Host Security Service

Melhores práticas

Edição	01
Data	2024-09-29

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 Melhores práticas de reforço da segurança de logon

A quebra de contas e senhas são as formas mais usadas para os invasores invadirem ou atacarem servidores. Aprimorar a segurança de logon é o primeiro passo para proteger a segurança do servidor e garantir que os serviços possam ser executados corretamente.

Pré-requisitos

Você comprou um ECS e ativou a proteção para ele.

Funções de reforço da segurança de logon

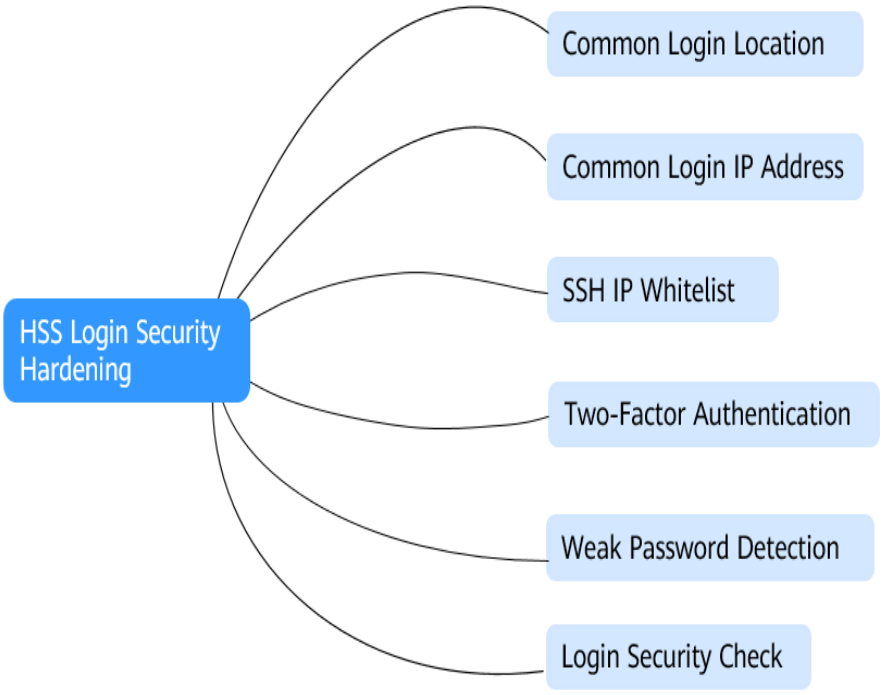
Você pode configurar locais comuns de logon, endereços IP comuns de logon, lista branca de endereços IP de logon SSH, autenticação de dois fatores, verificação de senha fraca e verificação de segurança de logon para proteger a segurança de logon.

Para garantir alta segurança de logon, é aconselhável configurar todas essas funções.

NOTA

A autenticação de logon de dois fatores é suportada pela edição básica do HSS, cobrada no modo anual/mensal, pela edição empresarial ou superior. A verificação de segurança de logon é suportada pela edição empresarial do HSS ou superior. Outras funções de proteção estão disponíveis na edição básica do HSS.

Figura 1-1 Funções de reforço de segurança de logon do HSS



Configuração de locais de logon comuns

Depois que os locais de logon comuns forem configurados, o HSS gerará alarmes para logons em ECSs em locais de logon não comuns. Você pode adicionar vários locais de logon comuns para cada ECS.

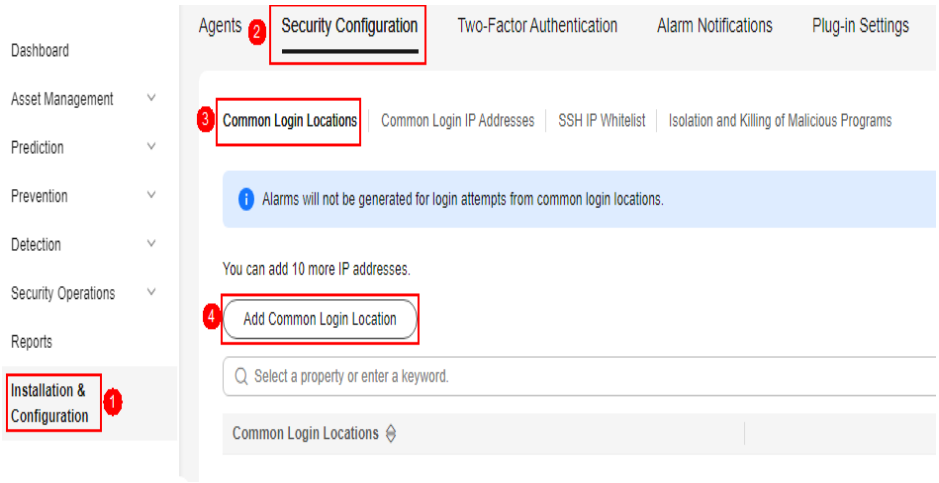
Restrições

Uma conta pode adicionar até 10 locais de logon comuns.

Procedimento

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

Figura 1-2 Adição de um local de logon comum



Passo 2 Na caixa de diálogo que é exibida, selecione um local geográfico e selecione servidores. Confirme as informações e clique em **OK**.

Passo 3 Retorne à guia **Security Configuration** da página **Installation & Configuration**. Verifique se os locais adicionados são exibidos na subguia **Common Login Locations**.

----Fim

Configuração do endereço IP de logon comum

Depois que você configurar endereços IP de logon comuns, o HSS gerará alarmes sobre os logons de outros endereços IP de logon.

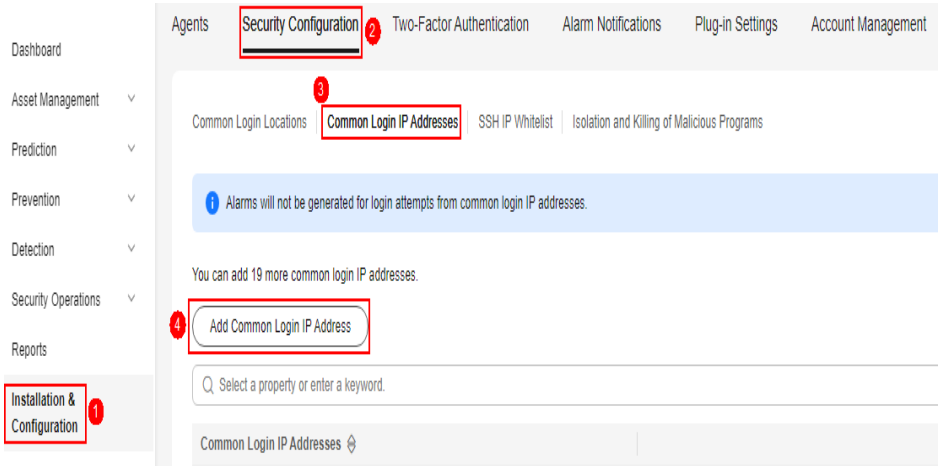
Restrição

Uma conta pode adicionar até 20 endereços IP comuns de logon.

Procedimento

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 1-3 Adição de 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.
- 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.

Passo 3 Retorne à guia **Security Configuration** da página **Installation & Configuration**. Verifique se os locais adicionados são exibidos na subguia **Common Login IP Addresses**.

----Fim

Configuração da lista branca de endereços IP de logon SSH

A lista branca de logon SSH controla o acesso SSH aos servidores, evitando a quebra da conta.

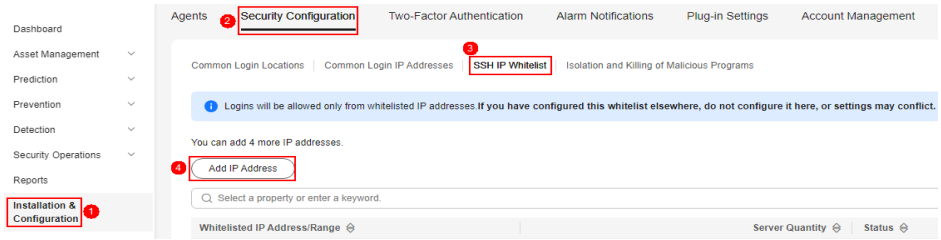
NOTA

- Uma conta pode ter até 10 endereços IP de logon SSH na lista branca.
- A lista branca de endereços IP SSH não entra em vigor para servidores que executam o Kunpeng EulerOS (EulerOS com Arm).
- Depois de configurar uma lista branca de endereço 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 precisar acessar um servidor, mas não necessariamente via SSH, não será necessário adicionar o endereço IP dele 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 1-4 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.
- 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.

Passo 3 Retorne à guia **Security Configuration** da página **Installation & Configuration**. Verifique se os locais adicionados são exibidos na subguia **Common Login IP Addresses**.

----Fim

Configuração da autenticação de dois fatores

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

Você tem que escolher um tópico de 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.

- Os servidores Linux exigem senhas de usuário para logon.
- Em um servidor Windows, a 2FA pode entrar em conflito com o G01 e o 360 Guard (edição do servidor). É aconselhável pará-los.

Restrições

- Se a 2FA estiver ativada, você não poderá fazer logon nos servidores que executam uma GUI Linux.
- Se você tiver ativado a 2FA em um servidor Linux, não poderá fazer logon nele por meio do CBH.
- A 2FA é suportada apenas quando a versão de OpenSSH do Linux é anterior à 8.

Procedimento

Passo 1 Escolha **Installation & Configuration** > **Two-Factor Authentication**.

- Localize o servidor de destino e clique em **Enable 2FA** na coluna **Operation**.
- Selecione vários servidores de destino e clique em **Enable 2FA** para ativar a autenticação de dois fatores para vários servidores em lotes.

Passo 2 Na caixa de diálogo exibida, selecione um modo de verificação.

