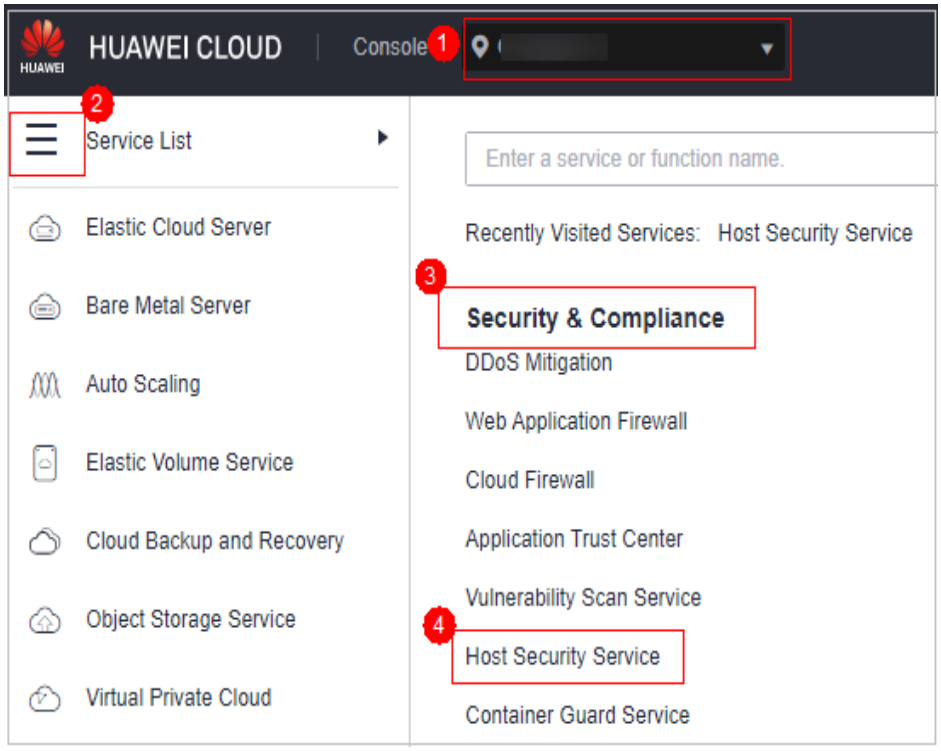
- Os servidores que não são protegidos pelo HSS são verificados gratuitamente no início da manhã de cada segunda-feira.
- Um relatório de verificação de integridade gratuito é gerado no primeiro dia de cada mês. Você só pode visualizar o relatório on-line, mas não pode baixá-lo.
- No relatório, até cinco resultados podem ser exibidos para cada item de verificação. Se um item de verificação tiver menos de cinco resultados, apenas metade deles será exibida.
- Você pode comprar o HSS para desfrutar de funções avançadas, como proteção em tempo real, download de relatórios, correção de vulnerabilidades on-line e assistência de conformidade.

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 8-21 Acessar o HSS

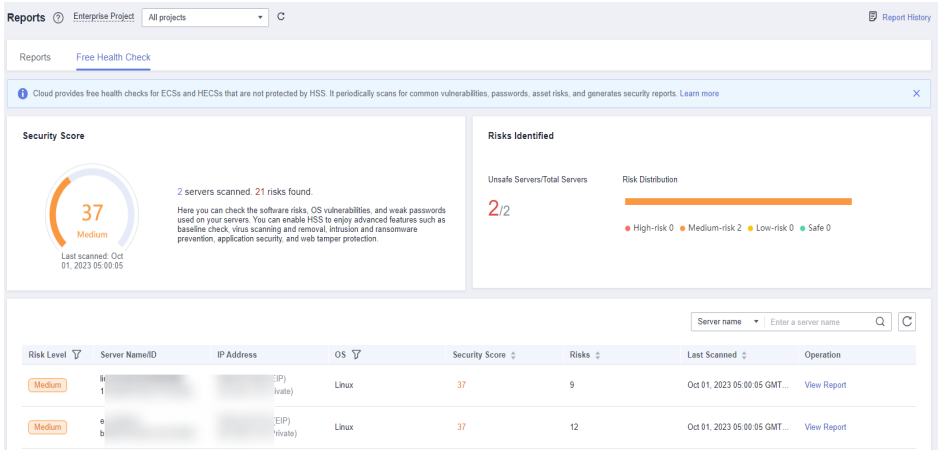


Passo 3 Escolha **Reports** e clique na guia **Free Health Check**. Verifique as estatísticas dos ativos que não estão protegidos.

NOTA

Somente servidores desprotegidos são exibidos nesta página.

Figura 8-22 Verificação de integridade gratuita



Passo 4 Na coluna **Operation** de um servidor, clique em **View Report** para visualizar o relatório de verificação de integridade on-line.

----Fim

9 Instalação e configuração

9.1 Gerenciamento do agente

9.1.1 Visualização do gerenciamento de agente

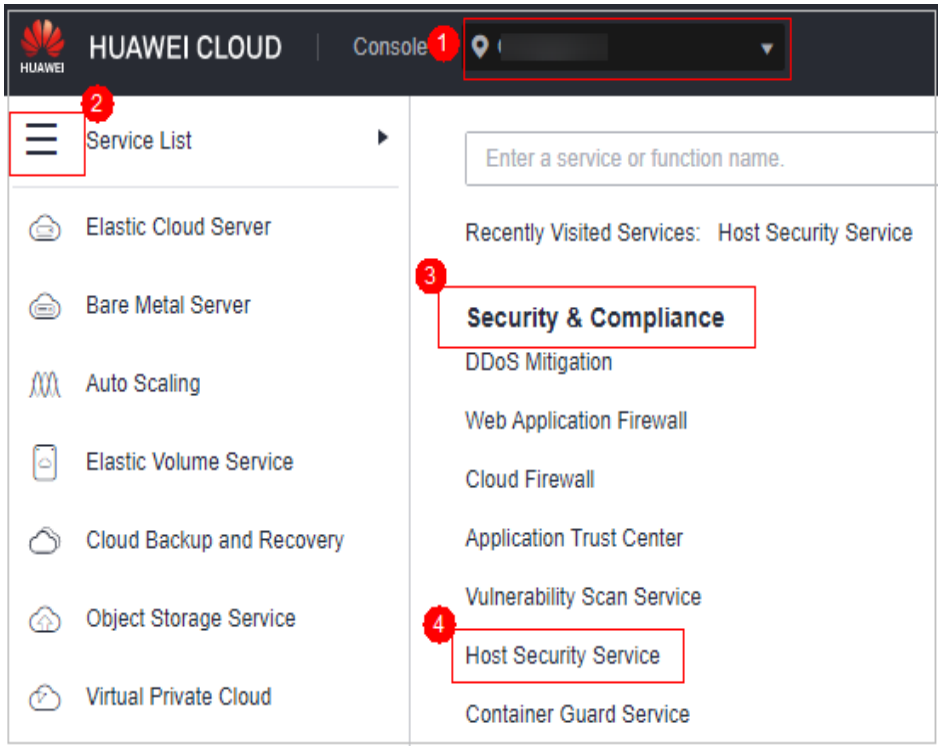
Você pode classificar servidores, verificar se o agente está instalado neles e pode instalar ou desinstalar o agente. No console, você pode encontrar as instruções de instalação do agente e o link para o pacote do agente.

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 9-1 Acessar o HSS

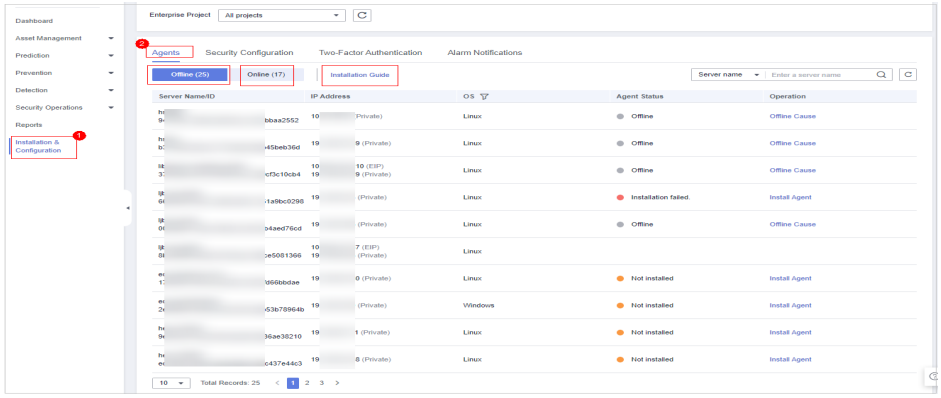


Passo 3 No painel de navegação, escolha **Installation & Configuration**. Clique na guia **Agents**.

NOTA

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

Figura 9-2 Acessar a página de gerenciamento do agente



Passo 4 Clique em **Offline** para verificar os servidores nos quais o agente não está instalado ou está off-line. Clique em **Online** para verificar os servidores em que o agente está on-line.

Passo 5 Clique em **Installation Guide** para verificar o guia de instalação do agente.

Passo 6 Clique em **Agent Version Information** para visualizar a versão mais recente, as versões anteriores e as alterações do agente.

----Fim

9.1.2 Instalação de um agente

Instalar o agente em um servidor. Só então o servidor pode ser protegido por HSS.

Precauções da instalação

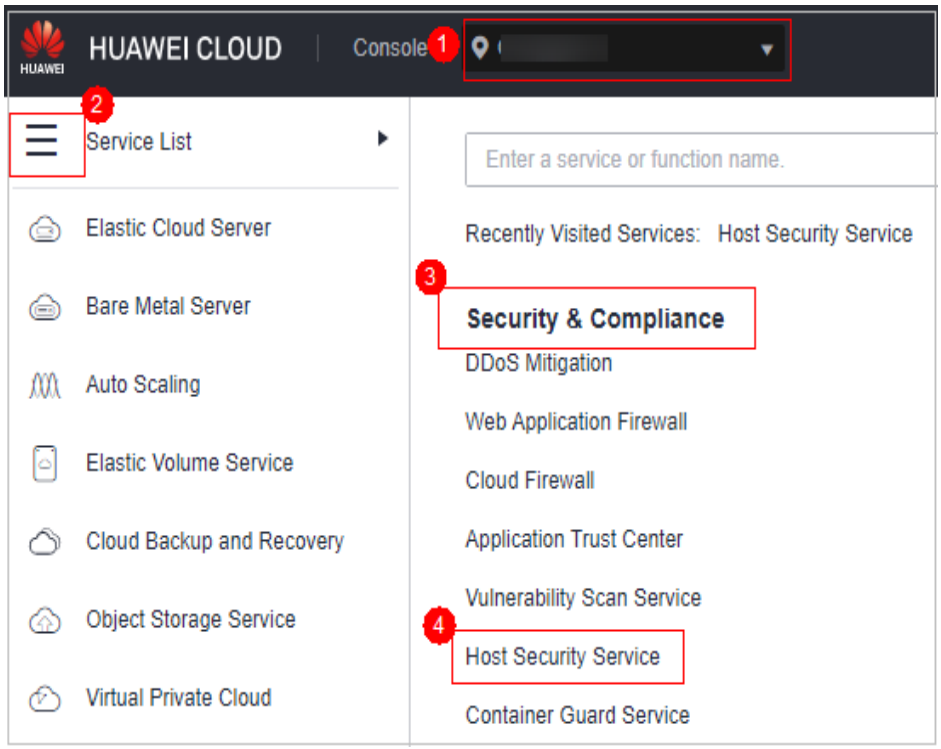
- Para obter detalhes sobre os SOs suportados pelo agente, consulte **SOs suportados**.
- Para uma melhor compatibilidade e experiência de serviço, é aconselhável usar os servidores da Huawei Cloud.
- Se algum software de segurança de terceiros tiver sido instalado no servidor, o agente do HSS pode falhar ao ser instalado. Nesse caso, desative ou desinstale o software antes de instalar o agente.
- A capacidade disponível do disco em que o agente está instalado deve ser maior que 300 MB. Caso contrário, a instalação do agente poderá falhar.
- Após a instalação, leva de 5 a 10 minutos para atualizar o status do agente. Você pode verificá-lo na guia "Servers" da página "Asset Management > Servers & Quota".
- Se esta é a primeira vez que você instala o agente, configure as notificações de alarme após a instalação.

Instalação de um agente em um 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 9-3 Acessar o HSS

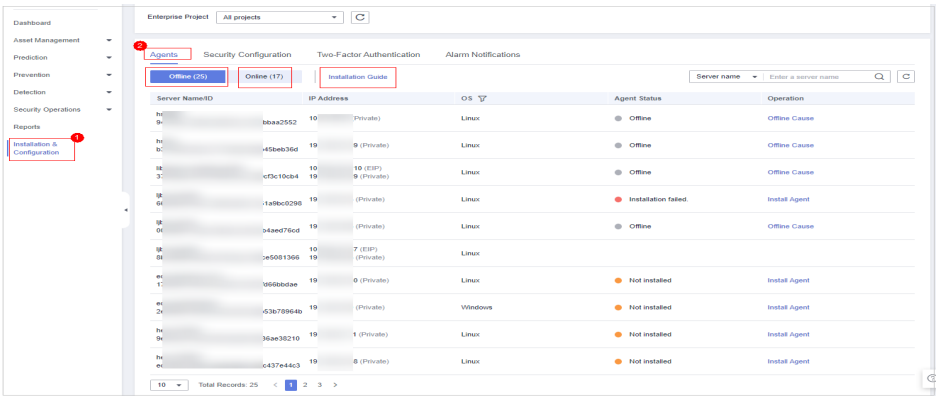


Passo 3 No painel de navegação, escolha **Installation & Configuration**. Clique na guia **Agents**.

NOTA

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

Figura 9-4 Acessar a página de gerenciamento do agente



Passo 4 Clique em **Offline** para verificar os servidores nos quais o agente não está instalado ou está off-line. Tabela 9-1 descreve os parâmetros.

Tabela 9-1 Parâmetros do agente off-line

Parâmetro	Descrição
Server Name/ID	Nome e ID do servidor
IP Address	EIP ou endereço IP privado de um servidor
OS	SO do servidor. Seu valor pode ser: ● **Linux** ● **Windows**
Agent Status	Status do agente de um servidor. Seu valor pode ser: ● **Offline** ● **Not installed** ● **Installation failed**
Agent Version	Versão do agente instalado no servidor de destino.
Agent Upgrade Status	O status do agente durante a atualização do agente.

Passo 5 Clique em **View Cause** na coluna **Operation** de um servidor para verificar por que um agente está off-line.