- **SMS/Email**

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

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

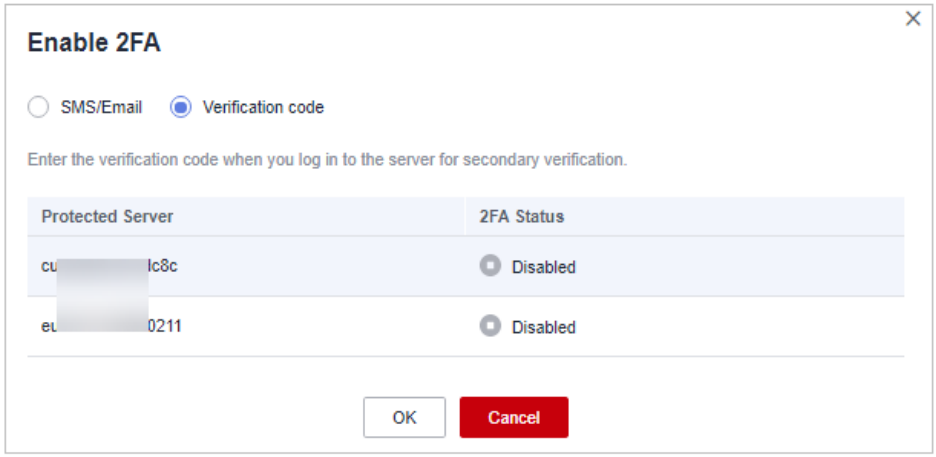
  – Se não houver nenhum tópico, clique em **View** para criar um. Para obter detalhes, consulte **Criação de um tópico**.

  – 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.

- **Verification code**

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

Figura 1-5 Código de verificação



Passo 3 Clique em **OK**.

Passo 4 Retorne à guia **Two-Factor Authentication** da página **Installation & Configuration**. Verifique se o **2FA Status** do servidor de destino é alterado para **Enabled**.

Demora cerca de 5 minutos para que a função de autenticação de dois fatores entre em vigor.

AVISO

Quando você faz logon em um servidor Windows remoto a partir de outro servidor 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

Configuração da detecção de senhas fracas

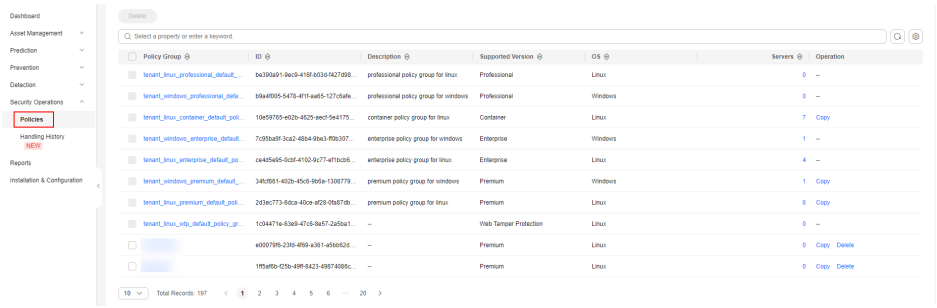
Senhas fracas não são atribuídas a um certo tipo de vulnerabilidade, mas elas não trazem menos riscos de segurança do que qualquer tipo de vulnerabilidade.

Dados e programas se tornarão inseguros se suas senhas forem quebradas.

O HSS detecta proativamente as contas que usam senhas fracas e gera alarmes para essas 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 Escolha **Security Operation** > **Policies**.

Figura 1-6 Acesso à página do grupo de políticas



Passo 2 Clique no nome do grupo de políticas de destino. A página do grupo de políticas é exibida.

Você pode determinar o sistema operacional e a versão de proteção suportados pela política de destino com base em seu **Policy Group Name** e **Supported Version** padrão.

NOTA

Se você precisar criar um grupo de políticas, execute esta etapa após **Criação de um grupo de políticas**.

Passo 3 Na lista de grupos de políticas, clique em **Weak password detection**.

Passo 4 A caixa de diálogo **Weak Password Detection** é exibida. Você pode modificar os parâmetros na área **Policy Settings** ou manter os valores padrão (recomendado). Para obter detalhes sobre os parâmetros, consulte **Tabela 1-1**.

Tabela 1-1 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.
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 5 Confirme as informações e clique em **OK**.

Passo 6 Escolha **Asset Management** > **Servers & Quota**, clique em **Servers**, selecione os servidores de destino e clique em **Apply Policy** acima da lista de servidores.

NOTA

Se você precisar implementar a mesma política para vários servidores ao mesmo tempo, certifique-se de que o **OS** e a **Edition** dos servidores selecionados sejam os mesmos da política de destino.

Passo 7 Na caixa de diálogo de implementação de políticas, selecione o grupo de políticas de destino e clique em **OK**.

Passo 8 Depois que a implementação for concluída, escolha **Security Operations** > **Policies**. Localize a política de destino, clique no valor na coluna **Servers** e verifique se os servidores que você adicionou são exibidos.

NOTA

Após a conclusão da implementação, aguarde cerca de 1 minuto e, em seguida, verifique se a implementação foi bem-sucedida.

----Fim

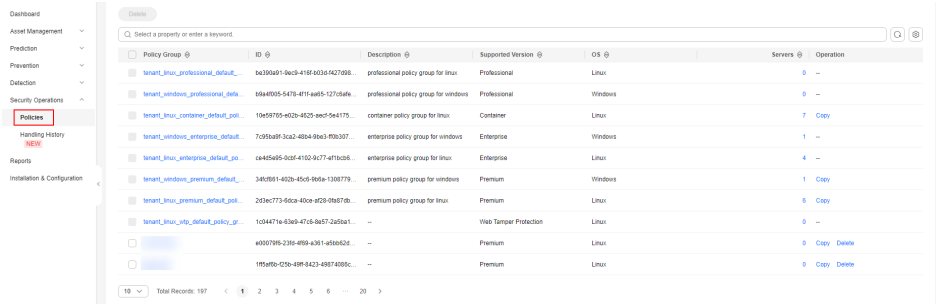
Configuração da verificação de segurança de logon

Depois que a segurança de logon for configurada, você poderá ativar a verificação de segurança de logon para o servidor de destino. O HSS detectará efetivamente ataques de força bruta, bloqueará automaticamente endereços IP de força bruta e acionará e relatará alarmes.

> **NOTA**
>
> Somente a edição empresarial e posteriores suportam a verificação de segurança de logon. Para a edição empresarial, a verificação de segurança de logon é realizada com base nos parâmetros padrão e a configuração de parâmetros personalizados não é suportada.

Passo 1 Escolha **Security Operation** > **Policies**.

Figura 1-7 Acesso à página do grupo de políticas



Passo 2 Clique no nome do grupo de políticas de destino. A página do grupo de políticas é exibida.

Você pode determinar o sistema operacional e a versão de proteção suportados pela política de destino com base em seu **Policy Group Name** e **Supported Version** padrão.

> **NOTA**
>
> Se você precisar criar um grupo de políticas, execute esta etapa após **Criação de um grupo de políticas**.

Passo 3 Clique em **Login Security Check** na lista de políticas.

Passo 4 A caixa de diálogo **Login Security Check** é exibida. Você pode modificar os parâmetros na área **Policy Settings** ou manter os valores padrão. Para obter detalhes sobre os parâmetros, consulte **Tabela 1-2**.

Figura 1-8 Modificar a política de verificação de segurança

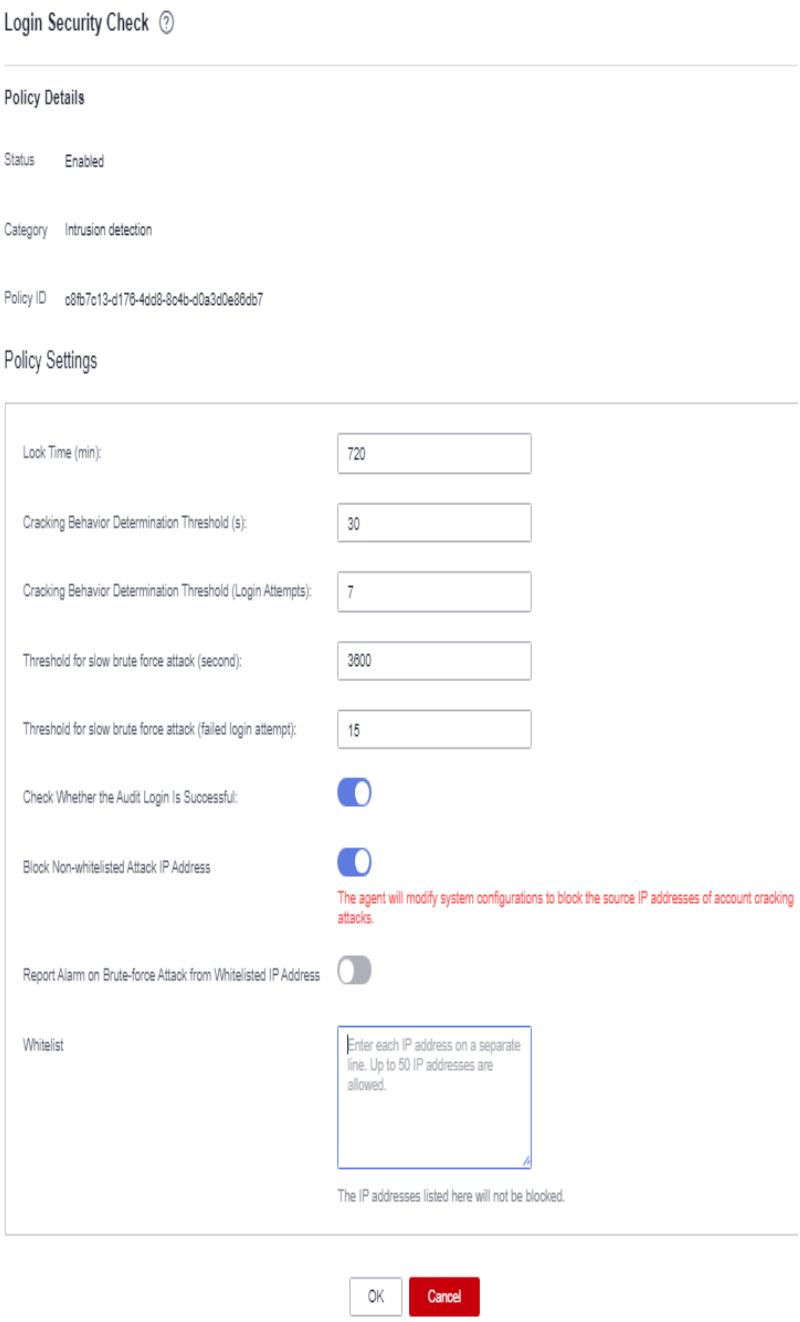


Tabela 1-2 Descrição do parâmetro

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

Passo 6 Escolha **Asset Management** > **Servers & Quota**, clique em **Servers**, selecione os servidores de destino e clique em **Apply Policy** acima da lista de servidores.

NOTA

Se você precisar implementar a mesma política para vários servidores ao mesmo tempo, certifique-se de que o **OS** e a **Edition** dos servidores selecionados sejam os mesmos da política de destino.

Passo 7 Na caixa de diálogo de implementação de políticas, selecione o grupo de políticas de destino e clique em **OK**.

Passo 8 Depois que a implementação for concluída, escolha **Security Operations** > **Policies**. Localize a política de destino, clique no valor na coluna **Servers** e verifique se os servidores que você adicionou são exibidos.

NOTA

Após a conclusão da implementação, aguarde cerca de 1 minuto e, em seguida, verifique se a implementação foi bem-sucedida.

----Fim

2 Detecção e correção de vulnerabilidades

2.1 Vulnerabilidade de divulgação de credenciais do Git (CVE-2020-5260)

O Git emitiu um boletim de segurança anunciando uma vulnerabilidade que poderia revelar as credenciais de usuário do Git (CVE-2020-5260). O Git usa um auxiliar de credenciais para armazenar e recuperar credenciais.

Mas quando um URL contém uma nova linha codificada (%0a), ele pode injetar valores inesperados no fluxo de protocolo do auxiliar de credenciais. Essa vulnerabilidade é acionada quando a versão afetada do Git é usada para executar um comando git clone em um URL malicioso.

ID da vulnerabilidade

CVE-2020-5260

Nome da vulnerabilidade

Vulnerabilidade de divulgação de credenciais do Git

Escopo do impacto

Versões afetadas:

- Git 2.17.x <= 2.17.3
- Git 2.18.x <= 2.18.2
- Git 2.19.x <= 2.19.3
- Git 2.20.x <= 2.20.2
- Git 2.21.x <= 2.21.1
- Git 2.22.x <= 2.22.2
- Git 2.23.x <= 2.23.1
- Git 2.24.x <= 2.24.1

- Git 2.25.x <= 2.25.2
- Git 2.26.x <= 2.26.0

Versões não afetadas:

- Git 2.17.4
- Git 2.18.3
- Git 2.19.4
- Git 2.20.3
- Git 2.21.2
- Git 2.22.3
- Git 2.23.2
- Git 2.24.2
- Git 2.25.3
- Git 2.26.1

Solução oficial

Essa vulnerabilidade foi corrigida na versão oficial mais recente. Se sua versão de serviço estiver dentro do intervalo afetado, atualize-a para a versão segura mais recente.

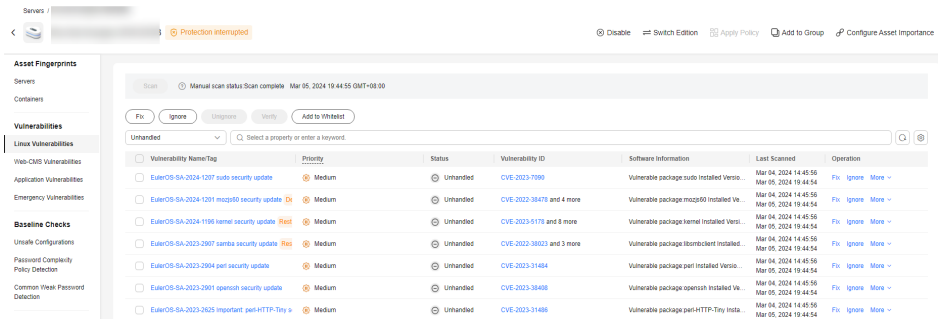
Endereço para download: **https://github.com/git/git/releases**

Sugestão

Execute as etapas a seguir para verificar e corrigir uma vulnerabilidade.

Passo 1 Detecte e visualize os detalhes da vulnerabilidade, conforme mostrado em **Inicialização manual de uma verificação de vulnerabilidades**. Para obter detalhes, consulte **Visualização de detalhes de vulnerabilidades**.

Figura 2-1 Inicialização manual de uma verificação de vulnerabilidades



Passo 2 Corrija as vulnerabilidades e verifique o resultado. Para obter detalhes, consulte **Manipulação de vulnerabilidades**.

----Fim

Outras medidas de proteção

Se você não pode realizar a atualização no momento, você pode tomar as seguintes medidas:

- Desative o auxiliar de credenciais executando os seguintes comandos:

  git config --unset credential.helper

  git config --global --unset credential.helper

  git config --system --unset credential.helper
- Fique atento aos URLs maliciosos.
  a. Examine o nome do servidor e a parte do nome do usuário dos URLs alimentados ao **git clone** para a presença de novas linhas codificadas (%0a) ou evidências de injeções de protocolo de credenciais (exemplo: **host=github.com**).
  b. Evite usar submódulos com repositórios não confiáveis (não use **clone –recurse-submodules**; use **git submodule update** somente após examinar os URLs encontrados em gitmodules).
  c. Evite ferramentas que podem executar o git clone.

2.2 Vulnerabilidades de execução remota de comando de SaltStack (CVE-2020-11651 e CVE-2020-11652)

Pesquisadores de segurança descobriram duas vulnerabilidades sérias nos produtos do SaltStack. O SaltStack fornece um conjunto de ofertas de produtos escritos em Python para O&M automática de C/S. Uma das duas vulnerabilidades descobertas é a vulnerabilidade de bypass de autenticação (CVE-2020-11651) e a outra é a vulnerabilidade de passagem de diretório (CVE-2020-11652). Os invasores podem explorar as vulnerabilidades para executar comandos remotamente, ler qualquer arquivo no servidor e obter informações confidenciais.

Se você é um usuário do SaltStack, verifique seu sistema e implemente o fortalecimento da segurança em tempo hábil.

ID de vulnerabilidade

- CVE-2020-11651
- CVE-2020-11652

Nome de vulnerabilidade

Vulnerabilidade de execução remota de comandos do SaltStack

Escopo do impacto

Versões afetadas:

- Versões anteriores ao SaltStack 2019.2.4
- Versões anteriores ao SaltStack 3000.2

Versões não afetadas:

- SaltStack 2019.2.4
- SaltStack 3000.2

Solução oficial

- Essas vulnerabilidades foram corrigidas na versão oficial mais recente. Se sua versão de serviço estiver dentro do intervalo afetado, atualize-a para a versão segura mais recente.

Endereço de download: **https://repo.saltstack.com**

- As portas de escuta padrão do Salt Master são 4505 e 4506. Você pode configurar regras de grupo de segurança que proíbam a abertura das duas portas para redes públicas ou que permitam que apenas objetos confiáveis se conectem às portas.

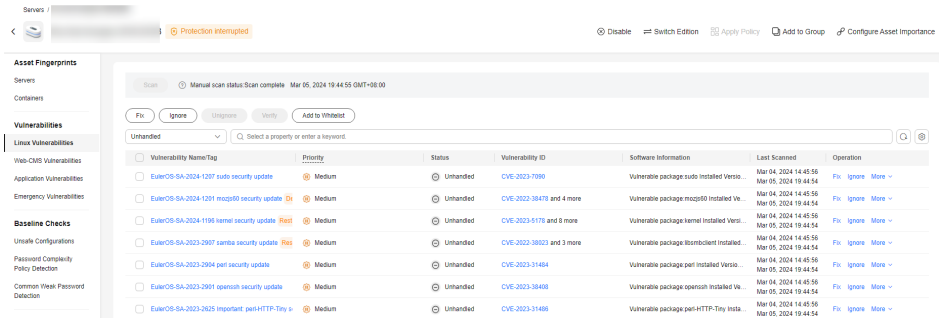
Sugestão

Execute as etapas a seguir para verificar e corrigir uma vulnerabilidade.

- Detecte e visualize detalhes do sistema. Para obter detalhes, consulte **Visualização de detalhes de vulnerabilidades**.

  Corrija as vulnerabilidades e verifique o resultado. Para obter detalhes, consulte **Manipulação de vulnerabilidades**.

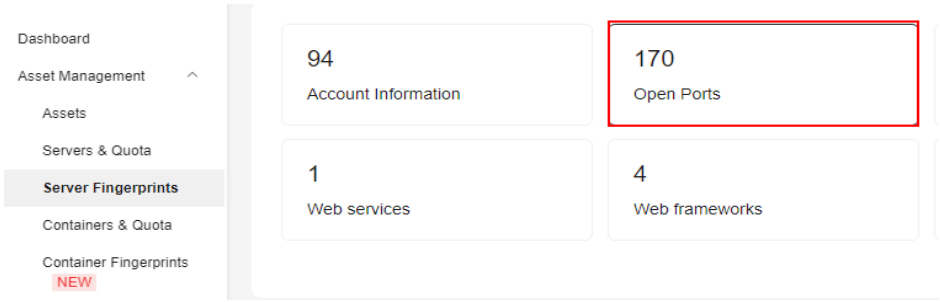
  Figura 2-2 Inicialização manual de uma verificação de vulnerabilidades



- Verifique se as portas 4505 e 4506 estão ativadas no servidor.

  Se as portas 4505 e 4506 estiverem ativadas, é aconselhável desativá-las ou ativá-las apenas para objetos confiáveis. Para obter detalhes, consulte **Visualização de impressões digitais de ativos do servidor**.