Passo 6 Clique em **Install Agent** na coluna **Operation**. Baixe o pacote do agente adequado para a arquitetura do seu servidor e SO. Para obter detalhes sobre como instalar o agente em um servidor do Linux, consulte **Instalação de um agente no Linux**. Para obter detalhes sobre como instalar o agente em um servidor do Windows, consulte **Instalação de um agente no Windows**.

----Fim

Instalação de um agente em vários servidores (com diferentes contas e senhas de servidor)

Você pode instalar o agente em vários servidores com contas e senhas diferentes.

Restrições

- Para obter detalhes sobre os SOs suportados pelo agente, consulte **SOs suportados**.
- Atualmente, os agentes do HSS podem ser instalados em um lote de servidores do Linux que executam diferentes contas e senhas na Huawei Cloud.
- Todos os servidores que você deseja instalar em lote o agente devem estar no mesmo grupo de segurança ou grupos de segurança conectados entre si.

Pré-requisitos

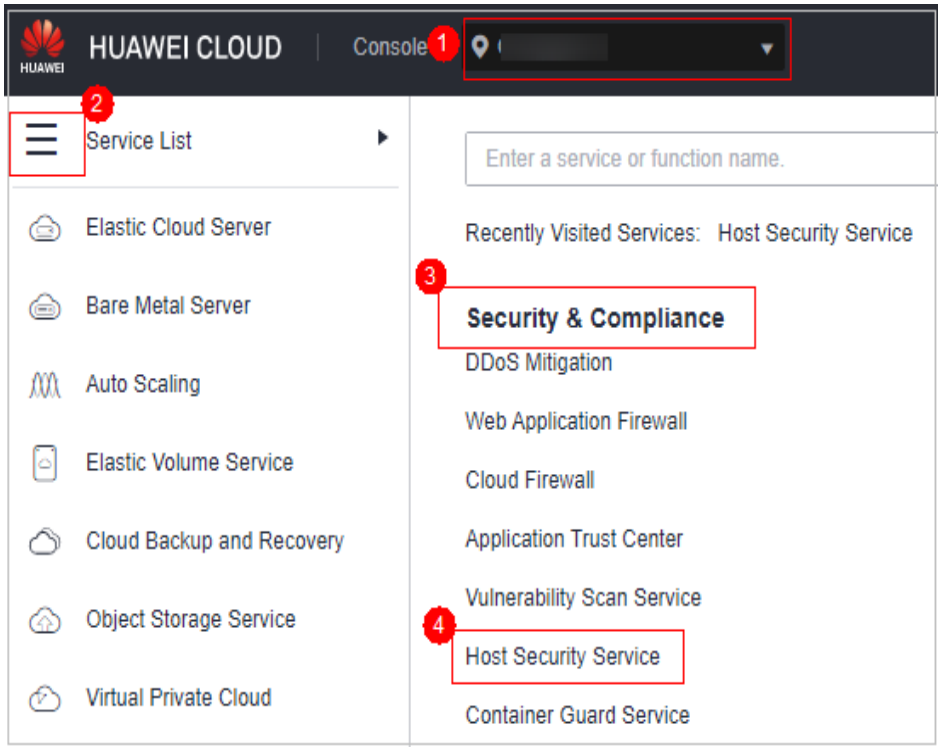
- Todos os servidores de destino devem suportar logon SSH.
- As contas de logon corretas, números de portas e senhas de todos os servidores foram obtidos.
- Todos os servidores de destino devem estar no estado **Running**.

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 9-5 Acessar o HSS

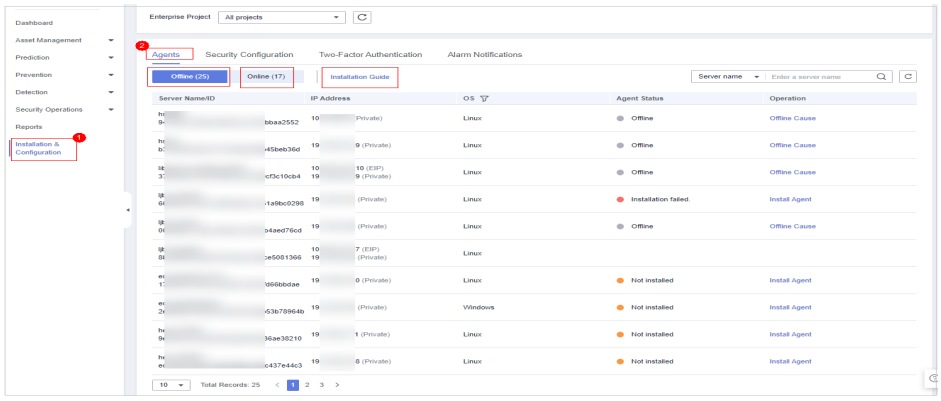


Passo 3 No painel de navegação, escolha **Installation & Configuration**. Clique na guia **Agents**.

NOTA

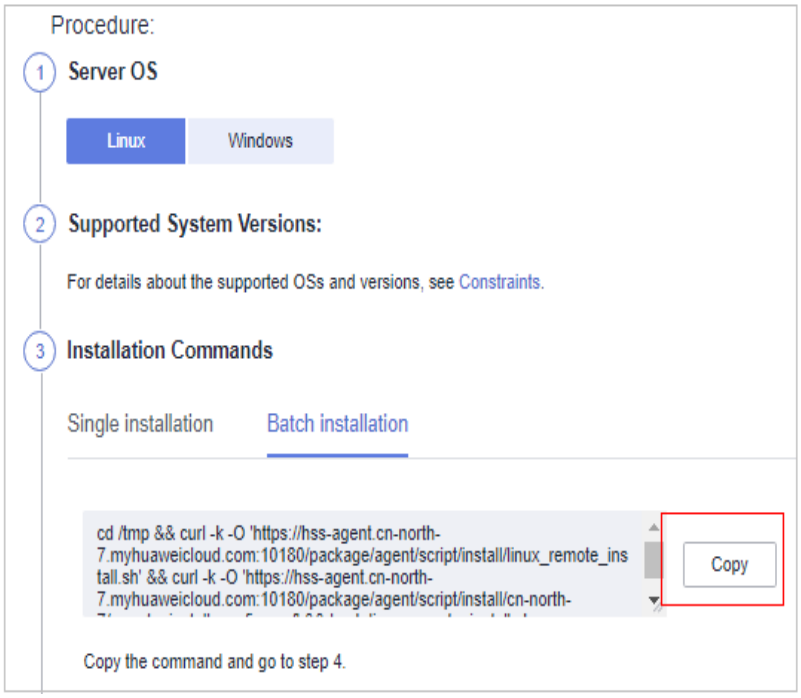
If your servers are managed by enterprise projects, you can select an enterprise project to view or operate the asset and scan information.

Figura 9-6 Acessar a página de gerenciamento do agente



Passo 4 Clique em **Installation Guide** e copie o comando de instalação em lote.

Figura 9-7 Copiar o comando de instalação em lote



Passo 5 Faça logon remotamente no servidor onde você planeja instalar o agente.

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**.

AVISO

Após efetuar logon no servidor, execute o seguinte comando para verificar se o comando esperado existe no servidor. Se o comando esperado não existir, configure o repositório de yum.

/bin/expect -v

Passo 6 Execute o seguinte comando para acessar o diretório **/tmp**:

cd /tmp/

Passo 7 Execute o seguinte comando para criar o arquivo **linux-host-list.txt** e adicione os endereços IP privados dos servidores que você deseja instalar o agente ao arquivo:

Formato do comando: **echo "***IP address Port***root rootPassword" >> linux-host-list.txt**

Ou **echo "***IP address Port* **user userPassword rootPassword" >> linux-host-list.txt**

Exemplo: **echo "127.8.10.8 22 root rootPassword" >> linux-host-list.txt**

Ou **echo "127.8.10.9 22 user userPassword rootPassword" >> linux-host-list.txt**

Para especificar vários endereços IP, escreva vários comandos, cada um em uma linha separada.

Exemplo: echo "127.8.10.1 22 root rootPassword" >> linux-host-list.txt

echo "127.8.10.8 22 user userPassword rootPassword" >> linux-host-list.txt

echo "127.8.10.3 22 root rootPassword" >> linux-host-list.txt

Passo 8 Pressione **Enter** para salvar o endereço IP. Execute o comando **cat linux-host-list.txt** para verificar se os endereços IP foram adicionados.

Passo 9 Cole o comando de instalação copiado e execute-o como usuário **root** para instalar o agente nos servidores.

Se forem exibidas informações semelhantes às seguintes, o agente foi instalado com sucesso:

remote_install finished. [OK]

Passo 10 Depois que a instalação for bem-sucedida, escolha **Installation and Configuration** > **Agents** > **Online** e verifique o status do agente do servidor de destino. Se o agente estiver on-line, o agente está funcionando corretamente.

----Fim

9.1.3 Desinstalação de um agente

Se você não precisar mais usar o HSS, desinstale o agente seguindo as instruções fornecidas nesta seção. Se o agente for desinstalado, o HSS deixará de proteger seus servidores e de detectar riscos.

Métodos de desinstalação

O agente pode ser desinstalado com um clique no console ou desinstalado manualmente.

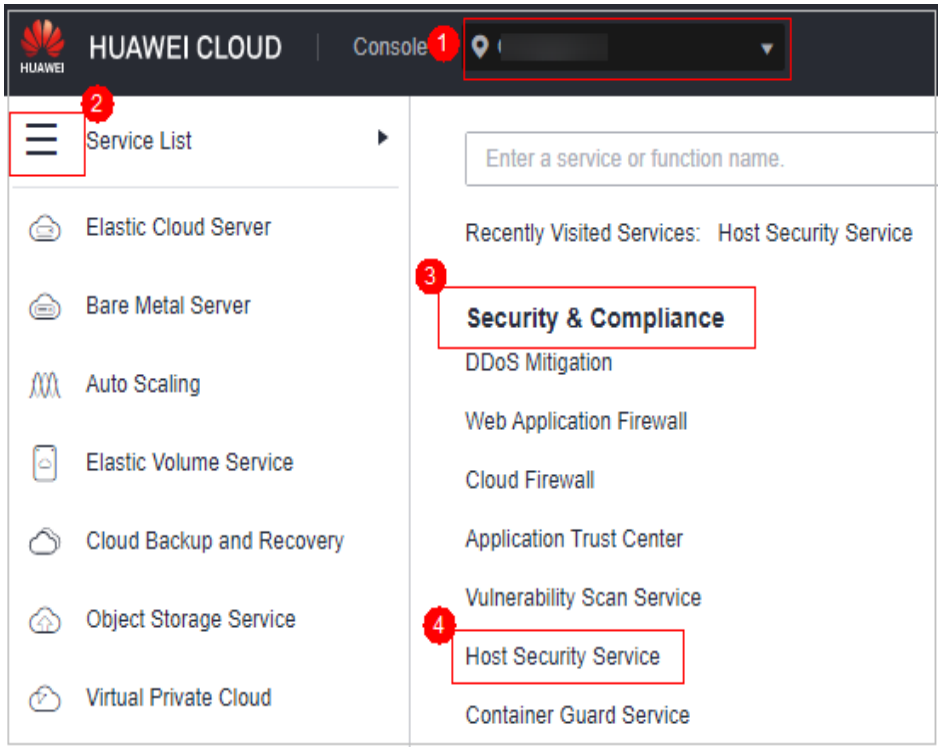
- Desinstalação do agente no console: se o agente estiver on-line, você poderá desinstalá-lo com um clique no console.
  - **Desinstalação do agente de um único servidor em um clique**
  - **Desinstalação do agente de vários servidores em um clique**
- Desinstalação manual do agente: se o agente estiver off-line, você poderá desinstalá-lo manualmente.
  - **Desinstalação manual do agente em um servidor do Linux**
  - **Desinstalação manual do agente em um servidor do Windows**

Desinstalação do agente de um único servidor em um clique

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 9-8 Acessar o HSS

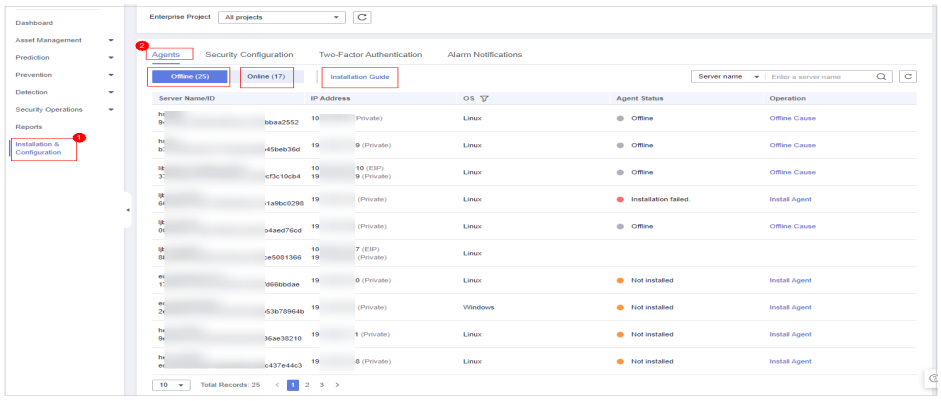


Passo 3 No painel de navegação, escolha **Installation & Configuration**. Clique na guia **Agents**.

NOTA

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

Figura 9-9 Acessar a página de gerenciamento do agente



Passo 4 Clique em **Offline** para verificar os servidores onde o agente está on-line. **Tabela 9-2** descreve os parâmetros.

Figura 9-10 Visualização da lista de agentes on-line

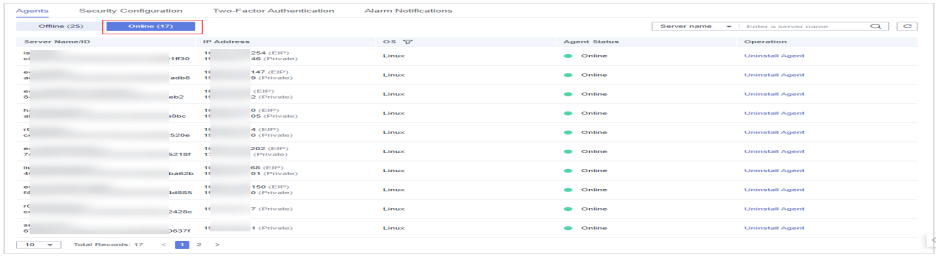


Tabela 9-2 Parâmetros do agente on-line

Parâmetro	Descrição
Server Name/ID	Nome e ID do servidor
IP Address	EIP ou endereço IP privado de um servidor
OS	SO do servidor. Seu valor pode ser: ● **Linux** ● **Windows**
Agent Status	Status do agente de um servidor. Seu valor pode ser: ● **Online**
Agent Version	Versão do agente instalado no servidor de destino.
Agent Upgrade Status	O status de atualização do agente.

Passo 5 Clique em **Uninstall Agent** na coluna **Operation** de um servidor. Na caixa de diálogo exibida, confirme as informações de desinstalação e clique em **OK**.

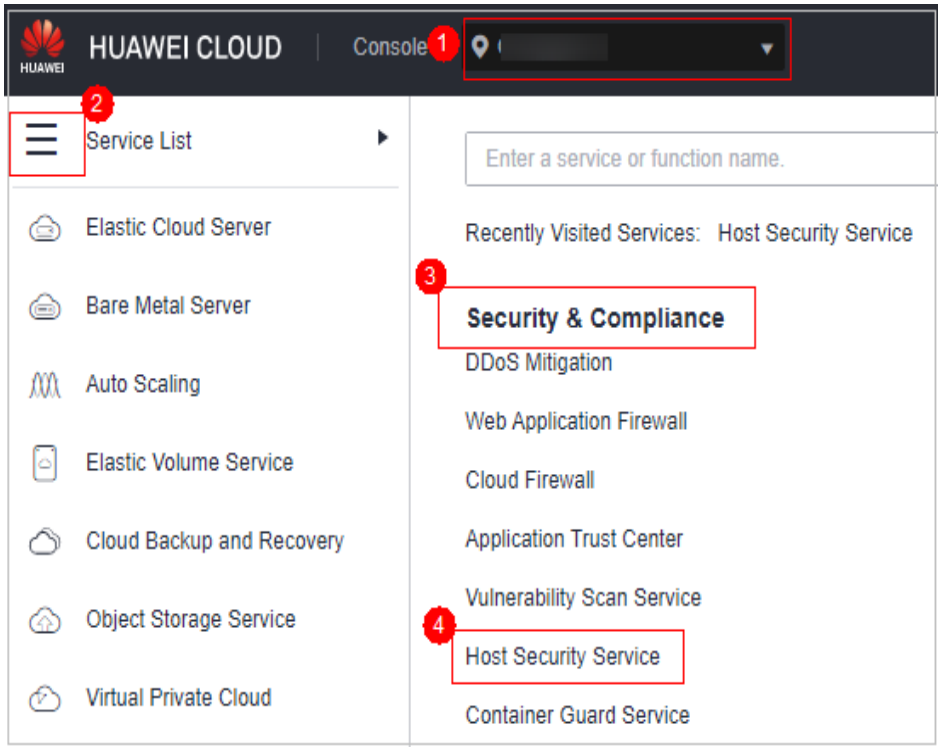
----Fim

Desinstalação do agente de vários servidores em um clique

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 9-11 Acessar o HSS

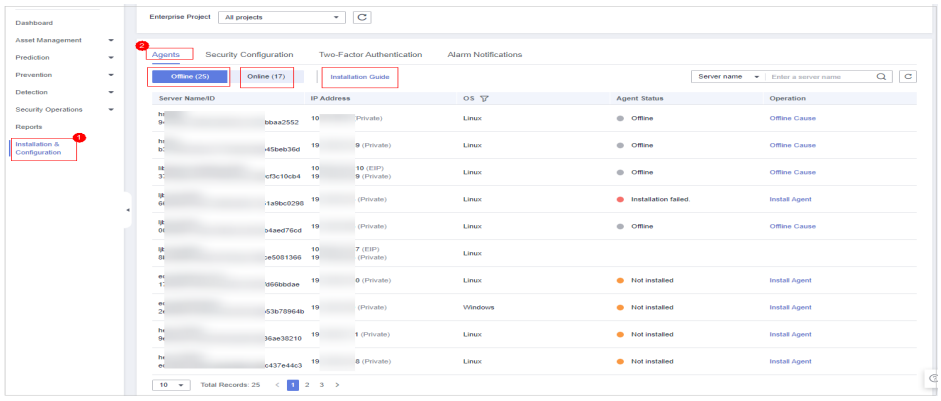


Passo 3 No painel de navegação, escolha **Installation & Configuration**. Clique na guia **Agents**.

NOTA

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

Figura 9-12 Acessar a página de gerenciamento do agente



Passo 4 Clique em **Offline** para verificar os servidores onde o agente está on-line. **Tabela 9-3** descreve os parâmetros.

Figura 9-13 Visualização da lista de agentes on-line

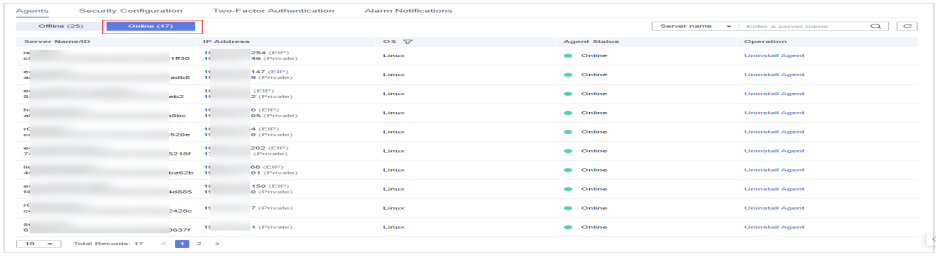


Tabela 9-3 Parâmetros do agente on-line

Parâmetro	Descrição
Server Name/ID	Nome e ID do servidor
IP Address	EIP ou endereço IP privado de um servidor
OS	SO do servidor. Seu valor pode ser: ● **Linux** ● **Windows**
Agent Status	Status do agente de um servidor. Seu valor pode ser: ● **Online**
Agent Version	Versão do agente instalado no servidor de destino.
Agent Upgrade Status	O status de atualização do agente.

Passo 5 Selecione os servidores de destino cujo agente você deseja desinstalar.

NOTA

Se você marcar a caixa antes de **Server Name/ID**, todos os servidores na página serão selecionados.

Passo 6 Clique em **Uninstall Agent** acima da lista de servidores. Na caixa de diálogo exibida, confirme os servidores dos quais você deseja desinstalar o agente e clique em **OK**.

----Fim

Desinstalação manual do agente em um servidor do Linux

Passo 1 Efetue logon remotamente no servidor do Linux onde o agente será desinstalado.

- **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 tiver sido instalado, execute o seguinte comando 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.

- No EulerOS, CentOS e Red Hat ou em outros SOs que suportam instalação 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 foi desinstalado.

----Fim

Desinstalação manual do agente em um servidor do Windows

Passo 1 Efetue logon remotamente no servidor do Windows onde o agente será desinstalado.

- 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 da 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 File\HostGuard** no servidor do Windows.

Passo 3 Clique duas vezes no arquivo **unins000.exe** para desinstalar o agente.

Passo 4 Na caixa de diálogo **HostGuard Uninstall**, clique em **Yes** para excluir o HostGuard e todos os seus componentes.

Passo 5 (Opcional) Reinicie o servidor.

- Se você ativou a WTP, será necessário reiniciar o servidor após desinstalar o agente. 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 6 Se o diretório **C:\Program Files\HostGuard** não existir no servidor do Windows, o agente foi desinstalado.

----Fim

9.1.4 Atualização do agente

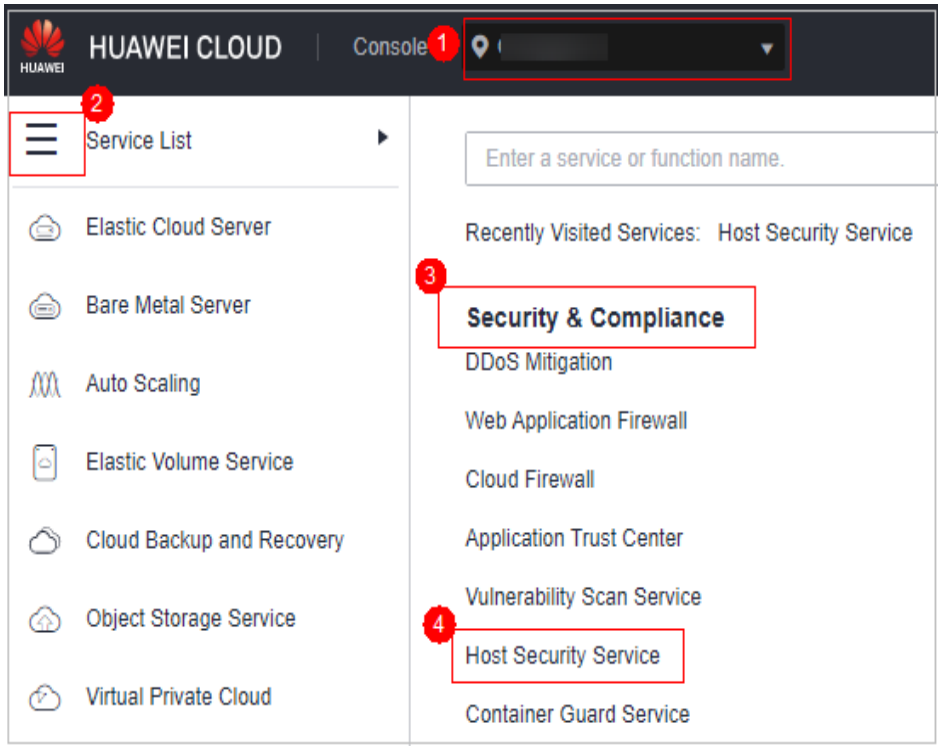
O HSS continua a melhorar suas capacidades de serviço, incluindo, mas não limitado a, novos recursos e correções de defeitos. Por favor, atualize seu agente para a versão mais recente em tempo hábil para desfrutar de um melhor serviço.

Atualização do agente em um 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 9-14 Acessar o HSS

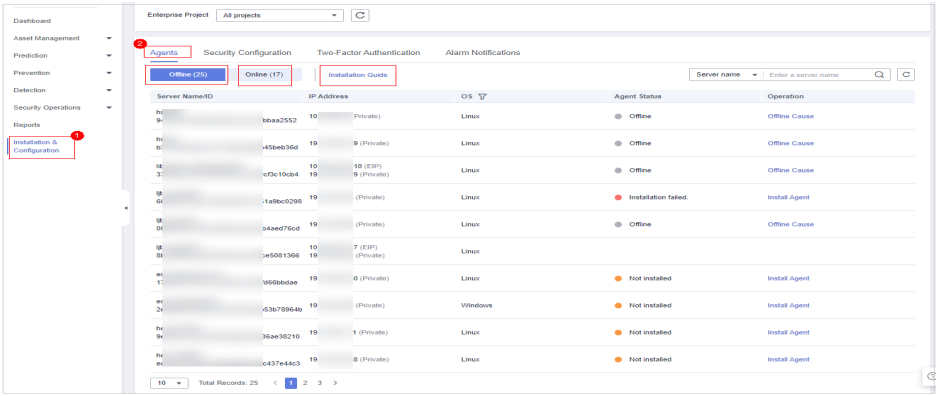


Passo 3 No painel de navegação, escolha **Installation & Configuration**. Clique na guia **Agents**.

NOTA

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

Figura 9-15 Acessar a página de gerenciamento do agente



Passo 4 Clique em **Offline** para verificar os servidores onde o agente está on-line. **Tabela 9-4** descreve os parâmetros.

Figura 9-16 Visualização da lista de agentes on-line

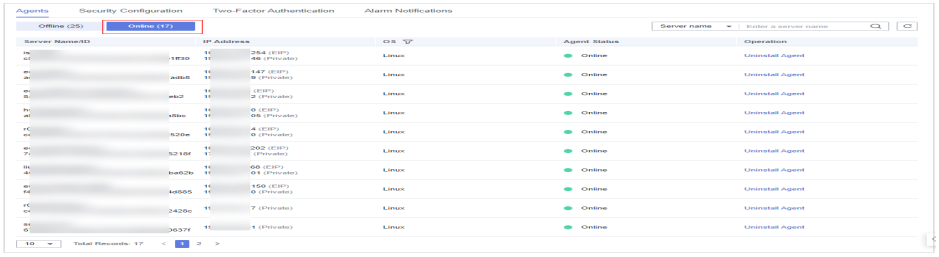


Tabela 9-4 Parâmetros do agente on-line

Parâmetro	Descrição
Server Name/ID	Nome e ID do servidor
IP Address	EIP ou endereço IP privado de um servidor
OS	SO do servidor. Seu valor pode ser: ● **Linux** ● **Windows**
Agent Status	Status do agente de um servidor. Seu valor pode ser: ● **Online**
Agent Version	Versão do agente instalado no servidor de destino.
Agent Upgrade Status	O status de atualização do agente.

Passo 5 Clique em **Upgrade** na coluna **Operation** do servidor de destino. Na caixa de diálogo exibida, confirme os detalhes da atualização e clique em **OK**.

Passo 6 Após a conclusão da atualização, verifique a versão do agente. Se o agente de versão mais recente for usado, a atualização será bem-sucedida.