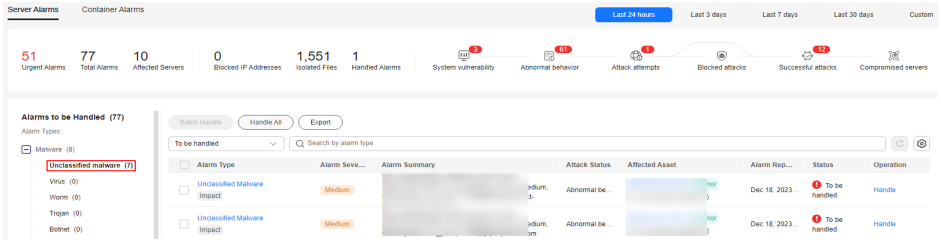
  Figura 2-3 Verificação de portas abertas



- Verifique, isole e elimine cavalos de Troia.

  Isole e elimine o cavalo de Troia de mineração. Para obter detalhes, consulte **Gerenciamento de arquivos isolados**.

Figura 2-4 Gerenciamento de arquivos isolados



2.3 Vulnerabilidade de alto risco do OpenSSL (CVE-2020-1967)

O Projeto OpenSSL divulgou informações de atualização sobre a vulnerabilidade CVE-2020-1967 do OpenSSL que afeta OpenSSL 1.1.1d, OpenSSL 1.1.1e e OpenSSL 1.1.1f. Esta vulnerabilidade pode ser explorada para lançar ataques DDoS.

ID de vulnerabilidade

CVE-2020-1967

Nome de vulnerabilidade

Vulnerabilidade de alto risco do OpenSSL

Escopo do impacto

- OpenSSL 1.1.1d
- OpenSSL 1.1.1e
- OpenSSL 1.1.1f

Solução oficial

Recomenda-se que os usuários afetados instalem o patch de vulnerabilidade mais recente o mais rápido possível.

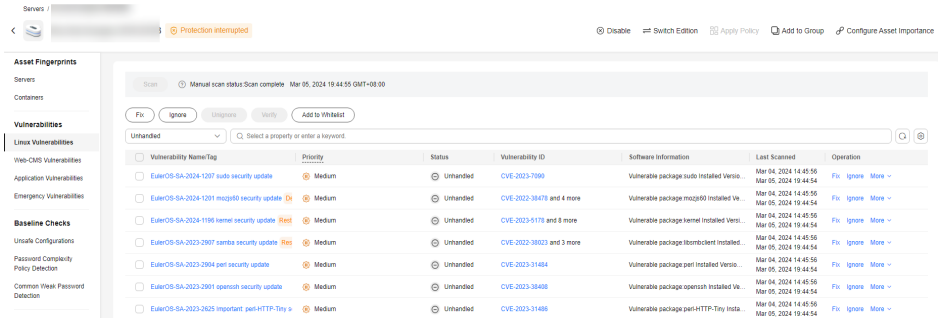
- **https://www.debian.org/security/2020/dsa-4661**
- **https://security.gentoo.org/glsa/202004-10**
- **https://lists.suse.com/pipermail/sle-security-updates/2020-April/006722.html**

Sugestão

Execute as etapas a seguir para verificar e corrigir uma vulnerabilidade.

Passo 1 Detecte e visualize os detalhes da vulnerabilidade, conforme mostrado em **Inicialização manual de uma verificação de vulnerabilidades**. Para obter detalhes, consulte **Visualização de detalhes de vulnerabilidades**.

Figura 2-5 Inicialização manual de uma verificação de vulnerabilidades



Passo 2 Corrija as vulnerabilidades e verifique o resultado. Para obter detalhes, consulte **Manipulação de vulnerabilidades**.

----Fim

2.4 Vulnerabilidade de execução remota de código da biblioteca do Adobe Font Manager (CVE-2020-1020/ CVE-2020-0938)

Existe uma vulnerabilidade de execução remota de código no Microsoft Windows quando a biblioteca do Adobe Type Manager processa incorretamente uma fonte multimestre especialmente criada - o formato Adobe Type 1 PostScript.

Para todos os sistemas, exceto o Windows 10, um invasor que explorasse com sucesso a vulnerabilidade poderia executar códigos remotamente. Para sistemas que executam o Windows 10, um invasor que explorasse com sucesso a vulnerabilidade poderia executar código em um contexto de área restrita do AppContainer com privilégios e recursos limitados. Um invasor poderia então instalar programas, visualizar, alterar ou excluir dados ou criar novas contas com direitos totais de usuário.

Há várias maneiras de um invasor explorar a vulnerabilidade, como convencer um usuário a abrir um documento especialmente criado ou visualizá-lo no painel de visualização do Windows.

ID da vulnerabilidade

- CVE-2020-1020
- CVE-2020-0938

Nome da vulnerabilidade

Vulnerabilidade de execução remota de código da biblioteca do Adobe Font Manager

Detalhes das vulnerabilidades

- Para todos os sistemas, exceto o Windows 10, um invasor que explorasse com sucesso a vulnerabilidade poderia executar códigos remotamente.
- Para sistemas que executam o Windows 10, um invasor que explorasse com sucesso a vulnerabilidade poderia executar código em um contexto de área restrita do AppContainer com privilégios e recursos limitados. Um invasor poderia então instalar

programas, visualizar, alterar ou excluir dados ou criar novas contas com direitos totais de usuário.

Escopo do impacto

Todos os sistemas operacionais Windows

Solução oficial

Recomenda-se que os usuários afetados instalem o patch de vulnerabilidade mais recente o mais rápido possível.

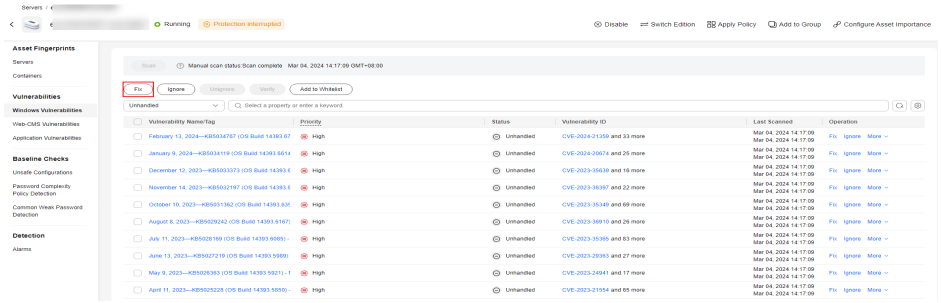
Para obter detalhes, consulte https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2020-1020.

Sugestão

Execute as etapas a seguir para verificar e corrigir uma vulnerabilidade.

Passo 1 Detecte e visualize detalhes da vulnerabilidade. Para obter detalhes, consulte **Visualização de detalhes de vulnerabilidade**.

Figura 2-6 Iniciar manualmente uma verificação de vulnerabilidades



Passo 2 Corrija as vulnerabilidades e verifique o resultado. Para obter detalhes, consulte **Manuseio de vulnerabilidades**.

----Fim

2.5 Vulnerabilidade de elevação de privilégio do kernel do Windows (CVE-2020-1027)

Existe uma vulnerabilidade de elevação de privilégios na forma como o kernel do Windows manipula objetos na memória. Um invasor que explorasse com sucesso a vulnerabilidade poderia executar códigos com permissões elevadas.

Para explorar a vulnerabilidade, um invasor autenticado localmente poderia executar uma aplicação especialmente criada.

ID de vulnerabilidade

CVE-2020-1027

Nome de vulnerabilidade

Vulnerabilidade de elevação de privilégio do kernel do Windows

Detalhes de vulnerabilidade

Existe uma vulnerabilidade de elevação de privilégios na forma como o kernel do Windows manipula objetos na memória. Um invasor que explorasse com sucesso a vulnerabilidade poderia executar códigos com permissões elevadas.

Versões afetadas

Todos os sistemas operacionais Windows

Solução oficial

Recomenda-se que os usuários afetados instalem o patch de vulnerabilidade mais recente o mais rápido possível.

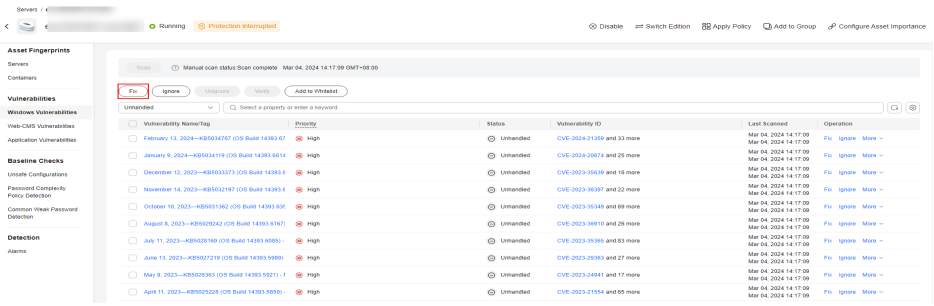
Para obter detalhes, consulte https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2020-1027.

Sugestão

Execute as etapas a seguir para verificar e corrigir uma vulnerabilidade.

Passo 1 Detecte e visualize detalhes de vulnerabilidade. Para obter detalhes, consulte **Visualização de detalhes de vulnerabilidades**.

Figura 2-7 Iniciar manualmente uma verificação de vulnerabilidades



Passo 2 Corrija as vulnerabilidades e verifique o resultado. Para obter detalhes, consulte **Manipulação de vulnerabilidades**.

----Fim

2.6 Vulnerabilidade de falsificação do Windows CryptoAPI (CVE-2020-0601)

Em 15 de janeiro de 2020, a Microsoft lançou uma lista de atualizações de patches que contém a vulnerabilidade de alto risco CVE-2020-0601, descoberta pela Agência de Segurança Nacional (NSA) e que afeta a criptografia do Microsoft Windows. Essa vulnerabilidade afeta o mecanismo de validação de certificados CryptoAPI de Criptografia de

curva elíptica (ECC). Como resultado, os invasores podem interromper o processo de confiança de autenticação e criptografia do Windows e executar códigos remotamente.

ID de vulnerabilidade

CVE-2020-0601

Nome de vulnerabilidade

Vulnerabilidade de falsificação do Windows CryptoAPI (CVE-2020-0601)

Detalhes de vulnerabilidade

Existe uma vulnerabilidade de falsificação na forma como o Windows CryptoAPI (Crypt32.dll) valida certificados ECC.

Um invasor pode explorar a vulnerabilidade usando um certificado de assinatura de código falsificado para assinar um arquivo executável malicioso. O arquivo parece ser de fontes confiáveis e legítimas, e o usuário não pode saber que ele é malicioso. Por exemplo, um invasor pode explorar essa vulnerabilidade para fornecer certificados de assinatura aparentemente confiáveis para malware, como ransomware, e ignorar o mecanismo de detecção de confiança do Windows e enganar os usuários para que instalem o malware.

Uma exploração bem-sucedida também pode permitir que o invasor realize ataques man-in-the-middle e descriptografe informações confidenciais nas conexões do usuário com o software afetado. As instâncias que afetam as relações de confiança do Windows incluem conexões HTTPS comuns, assinaturas de arquivos e assinaturas de e-mail.

Versões afetadas

- Windows 10
- Windows Server 2016 e Windows Server 2019
- Aplicações que dependem do Windows CryptoAPI

Solução oficial

Recomenda-se que os usuários afetados instalem o patch de vulnerabilidade mais recente o mais rápido possível.

Para mais detalhes, consulte https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2020-0601.

Sugestão

Execute as etapas a seguir para verificar e corrigir uma vulnerabilidade.

Certifique-se de ter instalado o agente do HSS no servidor a ser corrigido e de ter ativado a proteção.

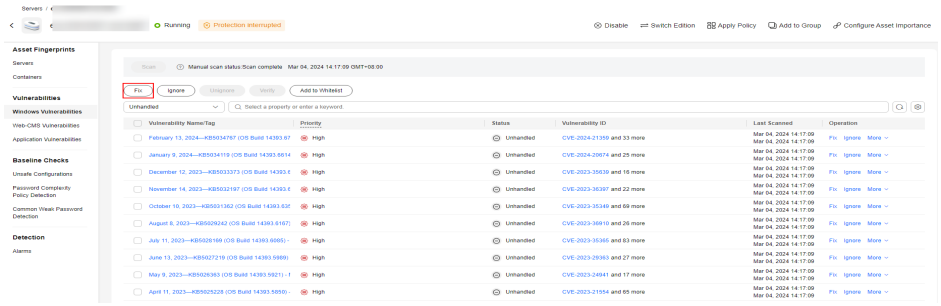
Passo 1 Faça logon no console de gerenciamento.

Passo 2 No canto superior esquerdo da página, selecione uma região, clique em ☰ e escolha **Security and Compliance** > HSS. A página do HSS é exibida.

Passo 3 No painel de navegação, escolha **Servers & Quota**. Na lista de servidores, clique no nome de um servidor Windows para exibir seus detalhes.

Passo 4 Na página de detalhes, escolha **Vulnerabilities** > **Windows Vulnerabilities** e clique em **Scan**.

Figura 2-8 Iniciar manualmente uma verificação de vulnerabilidades



Passo 5 Corrija as vulnerabilidades detectadas de acordo com a sugestão na coluna **Solution**.

Passo 6 Reinicie os servidores fixos.

Passo 7 Clique em **Manual Detection** novamente para verificar se as vulnerabilidades foram corrigidas.

NOTA

Você também pode escolher **Vulnerabilities** e clicar em **Windows Vulnerabilities**, procurar uma vulnerabilidade pelo nome e, em seguida, verificar e corrigir a vulnerabilidade.

- Windows Server 2019: KB4534273
- Windows Server 2016: KB4534271

----Fim

3 Gerenciamento e implementação de várias nuvens do HSS

3.1 Cenário de aplicação

Com o desenvolvimento de nuvens híbridas, há também uma necessidade crescente de as empresas executarem o gerenciamento de segurança unificado em nuvens híbridas. O HSS suporta várias plataformas de nuvem e fornece um conjunto completo de soluções de gerenciamento de operações de segurança para nuvens híbridas. Ele ajuda as empresas a reduzir os riscos de segurança do serviço na arquitetura de nuvem híbrida por meio de visualizações, experiência e gerenciamento unificados, melhorando a eficiência geral da operação de segurança.

Cenário

Para monitorar cargas de trabalho e gerenciar centralmente os recursos das nuvens, no local e em nuvens híbridas, o HSS fornece uma solução de segurança que ajuda a gerenciar a Huawei Cloud e as nuvens híbridas de maneira unificada. O HSS permite que você use as mesmas políticas de segurança em nuvens diferentes, evitando os riscos causados por políticas de segurança inconsistentes.

Solução da Huawei Cloud

No console do HSS da Huawei Cloud, você pode gerenciar centralmente seus servidores da Huawei Cloud, data centers, nuvens de borda e outras nuvens.

Solução de nuvem híbrida

No console do HSS de nuvem híbrida, você pode gerenciar centralmente seus servidores da Huawei Cloud, data centers, nuvens de borda e outras nuvens.

Figura 3-1 Solução da Huawei Cloud

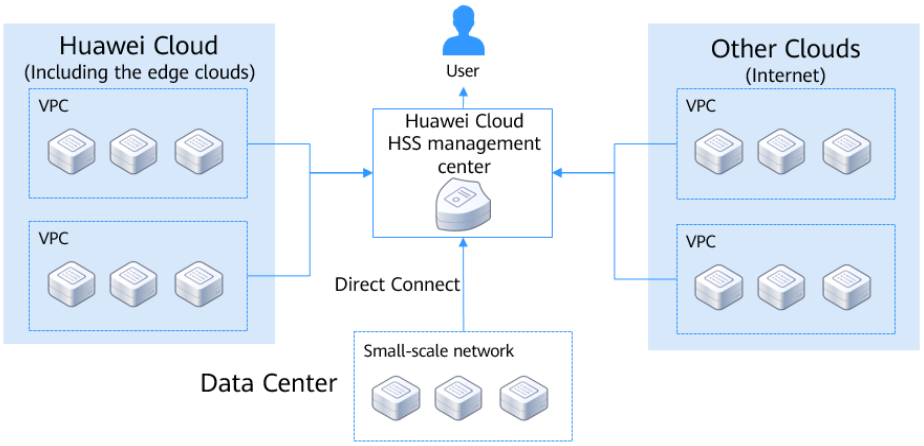
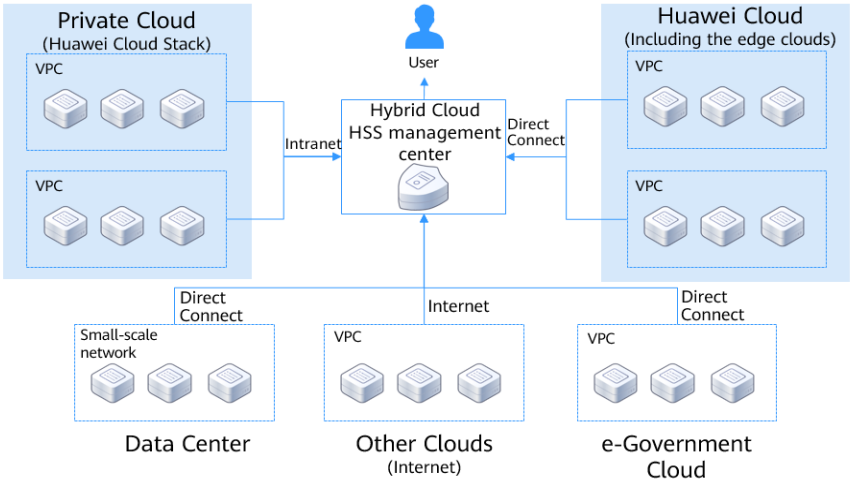


Figura 3-2 Solução de nuvem híbrida



3.2 Processo de instalação e implementação

Se você quiser gerenciar centralmente seus servidores no console de gerenciamento do HSS da Huawei Cloud ou da nuvem híbrida, e seus servidores incluem servidores da Huawei Cloud, servidores não da Huawei Cloud (acessados pela Internet) e servidores LAN (em data centers e em nuvens de governo eletrônico), você precisa instalar agentes em seus servidores em sequência com base em seus cenários de aplicações.

Soluções da Huawei Cloud

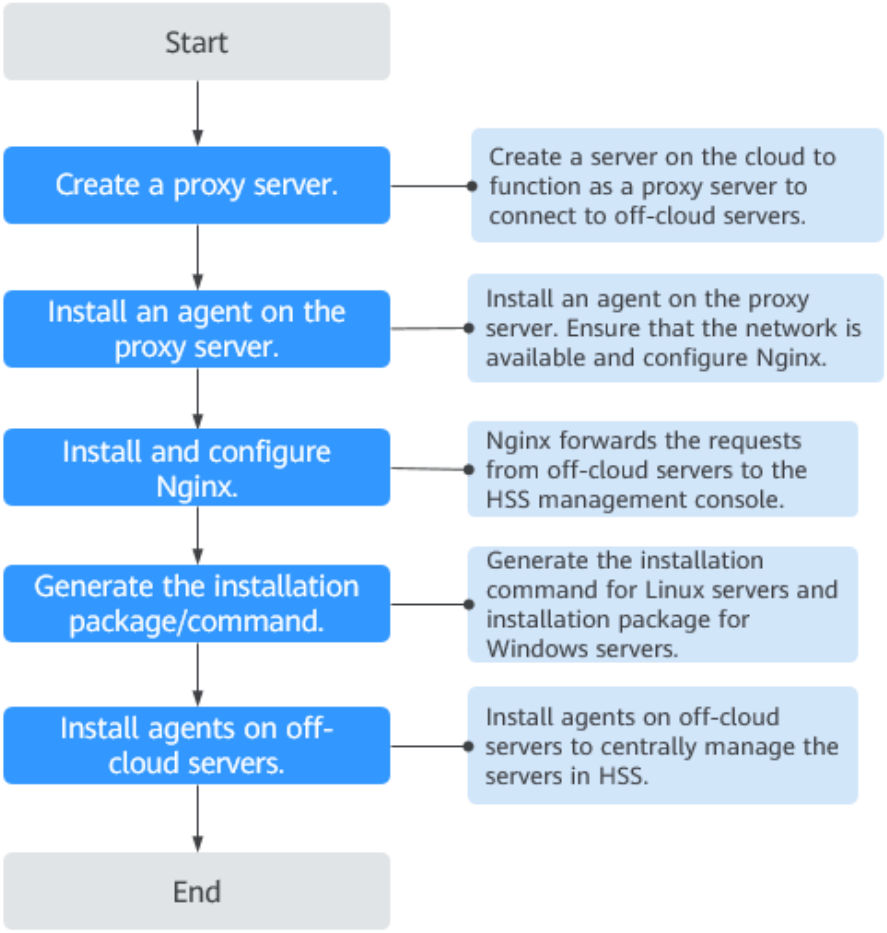
Os métodos e comandos usados para instalar agentes variam de acordo com os tipos de servidores.