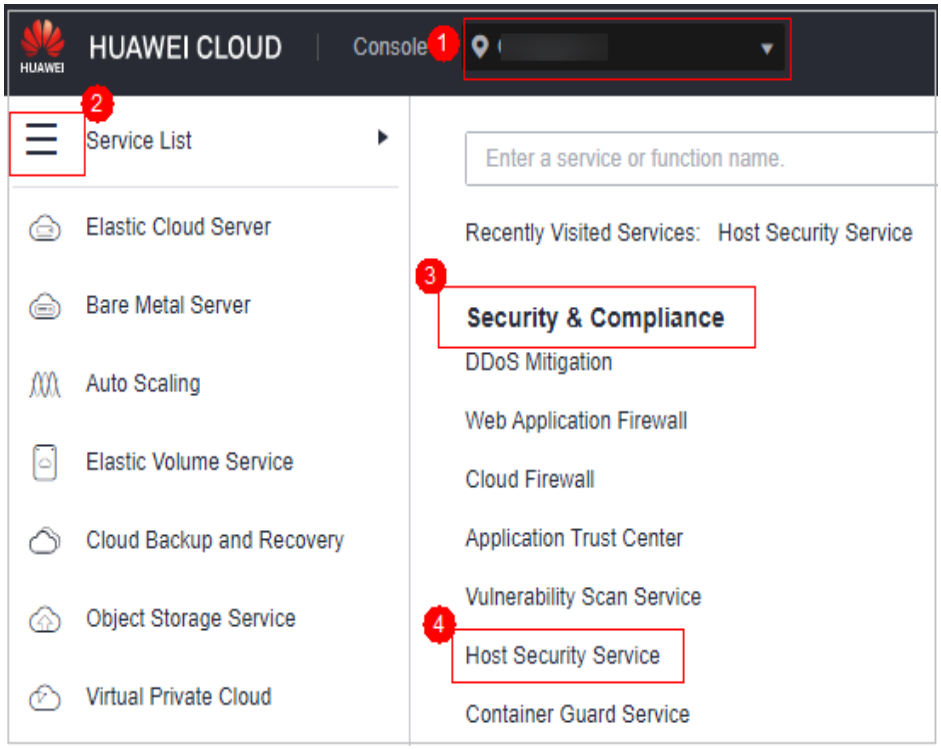
----Fim

Atualização do agente em vários servidores

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 9-17 Acessar o HSS

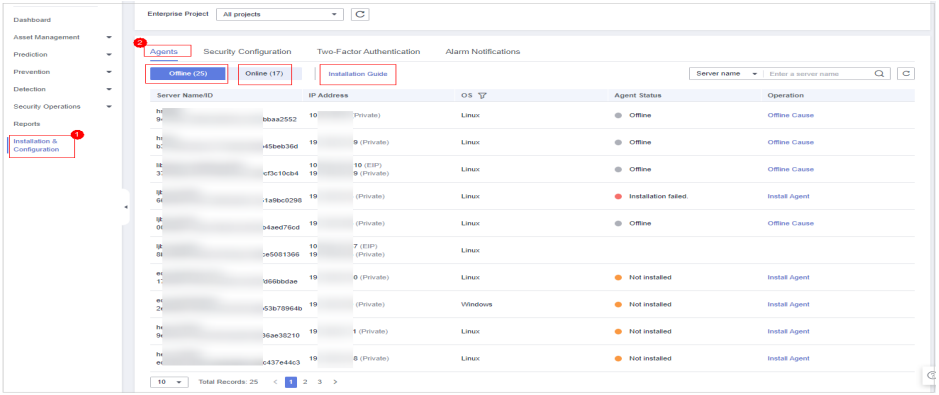


Passo 3 No painel de navegação, escolha **Installation & Configuration**. Clique na guia **Agents**.

NOTA

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

Figura 9-18 Acessar a página de gerenciamento do agente



Passo 4 Clique em **Offline** para verificar os servidores onde o agente está on-line. **Tabela 9-5** descreve os parâmetros.

Figura 9-19 Visualização da lista de agentes on-line

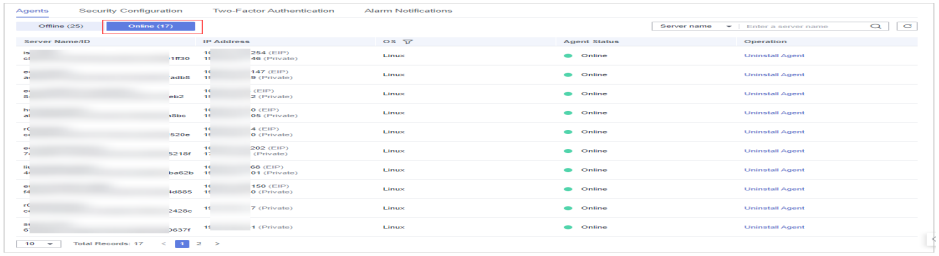


Tabela 9-5 Parâmetros do agente on-line

Parâmetro	Descrição
Server Name/ID	Nome e ID do servidor
IP Address	EIP ou endereço IP privado de um servidor
OS	SO do servidor. Seu valor pode ser: ● **Linux** ● **Windows**
Agent Status	Status do agente de um servidor. Seu valor pode ser: ● **Online**
Agent Version	Versão do agente instalado no servidor de destino.
Agent Upgrade Status	O status de atualização do agente.

Passo 5 Selecione os servidores de destino cujo agente você deseja atualizar.

NOTA

- Se você marcar a caixa antes de **Server Name/ID**, todos os servidores na página serão selecionados.
- Se você marcar a caixa antes de **Select all**, todos os servidores que você tiver serão selecionados.

Passo 6 Clique em **Upgrade Agent** acima da lista de servidores. Na caixa de diálogo exibida, confirme as informações do servidor e clique em **OK**.

Passo 7 Após a conclusão da atualização, verifique a versão do agente. Se o agente de versão mais recente for usado, a atualização será bem-sucedida.

----Fim

9.2 Configurações de segurança

Você pode adicionar localizações comuns de logon, endereços IP comuns e endereços IP da lista branca, além de ativar o isolamento e a eliminação de programas maliciosos para melhorar a segurança do servidor.

Para mais detalhes, consulte **Instalação e configuração**.

9.3 Gerenciamento de plug-ins

9.3.1 Visão geral dos plug-ins

Você pode instalar e gerenciar plug-ins.

Tipo de plug-ins

Atualmente, apenas os plug-ins do Docker podem ser gerenciados.

Cenários de aplicação de plug-in do Docker

Se a proteção de container estiver ativada e você quiser usar a função de bloqueio de imagem, será necessário **instalar o plug-in do Docker**.

O plug-in do Docker fornece o recurso de bloqueio de imagem. Ele pode impedir a inicialização de imagens de containers com vulnerabilidades de alto risco ou que não estejam em conformidade com os padrões de segurança no ambiente do Docker.

Você pode configurar o bloqueio de imagem nos seguintes cenários:

- Para aprimorar a segurança das imagens de container e evitar os riscos causados pelo uso de imagens não confiáveis ou desatualizadas, você pode configurar uma **política de bloqueio de imagens** para especificar o nível de vulnerabilidades a serem bloqueadas ou a lista branca.
- Se você precisar estar em conformidade com os requisitos de segurança de determinados setores ou regulamentos, como PCI DSS e CIS, poderá **configurar uma política de bloqueio de imagem** para especificar a linha de base de segurança ou os itens de verificação de conformidade a serem bloqueados.
- Se precisar implementar as melhores práticas de container DevSecOps e incorporar verificação de segurança e defesa em cada fase do ciclo de vida do container, você

poderá **configurar uma política de bloqueio de imagem** para aumentar a segurança da origem aos dispositivos.

9.3.2 Visualização de detalhes do plug-in

Você pode ver os detalhes sobre os plug-ins usados pelos servidores.

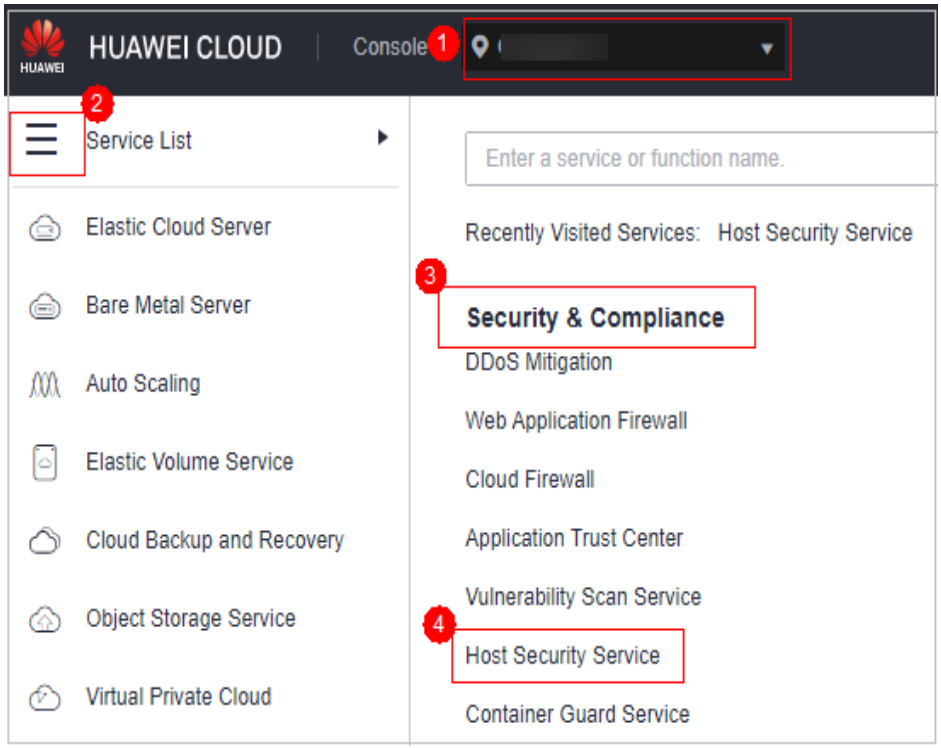
Você pode instalar, atualizar e desinstalar plug-ins conforme necessário.

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 9-20 Acessar o HSS



Passo 3 No painel de navegação à esquerda, escolha **Installation & Configuration** e clique na guia **Plug-in Settings** para visualizar detalhes sobre todos os plug-ins. Para obter mais informações, consulte **Tabela 9-6**.

Por padrão, todos os servidores são exibidos na lista de plug-ins. Se um plug-in estiver instalado em um servidor, os detalhes do plug-in serão exibidos. Se nenhum plug-in estiver instalado em um servidor, as informações do plug-in estarão vazias.

Tabela 9-6 Parâmetros da lista de plug-in Docker

Parâmetro	Descrição
Server Name/ID	Nome e ID do servidor

Parâmetro	Descrição
IP Address	Endereço IP do servidor
OS	Tipo do SO em execução no servidor
Plug-in Name	Nome do plug-in instalado no servidor.
Plug-in Version	Versão do plug-in instalado no servidor.
Plug-in Status	Status atual do plug-in. ● **Created**: o plug-in foi criado, mas não foi iniciado. ● **Running**: o plug-in está funcionando corretamente. ● **Paused**: o plug-in está em pausa. ● **Restarting**: o plug-in está sendo reiniciado. ● **Removing**: o plug-in está sendo excluído. ● **Exited**: o plug-in foi interrompido. ● **Dead**: o plug-in não pode ser iniciado ou foi excluído.
Plug-in Upgrade Status	Status de atualização do plug-in. ● **Not upgraded**: o plug-in não foi atualizado para a versão mais recente. ● **Upgrading**: o plug-in está sendo atualizado. ● **Upgraded**: o plug-in foi atualizado. ● **Upgrade failed**: o plug-in falhou ao ser atualizado.

----Fim

9.3.3 Instalação de um plug-in

Se a proteção de container estiver ativada e você quiser usar a função de bloqueio de imagem, instale o plug-in Docker seguindo as instruções fornecidas nesta seção.

Restrições

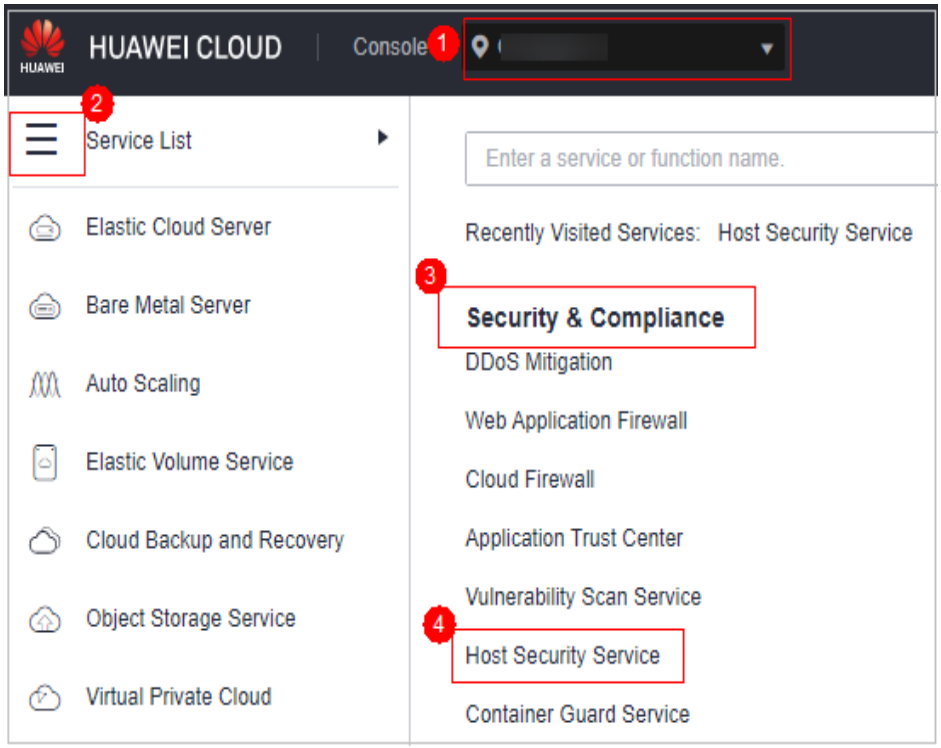
- Somente containers de Docker são suportados. Não há suporte para containers containerd.
- A versão do mecanismo de Docker é 18.06.0 ou posterior.
- A versão da API de Docker é 1.38 ou posterior.
- Somente servidores de Linux são suportados.
- Somente as arquiteturas de hardware x86 e Arm são suportadas.
- A edição de container do HSS foi ativada.
- Atualmente, apenas os servidores on-line da Huawei Cloud são suportados.

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 9-21 Acessar o HSS



Passo 3 Na árvore de navegação à esquerda, escolha **Installation & Configuration** e clique na guia **Plug-in Settings** > **Docker plug-in**. Clique em **Plug-in installation guide**, obtenha os comandos de instalação no painel deslizante e clique em **Copy**.

Passo 4 Efetue logon remotamente no servidor onde o plug-in será instalado como o usuário **root**.

- 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 fazer logon no servidor e instalar o plug-in no servidor como usuário **root**.

Passo 5 Execute o seguinte comando para acessar o diretório **/tmp**:

```
cd /tmp/
```

Passo 6 Crie **linux-host-list.txt**, que conterá os endereços IP privados do servidor onde o agente será instalado:

Sintaxe do comando:

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt
Or
echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

Para especificar vários endereços IP, escreva vários comandos, cada um em uma linha separada.

Exemplo:


```
echo 127.8.8.1 22 root rootPassword >> linux-host-list.txt
echo 127.8.8.2 22 user userPassword rootPassword >> linux-host-list.txt
echo 127.8.8.3 22 root rootPassword >> linux-host-list.txt
```

Passo 7 Pressione **Enter** para salvar o endereço IP. Execute o comando **cat linux-host-list.txt** para verificar se os endereços IP foram adicionados.

Passo 8 Copie os comandos de instalação em lote para o terminal de comando e pressione **Enter**.

NOTA

Se o pacote de instalação não puder ser baixado, verifique se o DNS pode resolver o nome de domínio no comando de instalação.

Passo 9 Se **remote_install finished. [OK]** é exibido, a instalação foi bem-sucedida. Aguarde de 3 a 5 minutos e escolha **Installation & Configuration** e clique na guia **Plug-in Settings** para verificar o status do plug-in Docker do servidor do painel.

----Fim

9.3.4 Atualização de um plug-in

Você pode atualizar plug-ins de um servidor de destino.

Restrições

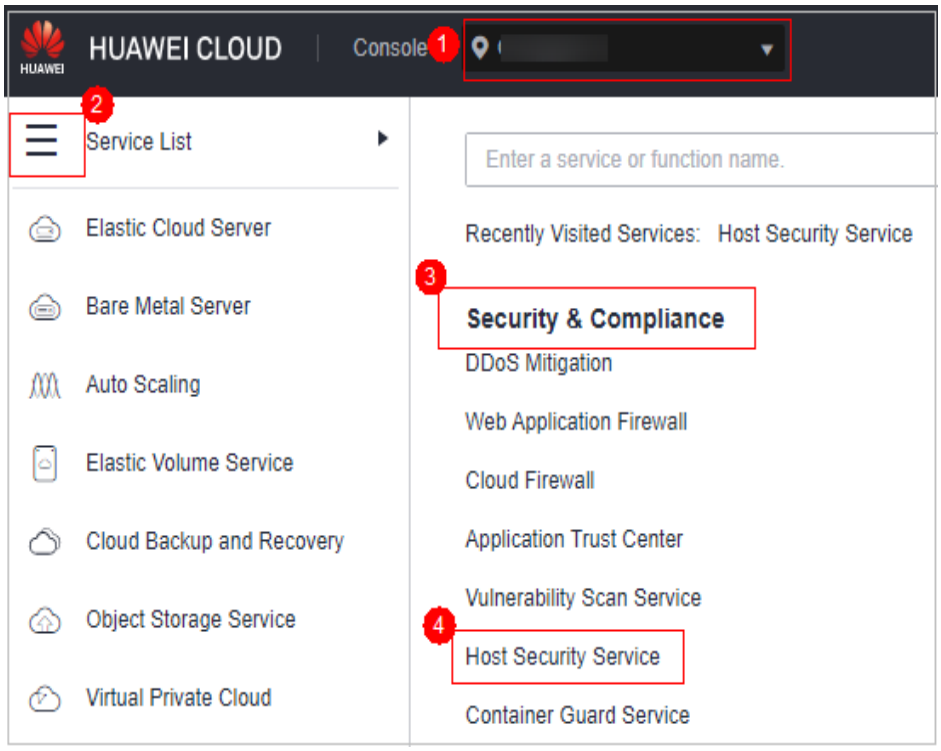
- Somente containers de Docker são suportados. Não há suporte para containers containerd.
- A versão do mecanismo de Docker é 18.06.0 ou posterior.
- A versão da API de Docker é 1.38 ou posterior.
- Somente servidores de Linux são suportados.
- Somente as arquiteturas de hardware x86 e Arm são suportadas.
- A edição de container do HSS foi ativada.
- Atualmente, apenas os servidores on-line da Huawei Cloud são suportados.

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 9-22 Acessar o HSS



Passo 3 Na árvore de navegação à esquerda, escolha **Installation & Configuration** e clique na guia **Plug-in Settings** > **Docker plug-in**. Clique em **Plug-in upgrade guide**, obtenha os comandos de atualização no painel deslizante e clique em **Copy**.

Passo 4 Efetue logon remotamente no servidor onde o plug-in deve ser atualizado como o usuário **root**.

- 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 atualizar o plug-in no servidor como usuário **root**.

Passo 5 Execute o seguinte comando para acessar o diretório **/tmp**:

```
cd /tmp/
```

Passo 6 Crie **linux-host-list.txt**, que conterá os endereços IP privados do servidor onde o plug-in será atualizado:

Sintaxe do comando:

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt
Or echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

Para especificar vários endereços IP, escreva vários comandos, cada um em uma linha separada.

Exemplo:

```
echo 127.8.8.1 22 root rootPassword >> linux-host-list.txt
echo 127.8.8.2 22 user userPassword rootPassword >> linux-host-list.txt
echo 127.8.8.3 22 root rootPassword >> linux-host-list.txt
```


Passo 7 Pressione **Enter** para salvar o endereço IP. Execute o comando **cat linux-host-list.txt** para verificar se os endereços IP foram adicionados.

Passo 8 Copie os comandos de atualização em lote para a caixa de comando e pressione **Enter**. A atualização é iniciada automaticamente.

NOTA

Se o pacote de instalação não puder ser baixado, verifique se o DNS pode resolver o nome de domínio nos comandos de instalação.

Passo 9 Se **remote_upgrade finished. [OK]** for exibido, a atualização foi bem-sucedida. Aguarde de 3 a 5 minutos e escolha **Installation & Configuration** e clique na guia **Plug-in Settings** para verificar o status do plug-in Docker do servidor do painel.

----Fim

9.3.5 Desinstalação de um plug-in

Restrições

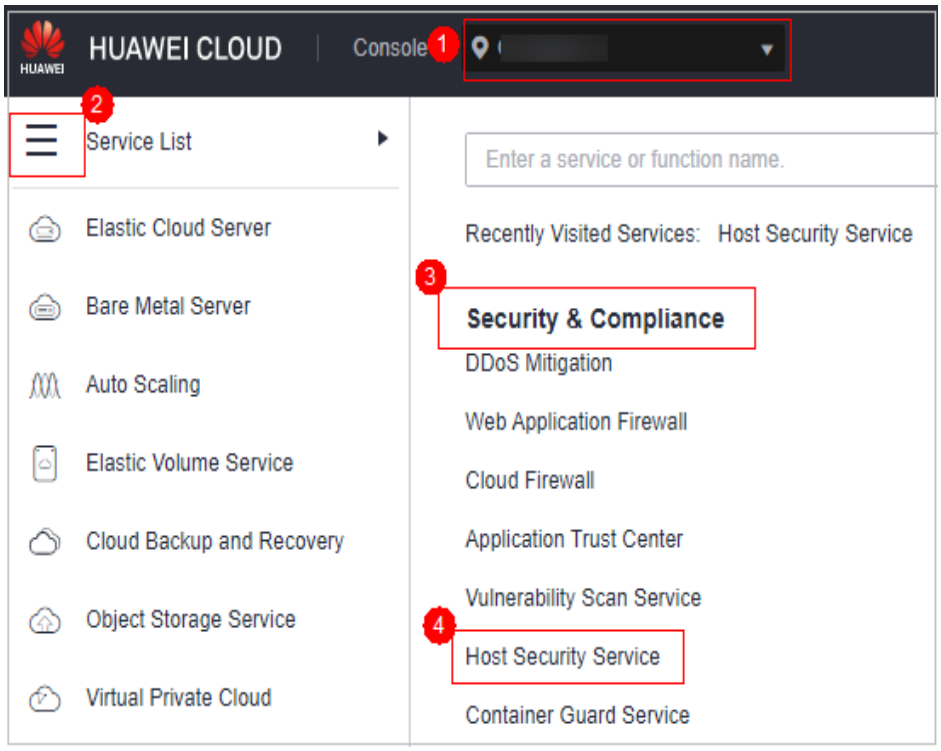
- Somente containers de Docker são suportados. Não há suporte para containers containerd.
- A versão do mecanismo de Docker é 18.06.0 ou posterior.
- A versão da API de Docker é 1.38 ou posterior.
- Somente servidores de Linux são suportados.
- Somente as arquiteturas de hardware x86 e Arm são suportadas.
- A edição de container do HSS foi ativada.
- Atualmente, apenas os servidores on-line da Huawei Cloud são suportados.

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 9-23 Acessar o HSS



Passo 3 Na árvore de navegação à esquerda, escolha **Installation & Configuration** e clique na guia **Plug-in Settings** > **Docker plug-in**. Clique em **Plug-in uninstallation guide**, obtenha os comandos de desinstalação no painel deslizante e clique em **Copy**.

Passo 4 Efetue logon remotamente no servidor onde o plug-in será desinstalado como usuário **root**.

- 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 desinstalar o plug-in no servidor como usuário **root**.

Passo 5 Execute o seguinte comando para acessar o diretório **/tmp**:

```
cd /tmp/
```

Passo 6 Crie **linux-host-list.txt**, que conterá os endereços IP privados do servidor onde o plug-in deve ser desinstalado:

Sintaxe do comando:

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt
Or echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

Para especificar vários endereços IP, escreva vários comandos, cada um em uma linha separada.

Exemplo:

```
echo 127.8.8.1 22 root rootPassword >> linux-host-list.txt
echo 127.8.8.2 22 user userPassword rootPassword >> linux-host-list.txt
echo 127.8.8.3 22 root rootPassword >> linux-host-list.txt
```


Passo 7 Pressione **Enter** para salvar o endereço IP. Execute o comando **cat linux-host-list.txt** para verificar se os endereços IP foram adicionados.

Passo 8 Copie os comandos de desinstalação em lote para a caixa de comando e pressione **Enter**. A desinstalação é iniciada automaticamente.

Passo 9 Se **remote_uninstall finished. [OK]** for exibido, a desinstalação foi bem-sucedida. Aguarde de 3 a 5 minutos e escolha **Installation & Configuration** e clique na guia **Plug-in Settings** para verificar o status do plug-in Docker do servidor do painel.

```
remote_uninstall finished. [OK]
```

----Fim

10 Auditoria

10.1 Operações do HSS suportadas pelo CTS

O Cloud Trace Service (CTS) registra todas as operações no HSS, incluindo solicitações iniciadas no console de gerenciamento ou em APIs abertas e respostas às solicitações, para que os locatários possam consultar, auditar e rastrear.

Tabela 10-1 lista as operações do HSS registradas pelo CTS.

Tabela 10-1 Operações do HSS que podem ser gravadas pelo CTS

Operação	Tipo de recurso	Nome do rastreamento
Cancelar a ignorância de uma porta	hss	notIgnorePortStatus
Ignorar uma porta	hss	ignorePortStatus
Cancelar a ignorância de itens de verificação de configuração	hss	notIgnoreCheckRuleStat
Ignorar itens de verificação de configuração	hss	ignoreCheckRuleStat
Tentar novamente uma verificação de linha de base	hss	runBaselineDetect
Desvincular a cota	hss	cancelHostsQuota
Desativar a proteção do container	hss	closeContainerProtectStatus
Ativar a proteção do container	hss	openContainerProtectStatus
Desbloquear um endereço IP	hss	changeBlockedIp
Manipular um evento	hss	changeEvent
Cancelar o isolamento de um arquivo	hss	changeIsolatedFile
Remover um alarme da lista branca	hss	removeAlarmWhiteList

Operação	Tipo de recurso	Nome do rastreamento
Configurar a lista branca de logon	hss	addLoginWhiteList
Remover informações de logon da lista branca de logon	hss	removeLoginWhiteList
Adicionar um grupo de servidores	hss	addHostsGroup
Adicionar servidores a um grupo	hss	associateHostsGroup
Modificar um grupo de servidores	hss	changeHostsGroup
Excluir um grupo de servidores	hss	deleteHostsGroup
Desativar o HSS	hss	closeHostsProtectStatus
Ativar o HSS	hss	openHostsProtectStatus
Desinstalar um agente	hss	uninstallAgents
Digitalizar uma imagem	hss	runImageScan
Sincronizar a lista de imagens a partir de SWR	hss	runImageSynchronizeTask
Atualizar e digitalizar uma imagem SWR	hss	runSwrImageScan
Realizar uma verificação de segurança novamente	hss	resetRiskScore
Adicionar um grupo de políticas	hss	addPolicyGroup
Remover um grupo de políticas	hss	deletePolicyGroup
Aplicar um grupo de políticas	hss	deployPolicyGroup
Modificar uma política	hss	modifyPolicyDetail
Modificar um grupo de políticas	hss	modifyPolicyGroup
Desativar o isolamento e a eliminação automáticos	hss	closeAutoKillVirusStatus
Ativar o isolamento e a eliminação automáticos	hss	openAutoKillVirusStatus
Configurar endereços IP de logon comuns	hss	modifyLoginCommonIp
Configurar localizações de logon comuns	hss	modifyLoginCommonLocation
Configurar a lista branca de logon SSH	hss	modifyLoginWhiteIp
Corrigir uma vulnerabilidade	hss	changeVulStatus
Adicionar um diretório protegido	hss	addHostProtectDirInfo

Operação	Tipo de recurso	Nome do rastreamento
Adicionar um processo privilegiado	hss	addPrivilegedProcessInfo
Adicionar uma configuração de proteção agendada	hss	addTimingOffConfigInfo
Remover um servidor de backup remoto	hss	deleteBackupHostInfo
Remover um diretório protegido	hss	deleteHostProtectDirInfo
Remover um processo privilegiado	hss	deletePrivilegedProcessInfo
Excluir configurações de proteção agendadas	hss	deleteTimingOffConfigInfo
Configurar o período de proteção agendado	hss	setDateOffConfigInfo
Modificar o status de um diretório protegido	hss	setProtectDirSwitchInfo
Ativar ou desativar a WTP dinâmica	hss	setRaspSwitch
Configurar um servidor de backup remoto	hss	setRemoteBackupInfo
Ativar ou desativar a proteção agendada	hss	setTimingOffSwitchInfo
Desativar a WTP	hss	closeWtpProtectionStatusInfo
Ativar a WTP	hss	openWtpProtectionStatusInfo
Modificar um servidor de backup remoto	hss	updateBackupHostInfo
Modificar um diretório protegido	hss	updateHostProtectDirInfo
Modificar um processo privilegiado	hss	updatePrivilegedProcessInfo
Modificar o diretório bin do Tomcat	hss	updateRaspPathInfo
Modificar o período de proteção agendado	hss	updateTimingOffConfigInfo

10.2 Visualização de logs de auditoria

Depois de ativar o CTS, o sistema começa a registrar operações no HSS. Os registros da operação para os últimos sete dias podem ser visualizados no console do CTS.

Visualização de um rastreamento do HSS no console do CTS

Passo 1 Faça logon no console de gerenciamento.

Passo 2 Clique em na parte superior da página e escolha **Cloud Trace Service** em **Management & Governance**. O console do CTS é exibido.

Passo 3 Escolha **Trace List** no painel de navegação.

Passo 4 Clique em **Filter** e especifique os critérios de filtragem conforme necessário. Os seguintes quatro filtros estão disponíveis:

- **Trace Type**, **Trace Source**, **Resource Type** e **Search By**.

  Selecione o filtro na lista suspensa.

  – Defina **Trace Type** como **Management**.

  – Defina **Trace Source** como **HSS**.