Tabela 3-1 Comandos para instalar a solução da Huawei Cloud

Tipo de servidores	Como obter
Servidor da Huawei Cloud	Copie os comandos de instalação da Huawei Cloud no console da Huawei Cloud.
Servidor não da Huawei Cloud (Internet)	Copie os comandos de instalação que não sejam da Huawei Cloud no console da Huawei Cloud. **NOTA** Os comandos de instalação que não são da Huawei Cloud podem ser usadosnos seguintes sites: CN North-Beijing 1, CN North-Beijing 4, CN East-Shanghai 1, CN East-Shanghai 2, CN South-Guangzhou, CN-Hong Kong, AP-Singapore, CN Southwest-Guiyang1 e AP-Jakarta. Para outras regiões, obtenha os comandos de instalação da mesma forma que o serviço LAN.
Servidor LAN (incluindo data centers e nuvens de governo eletrônico)	Configure um proxy e gere o comando ou pacote de instalação. O uso de um servidor proxy de conexão direta pode evitar o acesso à rede pública.

Para obter detalhes sobre como instalar servidores da Huawei Cloud e não da Huawei Cloud (Internet), consulte **Instalação de um agente**. Para obter detalhes sobre como instalar servidores LAN (incluindo data centers e nuvens de governo eletrônico), consulte **Figura 3-3**.

Figura 3-3 Implementação em um servidor LAN



Solução de nuvem híbrida

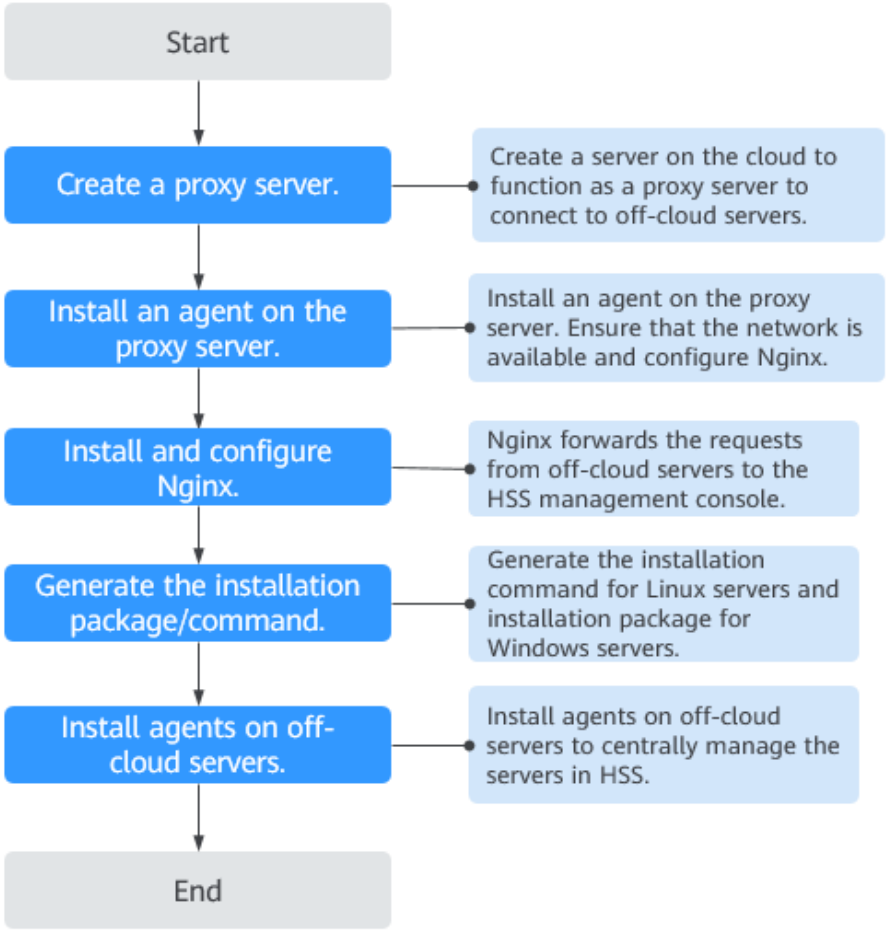
Os métodos e comandos usados para instalar agentes variam de acordo com os tipos de servidores.

Tabela 3-2 Comandos de instalação para a solução de nuvem híbrida

Tipo de servidores	Como obter
Servidor da Huawei Cloud	Copie os comandos de instalação da Huawei Cloud no console da Huawei Cloud.
Servidor não da Huawei Cloud (Internet)	Configure um proxy e gere os comandos ou pacotes de instalação. O uso de um servidor proxy de conexão direta pode evitar o acesso à rede pública.
Servidor LAN (incluindo data centers e nuvens de governo eletrônico)	

Para obter detalhes sobre como instalar servidores da Huawei Cloud, consulte **Instalação do agente**. Para obter detalhes sobre como instalar servidores não da Huawei Cloud (Internet) e servidores LAN (incluindo data centers e nuvens de governo eletrônico), consulte **Figura 3-4**.

Figura 3-4 Implementação em um servidor LAN



3.3 Instalação e implementação

3.3.1 Soluções da Huawei Cloud

Você pode usar o HSS para gerenciar centralmente seus servidores. Se seus tipos de servidores incluem servidores da Huawei Cloud, servidores não da Huawei Cloud (Internet) e servidores LAN (incluindo servidores de data center e de nuvem de governo eletrônico), instale agentes nos servidores com base no tipo de servidor.

Servidor da Huawei Cloud/servidor não da Huawei (Internet)

- Para gerenciar servidores da Huawei Cloud e não da Huawei Cloud (Internet) no console do HSS, você pode instalar agentes diretamente nos servidores na região de destino.

- Para obter detalhes sobre como instalar um agente em um servidor Linux da Huawei Cloud ou não da Huawei Cloud (Internet), consulte **Instalação de um agente no Linux**.
- Para obter detalhes sobre como instalar um agente em um servidor Windows da Huawei Cloud ou não da Huawei Cloud (Internet), consulte **Instalação de um agente no Windows**.

NOTA

Você pode instalar agentes em servidores não da Huawei Cloud (Internet) nos seguintes sites: CN North-Beijing 1, CN North-Beijing 4, CN East-Shanghai 1, CN East-Shanghai 2, CN South-Guangzhou, CN-Hong Kong, AP-Singapore, CN Southwest-Guiyang1 e AP-Jakarta. Para outras regiões, obtenha os comandos de instalação da mesma forma que para os servidores LAN.

Servidor LAN (data center, nuvem de governo eletrônico, nuvem privada)

Para gerenciar centralmente os servidores LAN no console do HSS da Huawei Cloud, crie um servidor proxy que use a Direct Connect, crie manualmente o comando (ou pacote) de instalação do agente e instale os agentes em seus servidores.

Para mais detalhes, consulte **Conexão de servidores fora da nuvem à nuvem pública por meio da Direct Connect**.

3.3.2 Solução de nuvem híbrida

Você pode usar o HSS híbrido para gerenciar centralmente seus servidores. Se seus tipos de servidores incluem servidores da Huawei Cloud, servidores não da Huawei Cloud (Internet) e servidores LAN (incluindo servidores de data center e de nuvem de governo eletrônico), instale agentes nos servidores com base no tipo de servidor.

Servidor da Huawei Cloud

Para gerenciar os servidores da Huawei Cloud no console do HSS de nuvem híbrida, você pode instalar agentes diretamente nos servidores na região de destino.

- Para obter detalhes sobre como instalar o agente em um servidor Linux da Huawei Cloud, consulte **Instalação de um agente no Linux**.
- Para obter detalhes sobre como instalar o agente em um servidor Windows da Huawei Cloud, consulte **Instalação de um agente no Windows**.

Servidor não da Huawei (Internet)/servidor LAN (data center, nuvem de governo eletrônico, nuvem privada)

Para gerenciar centralmente servidores não da Huawei Cloud (Internet) e servidores LAN no console do HSS da nuvem híbrida, crie um servidor proxy que use a Direct Connect, crie manualmente os comandos (ou pacotes) de instalação do agente e instale os agentes nos servidores.

Para mais detalhes, consulte **Conexão de servidores fora da nuvem à nuvem pública por meio da Direct Connect**.

3.4 Verificação e utilização

Após a conclusão da instalação, efetue logon no console do HSS da Huawei Cloud ou da nuvem híbrida e acesse a página da lista do ECS. Se o ECS de destino for exibido na lista, os ECSs off-line foram conectados ao console do HSS e gerenciados de maneira unificada.