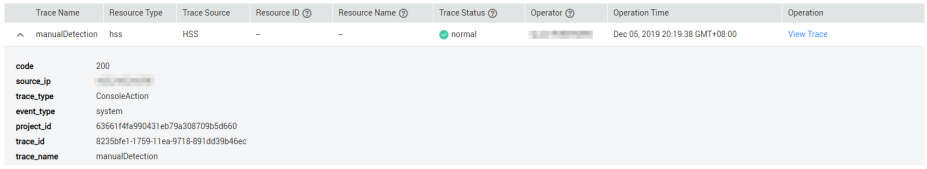
  – Ao selecionar **Trace name** para **Search By**, você também precisa selecionar um nome de rastreamento específico. Quando você seleciona **Resource ID** para **Search By**, também precisa selecionar ou inserir um ID de recurso específico. Ao selecionar **Resource name** para **Search By**, você também precisa selecionar ou inserir um nome de recurso específico.

- **Operator**: selecione um operador específico (um usuário que não seja locatário).
- **Trace Status**: as opções disponíveis incluem **All trace statuses**, **Normal**, **Warning** e **Incident**.
- **Time Range**: no canto superior direito da página, você pode consultar rastreamentos na última 1 hora, no último 1 dia, na última 1 semana ou dentro de um período personalizado.

Passo 5 Clique em **Query**.

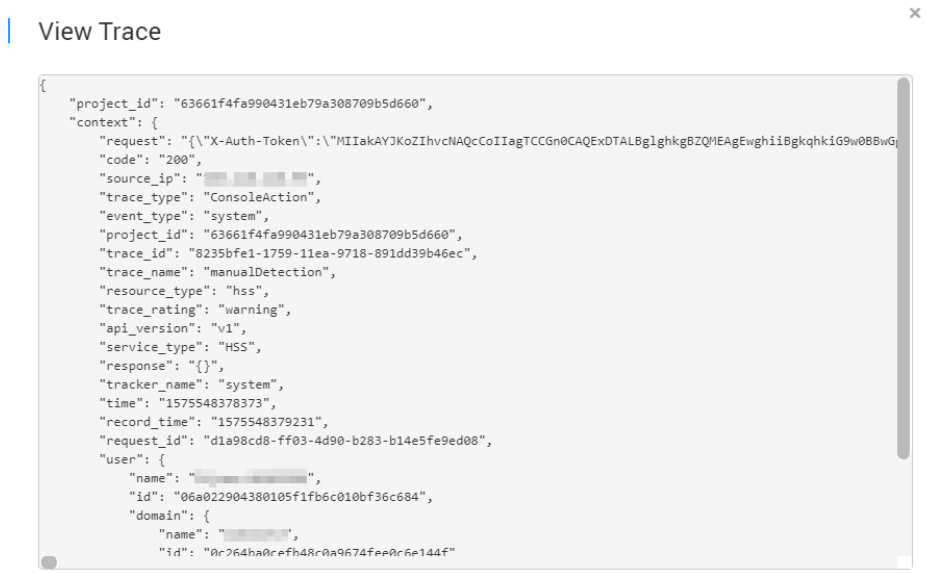
Passo 6 Clique em à esquerda de um rastreamento para expandir seus detalhes, conforme mostrado em **Figura 10-1**.

Figura 10-1 Expansão de detalhes do rastreamento



Passo 7 Clique em **View Trace** na coluna **Operation**. Na caixa de diálogo **View Trace** exibida, os detalhes da estrutura de rastreamento são exibidos.

Figura 10-2 Visualizar um rastreamento



----Fim

11 Monitoramento

11.1 Métricas de monitoramento do HSS

Descrição de recursos

Esta seção descreve as métricas relatadas pelo HSS para o Cloud Eye, bem como seus namespaces e dimensões. Você pode consultar as métricas e os alarmes gerados para o HSS no console do Cloud Eye ou usando as APIs fornecidas pelo Cloud Eye.

Namespace

SYS.HSS

Métricas

Tabela 11-1 Métricas do HSS

ID	Nome	Descrição	Intervalo de valor	Objeto monitorado	Período de monitoramento (métrica original)
host_num	Total Servers	Número total de servidores	≥ 0	Servidor	300s
unprotected_host_num	Unprotected Servers	Servidores para os quais a proteção não está ativada	≥ 0	Servidor	300s

ID	Nome	Descrição	Intervalo de valor	Objeto monitorado	Período de monitoramento (métrica original)
risky_host_num	Unsafe Servers	Número de servidores em que os riscos são detectados	≥ 0	Servidor	300s
uninstalled_or_offline_agent_num	Servers Without Agent Running	Número de servidores em que nenhum agente está instalado ou o agente está off-line	≥ 0	Servidor	300s

Dimensões

Tabela 11-2 Lista de dimensões

Chave	Valor
hss_enterprise_project_id	ID do projeto empresarial.

11.2 Configuração de uma regra de alarme de monitoramento

Você pode definir regras de alarme do HSS para personalizar os objetos monitorados e as políticas de notificação e definir parâmetros como o nome da regra de alarme, objeto monitorado, métrica, limite, período de monitoramento e se deseja enviar notificações. Isso ajuda você a aprender o status de proteção do HSS em tempo hábil.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Passe o mouse sobre no canto superior esquerdo da página e escolha **Management & Governance** > **Cloud Eye**.

Passo 4 No painel de navegação à esquerda, escolha **Alarm Management** > **Alarm Rules**.

Passo 5 No canto superior direito da página, clique em **Create Alarm Rule**.

Passo 6 Na página exibida, defina os parâmetros conforme solicitado.

Para obter mais informações, consulte **Criação de uma regra de alarme**. Os principais parâmetros são os seguintes:

- **Name**: nome da regra de alarme. O sistema gera um nome, que você pode modificar.
- **Resource Type**: **Host Security Service**
- **Dimension**: **Host Security**
- **Monitoring Scope**: escopo dos recursos aos quais a regra de alarme se aplica. Você pode selecionar **All resources** ou **Specific resources**.
- **Method**: selecione **Associate template**, **Use existing template** ou **Configure manually**.

  NOTA

  Depois que um modelo vinculado for modificado, as políticas contidas nessa regra de alarme a ser criada serão modificadas de acordo.
- **Alarm Policy**: política para acionar um alarme.

Passo 7 Configure a notificação de alarme.

Para enviar notificações de alarme por e-mail, SMS, HTTP ou HTTPS, ative **Alarm Notification** ( ).

Para obter mais informações, consulte **Criação de uma regra de alarme**. Os principais parâmetros são os seguintes:

Passo 8 Clique em **Create**.

----Fim

11.3 Visualização de métricas de monitoramento

O Cloud Eye pode monitorar os servidores protegidos pelo HSS. Você pode visualizar as métricas de monitoramento do HSS no console de gerenciamento.

Procedimento

Passo 1 **Efetue login no console de gerenciamento**.

Passo 2 Clique em no canto superior esquerdo do console de gerenciamento e selecione uma região ou um projeto.

Passo 3 Passe o mouse sobre no canto superior esquerdo da página e escolha **Management & Governance** > **Cloud Eye**.

Passo 4 No painel de navegação à esquerda, escolha **Cloud Service Monitoring** > **Host Security Service**.

Passo 5 Na coluna **Operation** de um ID de projeto empresarial, clique em **View Metric** para visualizar os detalhes da métrica de proteção do servidor do projeto.

----Fim

12 Gerenciamento de permissões

12.1 Criação de um usuário e concessão de permissões

Esta seção descreve o gerenciamento de permissões refinadas do IAM para seus recursos do HSS. Com **IAM**, você pode:

- Criar usuários do IAM para funcionários com base na estrutura organizacional da sua empresa. Cada usuário do IAM tem suas próprias credenciais de segurança, fornecendo acesso aos recursos do HSS.
- Conceder apenas as permissões necessárias para que os usuários executem uma tarefa específica.
- Confiar em uma conta ou serviço de nuvem da Huawei para realizar O&M profissional e eficiente em seus recursos do HSS.

Se sua conta da Huawei Cloud não exigir usuários individuais do IAM, pule este capítulo.

Esta seção descreve o procedimento para conceder permissões (consulte **Figura 12-1**).

Pré-requisito

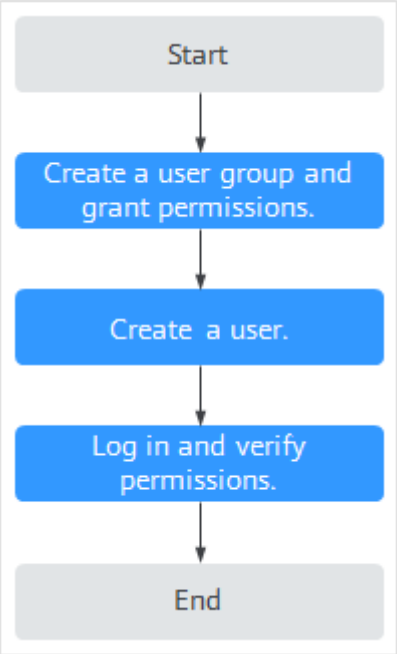
Antes de autorizar permissões para um grupo de usuários, você precisa saber quais permissões do HSS podem ser adicionadas ao grupo de usuários. A **Tabela 12-1** descreve os detalhes da política.

Tabela 12-1 Permissões definidas pelo sistema suportadas por HSS

Nome da função/ política	Descrição	Tipo	Dependência
HSS Administrator	Administrador do HSS, que tem todas as permissões do HSS	Função definida pelo sistema	• Depende da função **Tenant Guest**. Tenant Guest: um papel global, que deve ser atribuído no projeto global. • Para comprar cotas de proteção do HSS, você deve ter as funções **ECS ReadOnlyAccess**, **BSS Administrator** e **TMS ReadOnlyAccess**. – **ECS ReadOnlyAccess**: permissão de acesso somente leitura para o ECS. Esta é uma política do sistema. – **BSS Administrator**: uma função do sistema, que é o administrador de central de cobrança (BSS) e tem todas as permissões para o serviço. – **TMS ReadOnlyAccess**: uma política definida pelo sistema que concede acesso somente leitura ao TMS.
HSS FullAccess	Permissões completas para HSS	Política definida pelo sistema	Para comprar cotas de proteção do HSS, você deve ter a função **BSS Administrator**. **BSS Administrator**: uma função do sistema, que é o administrador de central de cobrança (BSS) e tem todas as permissões para o serviço. **SMN ReadOnlyAccess**: uma política definida pelo sistema que concede acesso somente leitura ao SMN.
HSS ReadOnlyAccess	Permissões somente leitura para o HSS.	Política definida pelo sistema	**SMN ReadOnlyAccess**: uma política definida pelo sistema que concede acesso somente leitura ao SMN.

Processo de autorização

Figura 12-1 Processo para conceder permissões



1. **Criar um grupo de usuários e atribuir permissões**. No console do IAM, conceda a permissão **HSS Administrator**.
2. **Criar um usuário e adicioná-lo ao grupo**. No console do IAM, adicione o usuário ao grupo criado em **1**.
3. **Fazer logon** e verificar as permissões.

   Efetue logon no console do HSS como o usuário criado e verifique se o usuário só tem permissões de leitura para HSS.

   Em L**Service List** no console, selecione quaisquer outros serviços (por exemplo, há apenas a política **HSS Administrator**). Se for exibida uma mensagem indicando que a permissão é insuficiente, a permissão **HSS Administrator** entrará em vigor.

12.2 Políticas personalizadas de HSS

Políticas personalizadas podem ser criadas para complementar as políticas de HSS definidas pelo sistema. Para obter detalhes sobre as ações suportadas por políticas personalizadas, consulte **Ações do HSS**.

Você pode criar políticas personalizadas usando um dos seguintes métodos:

- Editor visual: selecione serviços em nuvem, ações, recursos e condições de solicitação. Você não precisa ter conhecimento da sintaxe da política.
- JSON: crie uma política no formato JSON ou edite as cadeias JSON de uma política existente.

Para obter detalhes, consulte **Criação de uma política personalizada**. A seção a seguir contém exemplos de políticas personalizadas de HSS comuns.

Exemplos de políticas personalizadas

- Exemplo 1: permitir que os usuários consultem a lista de servidores protegidos

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "hss:hosts:list"
                                                        ]
                }
        ]
}
```

- Exemplo 2: negar a desinstalação do agente

  Uma política de negação deve ser usada em conjunto com outras políticas. Se as políticas atribuídas a um usuário contiverem "Allow" e "Deny", as permissões "Deny" terão precedência sobre as permissões "Allow".

  O método a seguir pode ser usado se você precisar atribuir permissões da política **HSS Administrator** a um usuário, mas também proibir o usuário de excluir pares de chaves (**hss:agent:uninstall**). Crie uma política personalizada com a ação para excluir pares de chaves, defina seu **Effect** como **Deny** e atribua esta política e a política **HSS Administrator** ao grupo ao qual o usuário pertence. Em seguida, o usuário pode realizar todas as operações no HSS, exceto a desinstalação. A seguir está um exemplo de política que nega a desinstalação do agente.

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Deny",
                        "Action": [

"hss:agent:uninstall"
                        ]
                },
        ]
}
```

- Políticas de múltiplas ações

  Uma política personalizada pode conter as ações de vários serviços que são do tipo de nível de projeto. A seguir está uma política com várias instruções:

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "hss:hosts:list"
                        ]
                },
               {
                        "Effect": "Allow",
                        "Action": [
                                "hss:hosts:switchVersion",
                                "hss:hosts:manualDetect",
                                "hss:manualDetectStatus:get"
                        ]
                }
        ]
}
```


12.3 Ações do HSS

Esta seção descreve o gerenciamento de permissões refinado para suas instâncias do HSS. Se sua conta da Huawei Cloud não precisar de usuários individuais do IAM, você pode pular esta seção.

Por padrão, os novos usuários do IAM não têm nenhuma permissão atribuída. Você precisa adicionar um usuário a um ou mais grupos e atribuir políticas ou funções a esses grupos. O usuário então herda as permissões dos grupos dos quais é membro. Esse processo é chamado de autorização. Após a autorização, o usuário pode executar operações especificadas em serviços de nuvem com base nas permissões.

Você pode conceder permissões aos usuários usando **funções** e **políticas**. As funções são fornecidas pelo IAM para definir permissões baseadas em serviço, dependendo das responsabilidades de trabalho do usuário. O IAM usa políticas para executar uma autorização refinada. Uma política define as permissões necessárias para executar operações em recursos de nuvem específicos sob determinadas condições.

Ações suportadas

O HSS fornece políticas definidas pelo sistema que podem ser usadas diretamente no IAM. Você também pode criar políticas personalizadas e usá-las para complementar políticas definidas pelo sistema, implementando um controle de acesso mais refinado. A seguir estão conceitos relacionados:

- Permissões: permitir ou negar determinadas operações.
- Ações: operações específicas que são permitidas ou negadas.
- Ações dependentes: ao atribuir permissões para uma ação, você também precisa atribuir permissões para as ações dependentes.

O HSS oferece suporte às seguintes ações que podem ser definidas em políticas personalizadas:

Ações

Permissão	Ação	Ação relacionada
Consultar a lista de servidores protegidos	hss:hosts:list	vpc:ports:get vpc:publicIps:list ecs:cloudServers:list
Ativar ou desativar a proteção em servidores	hss:hosts:switchVersion	-
Verificação manual	hss:hosts:manualDetect	-
Verificar o status de uma verificação manual	hss:manualDetectStatus:get	-
Consultar relatórios de verificação de senha fraca	hss:weakPwds:list	-

Permissão	Ação	Ação relacionada
Consultar relatórios de proteção contra quebra de conta	hss:accountCracks:list	-
Desbloquear um endereço IP que foi bloqueado durante a prevenção de quebra de conta	hss:accountCracks:unblock	-
Consultar resultados de verificação de programas maliciosos	hss:maliciousPrograms:list	-
Consultar resultados de verificação de logon remoto	hss:abnorLogins:list	-
Consultar relatórios de alterações de arquivos importantes	hss:keyfiles:list	-
Consultar a lista de portas abertas	hss:ports:list	-
Consultar a lista de vulnerabilidades	hss:vuls:list	-
Executar operações em lote em vulnerabilidades	hss:vuls:operate	-
Consultar a lista de contas	hss:accounts:list	-
Consultar a lista de software	hss:softwares:list	-
Consultar a lista de caminhos da Web	hss:webdirs:list	-
Consultar a lista de processos	hss:processes:list	-
Consultar relatórios de verificação de configuração	hss:configDetects:list	-
Consultar resultados da verificação de web shell	hss:Webshells:list	-
Consultar relatórios de verificação de conta arriscadas	hss:riskyAccounts:list	-

Permissão	Ação	Ação relacionada
Obter estatísticas de risco do servidor	hss:riskyDashboard:get	-
Consultar relatórios de verificação de política de complexidade de senha	hss:complexityPolicys:list	-
Executar operações em lote em programas maliciosos	hss:maliciousPrograms:operate	-
Executar operações em lote em portas abertas	hss:ports:operate	-
Executar operações em configurações inseguras detectadas	hss:configDetects:operate	-
Executar operações em lote em web shells	hss:Webshells:operate	-
Configurar localizações de logon comuns	hss:commonLocations:set	-
Consultar localizações de logon comuns	hss:commonLocations:list	-
Configurar endereços IP de logon comuns	hss:commonIPs:set	-
Consultar endereços IP de logon comuns	hss:commonIPs:list	-
Configurar a lista branca de endereços IP de logon	hss:whiteIps:set	-
Consultar a lista branca de endereços IP de logon	hss:whiteIps:list	-
Configurar senhas fracas	hss:weakPwds:set	-
Consultar senhas fracas	hss:weakPwds:get	-
Configurar caminhos da Web	hss:webDirs:set	-
Consultar caminhos da Web	hss:webDirs:get	-
Obter a lista de servidores em que a 2FA está ativada	hss:twofactorAuth:list	-
Ativar 2FA	hss:twofactorAuth:set	-

Permissão	Ação	Ação relacionada
Ativar ou desativar o isolamento automático e a eliminação de programas maliciosos	hss:automaticKillMp:set	-
Consultar os programas que foram automaticamente isolados e eliminados	hss:automaticKillMp:get	-
Consultar o endereço de download do agente	hss:installAgent:get	-
Desinstalar um agente	hss:agent:uninstall	-
Consultar alarmes do HSS	hss:alertConfig:get	-
Configurar alarmes do HSS	hss:alertConfig:set	-
Consultar a lista de WTP	hss:wtpHosts:list	vpc:ports:get vpc:publicIps:list ecs:cloudServers:list
Ativar ou desativar WTP	hss:wtpProtect:switch	-
Configurar servidores de backup	hss:wtpBackup:set	-
Consultar servidores de backup	hss:wtpBackup:get	-
Configurar diretórios protegidos	hss:wtpDirectorys:set	-
Consultar a lista de diretórios protegidos	hss:wtpDirectorys:list	-
Consultar registros de WTP	hss:wtpReports:list	-
Configurar processos privilegiados	hss:wtpPrivilegedProcess:set	-
Consultar a lista de processos privilegiados	hss:wtpPrivilegedProcesses:list	-
Configurar um modo de proteção	hss:wtpProtectMode:set	-
Consultar o modo de proteção	hss:wtpProtectMode:get	-

Permissão	Ação	Ação relacionada
Configurar um sistema de arquivo protegido	hss:wtpFilesystems:set	-
Consultar a lista do sistema de arquivo protegido	hss:wtpFilesystems:list	-
Configurar a proteção agendada	hss:wtpScheduledProtections:set	-
Consultar a proteção agendada	hss:wtpScheduledProtections:get	-
Configurar alarmes de WTP	hss:wtpAlertConfig:set	-
Consultar alarmes de WTP	hss:wtpAlertConfig:get	-
Consultar estatísticas de WTP	hss:wtpDashboard:get	-
Consultar grupos de políticas	hss:policy:get	-
Configurar um grupo de políticas	hss:policy:set	-
Consultar a lista de intrusões detectadas	hss:event:get	-
Executar operações em intrusões	hss:event:set	-
Consultar grupos de servidores	hss:hostGroup:get	-
Configurar grupos de servidores	hss:hostGroup:set	-
Monitorar a integridade do arquivo	hss:keyfiles:set	-
Consultar relatórios de alterações de arquivos importantes	hss:keyfiles:list	-
Consultar a lista de inicialização automática	hss:launch:list	-

13 (Opcional) Gerenciamento de projetos empresariais

13.1 Gerenciamento de projetos e projetos empresariais

As seleções estarão disponíveis somente se você tiver ativado a função do projeto empresarial ou se sua conta for uma conta empresarial. Para ativar essa função, entre em contato com seu gerente de clientes. Um projeto empresarial fornece um modo de gerenciamento de recursos de nuvem, no qual os recursos e os membros da nuvem são gerenciados centralmente pelo projeto.

Criar um projeto e atribuir permissões

- Criar um projeto

  Faça logon no console de gerenciamento, clique no nome de usuário no canto superior direito e selecione **Identity and Access Management**. No painel de navegação à esquerda, escolha **Projects**. No painel direito, clique em **Create Project**. Na página **Create Project** exibida, selecione uma região e insira um nome de projeto.

- Conceder permissões

  Você pode atribuir permissões (de recursos e operações) a grupos de usuários para vincular projetos a grupos de usuários. Você pode adicionar usuários a um grupo de usuários para controlar quais projetos eles podem acessar e em quais recursos eles podem executar operações. Para fazer isso, execute as seguintes operações:

  a. Na página **User Groups**, localize o grupo de usuários de destino e clique em **Configure Permission** na coluna **Operation**. A página **User Group Permissions** é exibida. Localize a linha que contém o projeto de destino, clique em **Configure Policy** e selecione as políticas necessárias para o projeto.

  b. Na página **Users**, localize o usuário de destino e clique em **Modify** na coluna **Operation**. Na área **User Groups**, adicione um grupo de usuários para o usuário.

Criar um projeto empresarial e atribuir permissões

- Criar um projeto empresarial

  No console de gerenciamento, clique em **Enterprise** no canto superior direito. A página **Enterprise Management** é exibida. No painel de navegação à esquerda, escolha

Enterprise Project Management. No painel direito, clique em **Create Enterprise Project** e insira um nome.

NOTA

Enterprise estará disponível no console de gerenciamento somente se você tiver ativado o projeto empresarial ou se tiver uma conta empresarial. Para ativar essa função, entre em contato com o atendimento ao cliente.

- Conceder permissões

  Você pode adicionar um grupo de usuários a um projeto empresarial e configurar uma política para vincular o projeto empresarial ao grupo de usuários. Você pode adicionar usuários a um grupo de usuários para controlar quais projetos eles podem acessar e em quais recursos eles podem executar operações. Para fazer isso, execute as seguintes operações:

  a. Localize a linha que contém o projeto empresarial de destino, clique em **More** na coluna **Operation** e selecione **View User Group**. Na página **User Groups** exibida, clique em **Add User Group**. Na caixa de diálogo **Add User Group** exibida, selecione os grupos de usuários que você deseja adicionar e mova-os para o painel direito. Clique em **Next** e selecione as políticas.

  b. No painel de navegação à esquerda, escolha **Personnel Management** > **User Management**. Localize a linha que contém o usuário de destino, clique em **More** na coluna **Operation** e selecione **Add to User Group**. Na caixa de diálogo **Add to User Group** exibida, selecione os grupos de usuários para os quais as políticas foram configuradas e clique em **OK**.

- Vincular HSS a projetos empresariais

  Você pode usar projetos empresariais para gerenciar recursos de nuvem.

  – Selecione um projeto empresarial ao comprar HSS.

    Na página para compra de HSS, selecione um projeto empresarial na lista suspensa **Enterprise Project**.

  – Adicionar recursos

    Na página **Enterprise Project Management**, você pode adicionar ECSs/BMSs existentes a um projeto empresarial.

    Valor **default** indica o projeto empresarial padrão. Os recursos que não estão alocados a nenhum projeto empresarial na sua conta são exibidos no projeto empresarial padrão.

  Para obter mais informações, consulte **Criação de um projeto empresarial**.

13.2 Gerenciamento de todas as configurações de projetos

Se você tiver ativado a função de projeto empresarial, poderá selecionar **All projects** na lista suspensa **Enterprise Project** e definir em lote todos os servidores em todos os seus projetos.

- Vinculação de cotas a servidores

  Em **All projects**, você pode vincular a cota de um projeto empresarial a um servidor de outro projeto. O projeto ao qual a cota pertence será cobrado pela cota.

- Instalação e configuração em lote