NOTA

- Após a conclusão da instalação, verifique se a porta 10180 do servidor de destino pode ser conectada corretamente e se o servidor está on-line.
- O status do servidor não é exibido depois que servidores não da Huawei (Internet) e servidores LAN (como data centers, nuvens de governo eletrônico e nuvens privadas) são conectados ao console do HSS.

3.5 Conexão de servidores fora da nuvem à nuvem pública por meio da Direct Connect

3.5.1 Etapa 1: criar um servidor proxy

Crie um servidor na nuvem para funcionar como um servidor proxy para se conectar a servidores fora da nuvem.

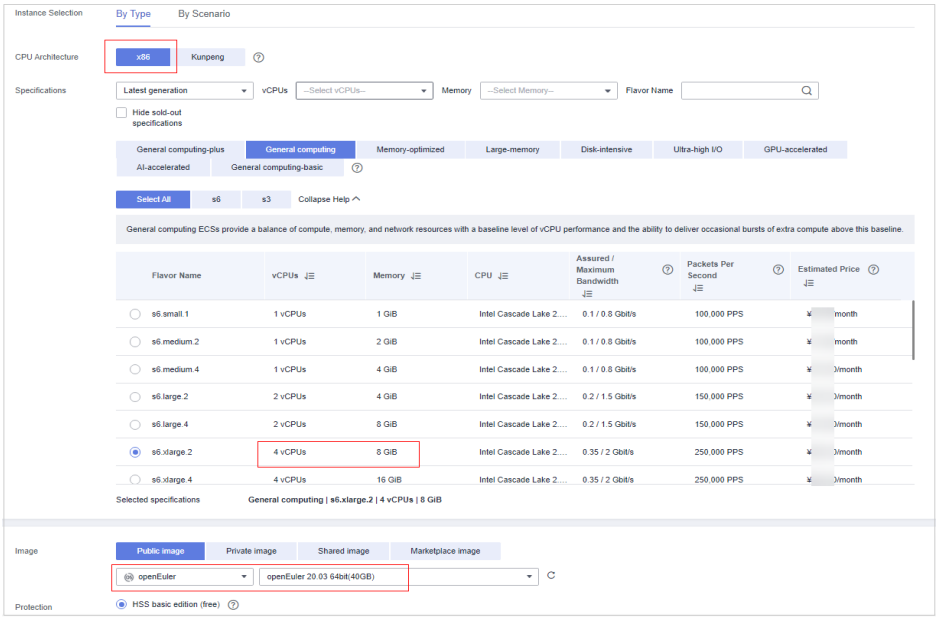
Procedimento

Faça logon no console de gerenciamento da Huawei Cloud e compre um ECS. Para obter detalhes, consulte **Compra de um ECS**.

AVISO

- A arquitetura da CPU do servidor proxy deve ser x86.
- O número de vCPUs do servidor proxy deve ser 4 ou superior e a memória deve ser 8 GiB ou superior.
- A imagem do servidor proxy deve ser uma imagem do Linux que possa usar o comando **yum**. Você é aconselhado a usar a imagem de HCE.

Figura 3-5 Criação de um servidor proxy



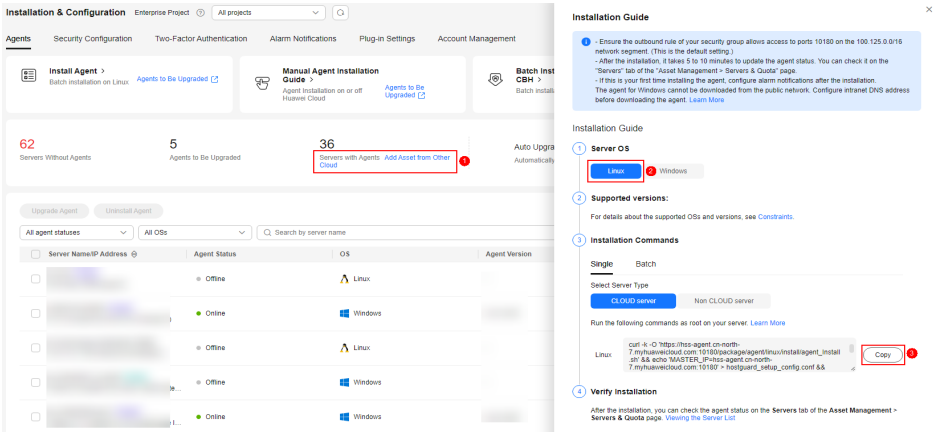
3.5.2 Etapa 2: instalar um agente para o servidor proxy

Instale um agente no servidor proxy. Certifique-se de que a rede esteja disponível e configure o Nginx.

Procedimento

Passo 1 Faça logon no console do HSS (novo), escolha **Installation & Configuration** e clique em **Agents** > **Add Asset from Other Cloud**. Selecione servidor **Linux** de Huawei Cloud e **x86** e copie os comandos de instalação do EulerOS.

Figura 3-6 Cópia do comando de instalação



Passo 2 Faça logon no servidor proxy, cole e execute os comandos copiados para instalar o agente. Para obter detalhes, consulte **Instalação de um agente no Linux**.

Figura 3-7 Instalação de um agente

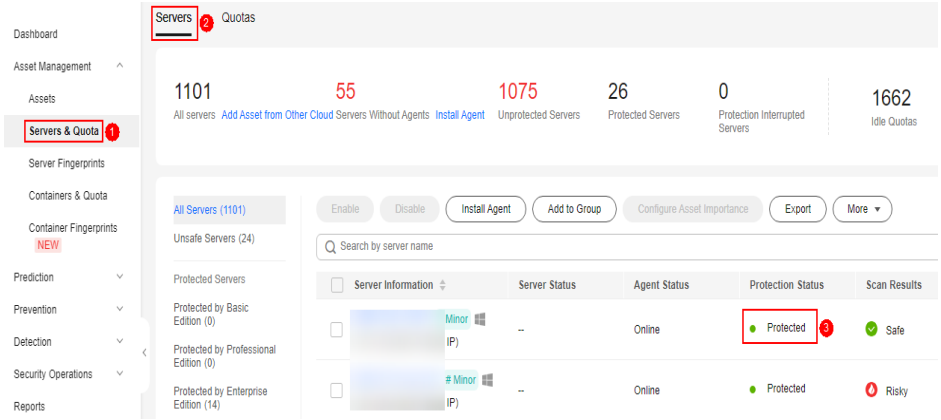
```
Preparing...                          ################################# [100%]
Updating / installing...
   1:hostguard-3.2.8-1                ################################# [100%]
hostguard starting ...
memory cgroup is disabled
your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
Hostguard is running...
Hostguard installed.
```

Passo 3 Cerca de 10 minutos depois, acesse a página da lista do ECS e verifique se o **Agent Status** do servidor proxy está **Online**.

AVISO

Certifique-se de que o servidor do agente esteja on-line antes de executar as etapas subsequentes. Caso contrário, as etapas subsequentes podem falhar.

Figura 3-8 Verificação do status do agente



----Fim

3.5.3 Etapa 3: instalar e configurar o Nginx

O Nginx encaminha solicitações de servidores fora da nuvem para o console de gerenciamento do HSS.

Preparação: verificar o repositório Yum

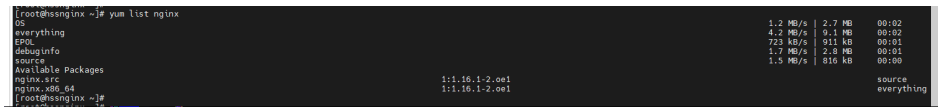
Verifique se o pacote de software Nginx existe no repositório Yum. Se o pacote de software Nginx não existir, configure o repositório Yum e vincule o endereço IP público temporariamente. Após a conclusão da instalação, desvincule o endereço IP público.

Passo 1 Faça logon remotamente no servidor proxy e execute o seguinte comando para verificar se o pacote Nginx existe no repositório Yum:

yum list nginx

Passo 2 Se as informações mostradas em **Figura 3-9** forem exibidas, o pacote Nginx existe.

Figura 3-9 O pacote Nginx existe



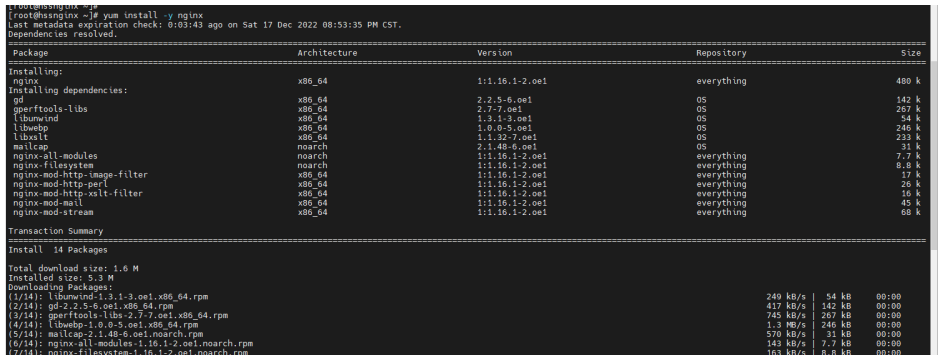
----Fim

Instalação do Nginx

Passo 1 Execute o seguinte comando para instalar o Nginx usando o Yum:

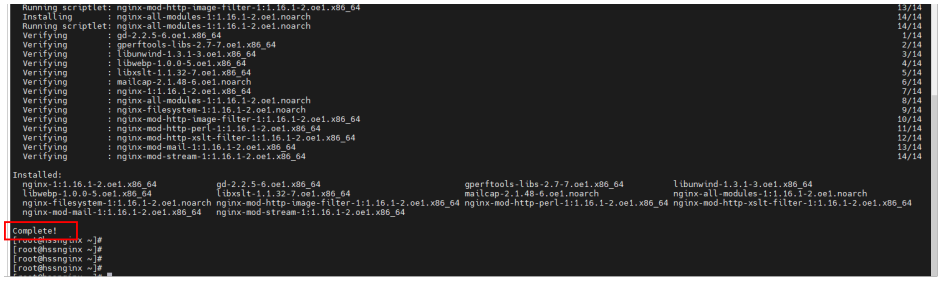
yum install -y nginx

Figura 3-10 Instalação do Nginx



Passo 2 O Nginx é instalado automaticamente. Se **Complete!** mostrado em **Figura 3-11** for exibido, a instalação foi bem-sucedida.