  Configure a lista branca de alarmes, a lista branca de logon, o isolamento e a eliminação de programas maliciosos e as notificações de alarme para todos os servidores.

- Aplicação de um grupo de políticas

  Os grupos de políticas em **All projects** podem ser aplicados a qualquer servidor em qualquer projeto empresarial protegido pela edição premium.

  Os grupos de políticas em **All projects** não pertencem a nenhum projeto específico e não afetam os grupos de políticas em nenhum outro projeto.
- Assinatura de relatórios de segurança em **All projects**

  Os relatórios de segurança em **All projects** não pertencem a nenhum projeto específico e não afetam os relatórios de segurança em nenhum outro projeto.

Você pode definir configurações uniformes para todos os projetos em **All projects** e personalizar as configurações em um projeto específico. As definições de um projeto empresarial não afetam as de outros projetos empresariais.

Pré-requisitos

Você tem as permissões **Tenant Administrator** ou **HSS Administrator+Tenant Guest**.

Vinculação de cotas a servidores

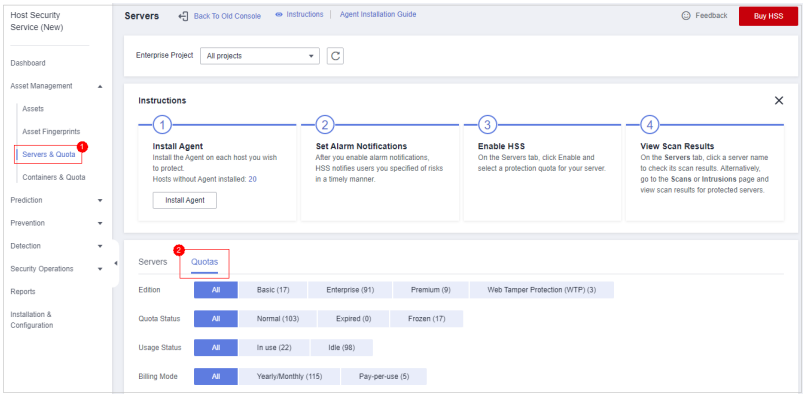
Execute as etapas a seguir para vincular a cota de edição WTP a um servidor em **All projects**.

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**.

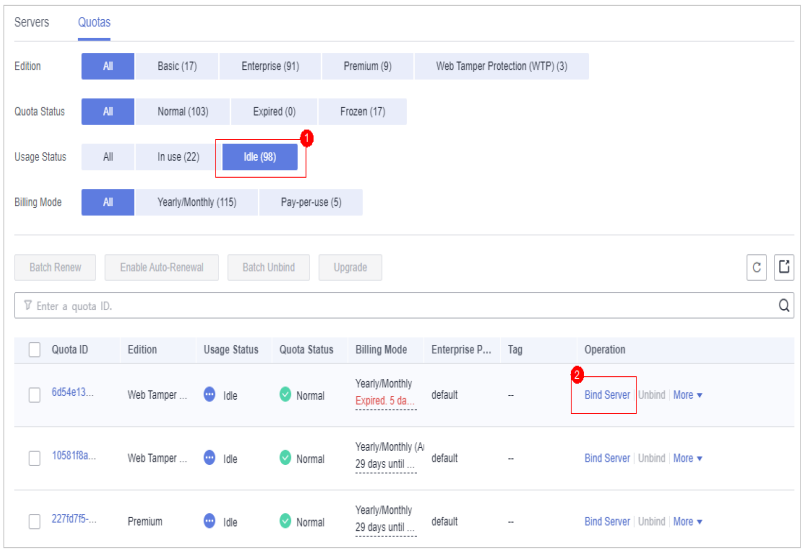
Passo 3 Escolha **Asset Management** > **Servers & Quota** e clique em **Quotas**. As cotas de proteção do servidor são exibidas, conforme mostrado em **Figura 13-1**.

Figura 13-1 Cotas de proteção



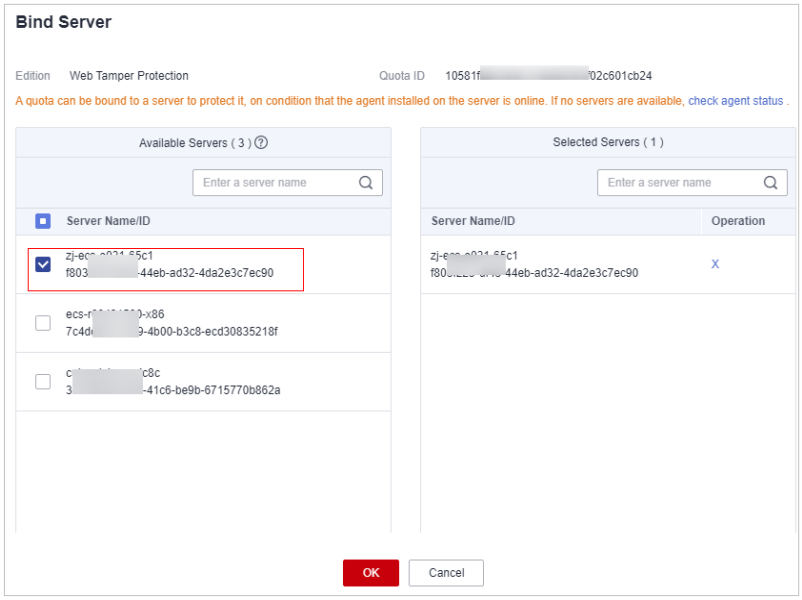
Passo 4 Na lista de cotas, selecione uma cota cujo **Usage Status** seja **Idle** e clique em **Bind Server**.

Figura 13-2 Vinculação da cota a um servidor



Passo 5 Selecione servidores na caixa de diálogo **Bind Server**.

Figura 13-3 Selecionar servidores



Passo 6 Clique em **OK**. O **Protection Status** do servidor mudará para **Enabled**.

----Fim

Vinculação de cotas a containers

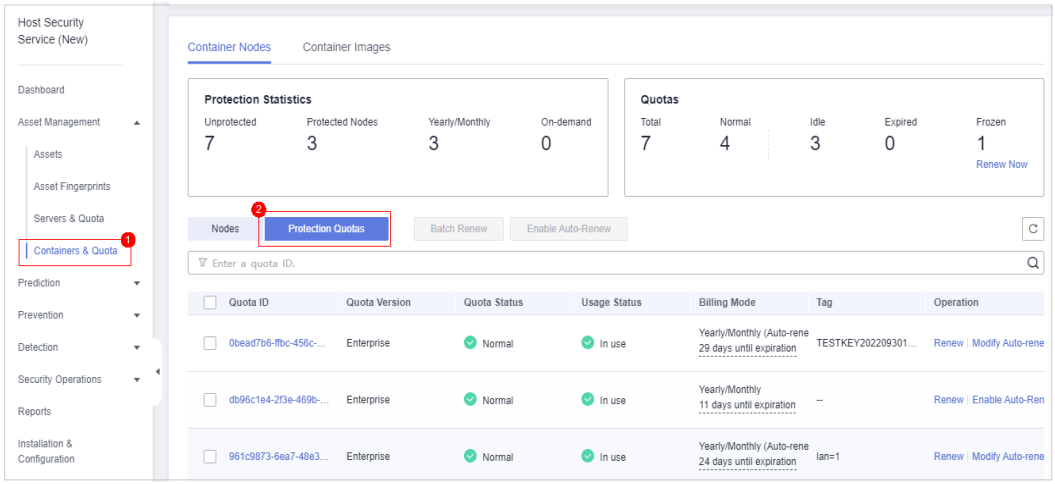
Execute as etapas a seguir para vincular a cota de edição de container a um servidor em **All projects**.

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 **Asset Management** > **Containers & Quota** e clique em **Protection Quotas**. As cotas de proteção do servidor são exibidas, conforme mostrado em **Figura 13-4**.

Figura 13-4 Cotas de proteção de containers



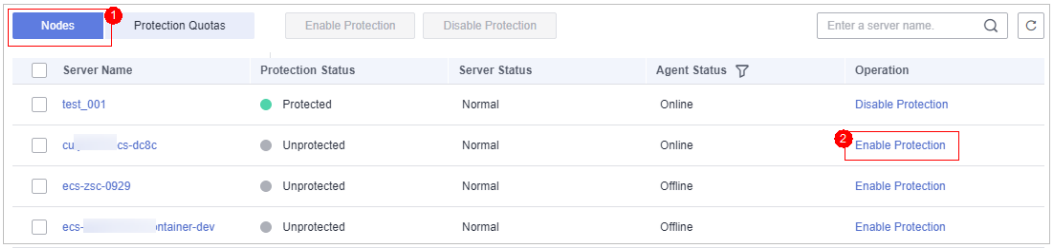
Passo 4 Na lista de cotas, selecione uma cota cujo **Usage Status** seja **Idle** e clique em **Bind Server**.

Passo 5 Clique na guia **Nodes**. Localize o servidor de destino e clique em **Enable Protection** na coluna **Operation**.

NOTA

O status do servidor a ser protegido deve ser **Normal** e o status do agente deve ser **Online**.

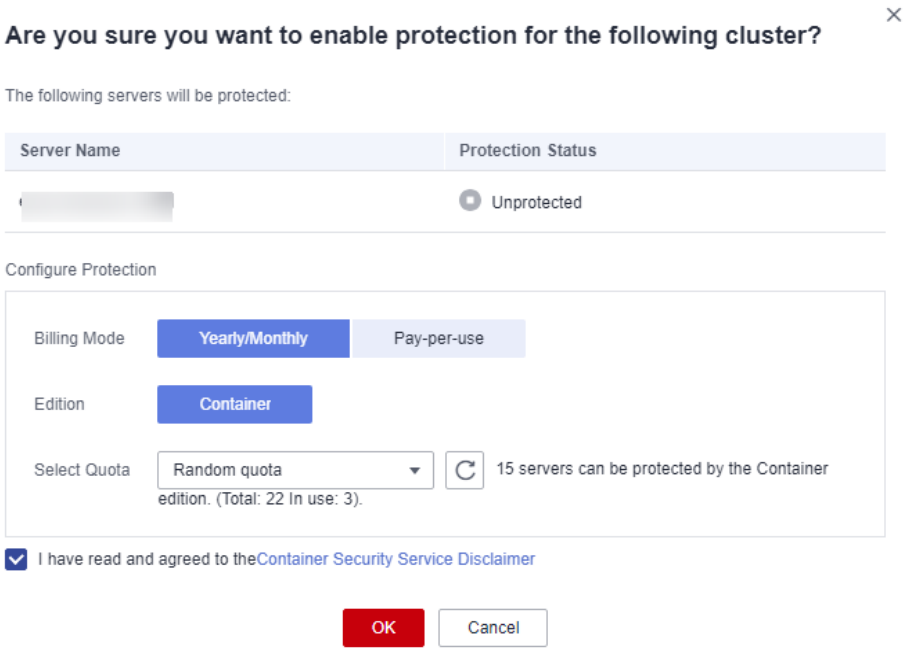
Figura 13-5 Vinculação da cota de container a um servidor



Passo 6 Selecione servidores na caixa de diálogo **Bind Server**.

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 13-6 Ativar a proteção anual/mensal



A cota pode ser alocada das seguintes maneiras:

- **Selecionar uma cota aleatoriamente**: deixe o sistema alocar a cota com a validade restante mais longa para o servidor.
- Selecione um ID de cota e atribua-o a um servidor.

Passo 7 Clique em **OK**. O **Protection Status** do servidor mudará para **Enabled**.

----Fim

A História de mudanças

Lançado em	Descrição
27/10/2023	Este é o décimo oitavo lançamento oficial. Adição de: ● **Gerenciamento de agentes de cluster** ● **Controle de processo de aplicação** ● **Proteção do cluster de containers** ● **Monitoramento** ● **Exportação de alarmes do servidor** ● **Exportação de alarmes de container** ● **Verificação do histórico de tratamento de alarmes** Otimização de: ● Revisão de **Painel**. ● Adição dos seguintes tipos de alarme a **Alarmes do servidor**: execução de processo suspeito, acesso a arquivos de processo suspeito, conexão de saída anormal e encaminhamento de porta ● Adição dos seguintes tipos de alarme a **Eventos de alarme de container**: ferramenta hacker, escalonamento de privilégios de arquivo, alteração importante de arquivo, comportamento anormal de processo, execução de comandos suspeitos, roubo de senha de usuário, conexão de saída anormal e encaminhamento de porta ● A prevenção de ransomware e o backup de ransomware podem ser ativados separadamente em **Prevenção contra ransomware**. ● Regras definidas pelo usuário podem ser adicionadas à lista branca de alarmes e alarmes duplicados podem ser tratados em lotes em **Manipulação de alarmes do servidor**. ● Regras definidas pelo usuário podem ser adicionadas à lista branca de alarmes e alarmes duplicados podem ser tratados em lotes em **Manipulação de alarmes de container**. ● Backup antes que a correção de vulnerabilidades seja ativado em **Manipulação de vulnerabilidades**.

Lançado em	Descrição
25/07/2023	Esta edição é o décimo sétimo lançamento oficial. Adição de: ● **Firewalls de container** ● **Configuração da lista branca de usuários do sistema** ● **Visualização de informações do container** ● **Manuseio de containers de risco** ● **Visualização do histórico de tratamento de vulnerabilidades** Otimização de: ● **Verificação de segurança de logon**: adição da configuração da lista branca de quebra de força bruta. ● **Visualização de cotas**: suporte a visualização dos servidores vinculados às cotas de container. ● **Visualização de detalhes da verificação da linha de base**: adição da descrição da diferença sobre as versões do MySQL. ● **Adição de um diretório protegido**: adição da descrição sobre restrições em subdiretórios excluídos e exportação de diretórios protegidos. ● **Vinculação de uma cota de proteção**: suporte a vinculação de cota de container. ● **Desvinculação de uma cota de um servidor**: suporte a desvinculação de cota de container. ● **Visão geral da verificação da linha de base**: adição da descrição da seleção de políticas diferentes e da visualização dos resultados da detecção. ● **Visualização de detalhes da verificação da linha de base**: adição da descrição da seleção de políticas diferentes e da visualização dos resultados da detecção. ● **Imagens locais**: suporte a exportação de relatórios de vulnerabilidade. ● **Gerenciamento de imagens privadas do SWR**: suporte a exportação de relatórios de vulnerabilidade, verificação de conformidade de software e detecção de informações de imagem de base. ● **Gerenciamento de imagens compartilhadas do SWR**: suporte a exportação de relatório de vulnerabilidades e verificação de segurança. ● **Eventos de alarme de container**: suporte a detecção e relatórios de alarmes para escalonamento de privilégios de processo, quebra de força bruta, contas de usuário do sistema não autorizadas e execução de comandos de alto risco. ● **Detecção de arquivos maliciosos**: suporte a bloqueio automático de shells reversos. ● **Visualização de um grupo de políticas**: adição de autoproteção automática. ● **Ativação de notificações de alarme**: adição do alarme do agente desinstalado à notificação diária de alarme.

Lançado em	Descrição
	● **Restauração de dados do servidor**: adição da descrição dos propósitos de backup. ● **Gerenciamento de vulnerabilidades**: otimização do processo de operação e suporte a adição de vulnerabilidades à lista branca. ● **Impressões digitais do servidor**: suporte ao middleware, aplicações Web e bancos de dados em execução no Windows. ● **Impressões digitais de containers**: suporte a contas, bancos de dados, clusters, serviços, cargas de trabalho e containers. ● **Atualização manual de informações de ativos de containers em tempo real**: suporte a clusters, serviços, cargas de trabalho e containers.
15/06/2023	Esta edição é o décimo sexto lançamento oficial. Otimização de: ● Adição de detecção de vulnerabilidades para um único servidor em **Verificação de vulnerabilidade**. ● Adição da operação de visualização de vulnerabilidades em um único servidor em **Visualização de detalhes da vulnerabilidade**.
01/06/2023	Este é o décimo quinto lançamento oficial. Alteração do nome da edição avançada do HSS para edição profissional.
24/05/2023	Este é o décimo quarto lançamento oficial. Otimização de: ● Otimização de **Configuração da importância do ativo**. ● Otimização de restrições em **Imagens do container**. ● Otimização de **Visualização de detalhes do plug-in**.
27/04/2023	Esta edição é o décimo terceiro lançamento oficial. Adição de: ● 2.4.3.2-Verificação de vulnerabilidades (automática) ● **Compra de um cofre de backup** Otimização de: Otimização de pré-requisitos em **Ativação da prevenção de ransomware**.

Lançado em	Descrição
31/03/2023	Esta edição é o décimo primeiro lançamento oficial. Adição da descrição sobre: ● As funções e políticas suportadas pela edição avançada. ● Recursos de detecção, como detecção AV e detecção de HIPS em grupos de políticas. ● Novos tipos de alarmes de detecção de intrusão, como cavalos de Troia, vírus e worms. ● O recurso de detecção de honeypot para servidores do Windows. ● Atualização de ativos do servidor (manual). ● Gerenciamento unificado de contas. ● Intervalos definidos pelo usuário nas políticas de ativos. ● Instalação do plug-in
18/01/2023	Este é o décimo lançamento oficial. Adição das seguintes seções: ● **Imagens locais** ● **Gerenciamento de imagens compartilhadas do SWR** ● **Visualização de impressões digitais de ativos de containers** ● **Gerenciamento de políticas** ● **Adição de um processo privilegiado** ● **Instalação de um agente em vários servidores (com diferentes contas e senhas de servidor)** ● **Atualização do agente** Adição do seguinte conteúdo: ● A política de arquivos maliciosos da edição empresarial do HSS suportava a detecção de shell reverso. ● A lista de programas e os nomes dos pacotes podem ser visualizados. ● O tempo e o período de detecção podem ser personalizados para as políticas de detecção de ativos. ● Alarmes do rootkit ● Os riscos na configuração da linha de base podem ser corrigidos no modo com um clique.
10/12/2022	Este é o nono lançamento oficial. Modificação de: ● **Prevenção de ransomware** ● **Ativação da prevenção de ransomware** ● **Managing Ransomware Prevention Policies** ● **Desabilitação da prevenção de ransomware**

Lançado em	Descrição
10/11/2022	Este é o oitavo lançamento oficial. Adição das seguintes seções: **Verificação gratuita em servidores desprotegidos** **Verificação de vulnerabilidade**
11/10/2022	Este é o sétimo lançamento oficial. Adição de **Atualização de sua edição**.
30/09/2022	Este é o sexto lançamento oficial. Adição das seguintes seções: **Habilitação da proteção** **Desativação da proteção** **Instalação de agentes em lotes (com a mesma conta de servidor e senha)**
20/09/2022	Este é o quinto lançamento oficial. Adição da edição básica (anual/mensal) na página de compra.
31/08/2022	Este é o quarto lançamento oficial. Modificação da descrição sobre a edição básica. A edição básica pode ser usada gratuitamente dentro de um período específico.
28/07/2022	Este é o terceiro lançamento oficial. Adição da função de proteção de aplicações. Esta função está disponível nas seguintes regiões: CN-Hong Kong, AP-Bangkok e AP-Singapore. A prevenção de ransomware é suportada no Windows.
05/07/2022	Esta edição é o segundo lançamento oficial. Adição de descrição sobre a especificação da importância do ativo. Adição de descrição sobre a exportação de itens de verificação de linha de base. Adição de descrição sobre a detecção de vulnerabilidades de aplicações.
30/05/2022	Esta edição é o primeiro lançamento oficial.