Figura 3-11 Nginx instalado com sucesso



----Fim

Configuração do Nginx

Passo 1 Execute o seguinte comando para ir para o diretório Nginx:

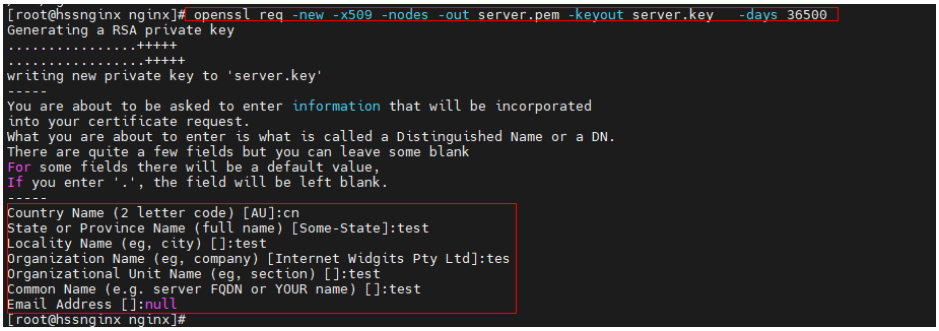
cd /etc/nginx/

Passo 2 Execute o seguinte comando para assinar o certificado:

openssl req -new -x509 -nodes -out server.pem -keyout server.key -days 36500

Após a execução do comando, insira as informações do certificado.

Figura 3-12 Certificado autoassinado



NOTA

O valor de **Country Name** pode conter apenas dois caracteres.

Passo 3 Execute o seguinte comando para modificar **nginx.conf**:

vi nginx.conf

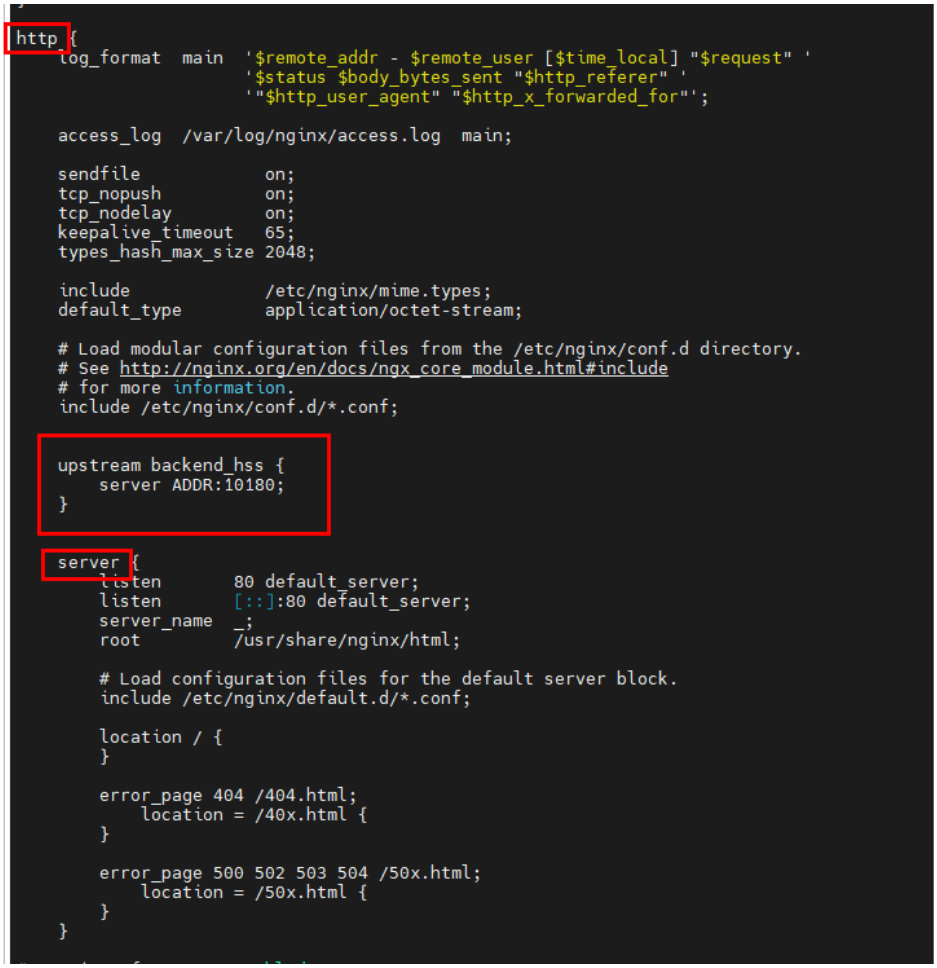
Passo 4 Configure **upstream**. Encontre **server** em **http** e adicione as seguintes informações acima do **server**:

upstream backend_hss {

server ADDR:10180;

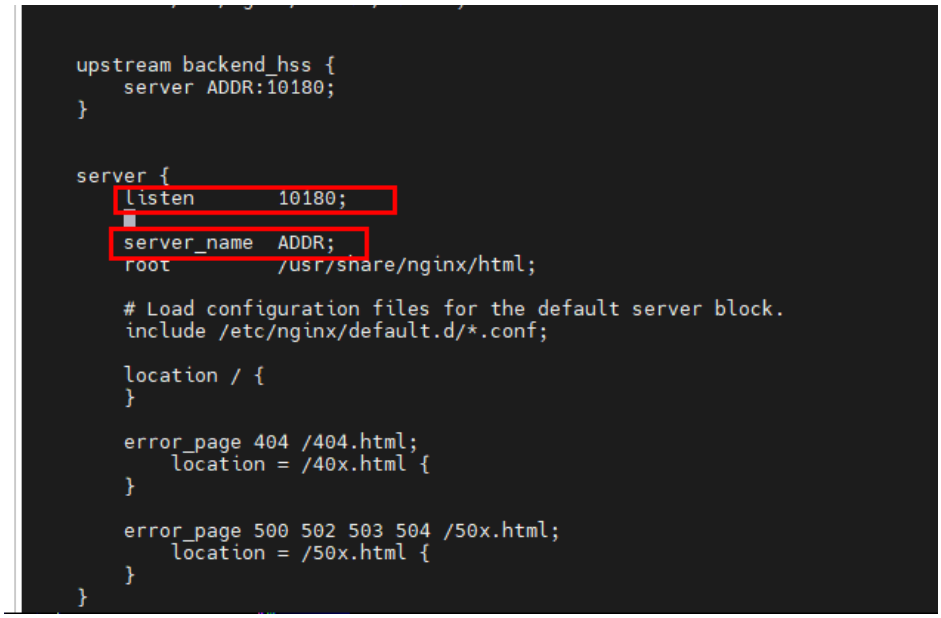
}

Figura 3-13 Configuração de upstream



Passo 5 Configure **server**. Mantenha um registro de **listen** na porta de escuta e altere o valor para **10180**. Altere o valor de **server_name** para **ADDR**.

Figura 3-14 Configuração do servidor



Passo 6 Adicione as seguintes informações em **server** para ativar a autenticação SSL:

ssl on;

ssl_protocols TLSv1.2;

ssl_certificate "server.pem";

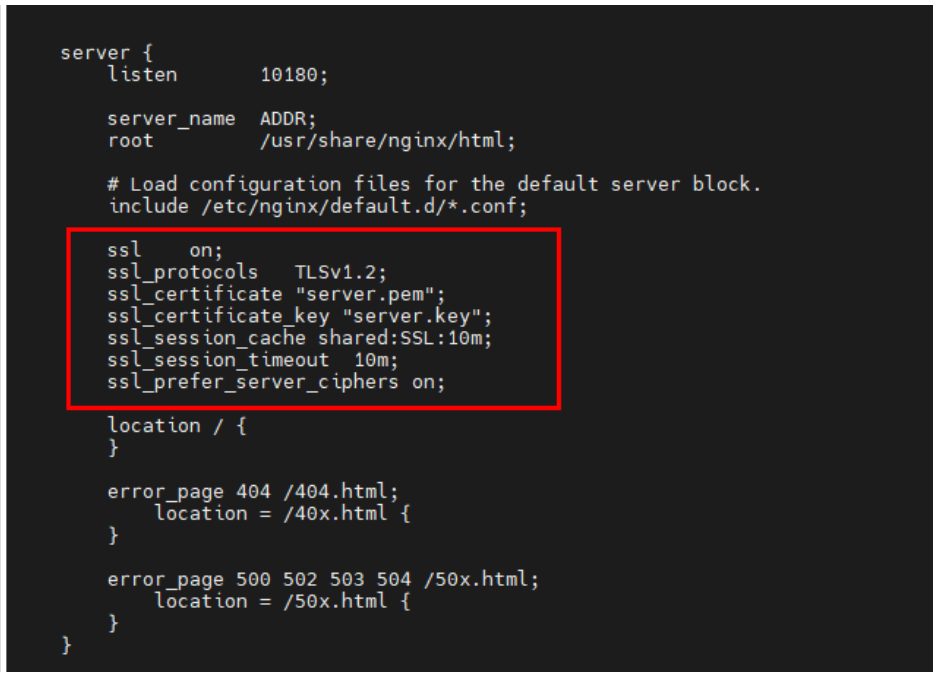
ssl_certificate_key "server.key";

ssl_session_cache shared:ssl:10m;

ssl_session_timeout 10m;

ssl_prefer_server_ciphers on;

Figura 3-15 Ativação da autenticação SSL



Passo 7 Configure **location**. Encontre **location** em **server** e adicione as seguintes informações a **{}** em **location**:

limit_except GET POST PUT

{

deny all;

}

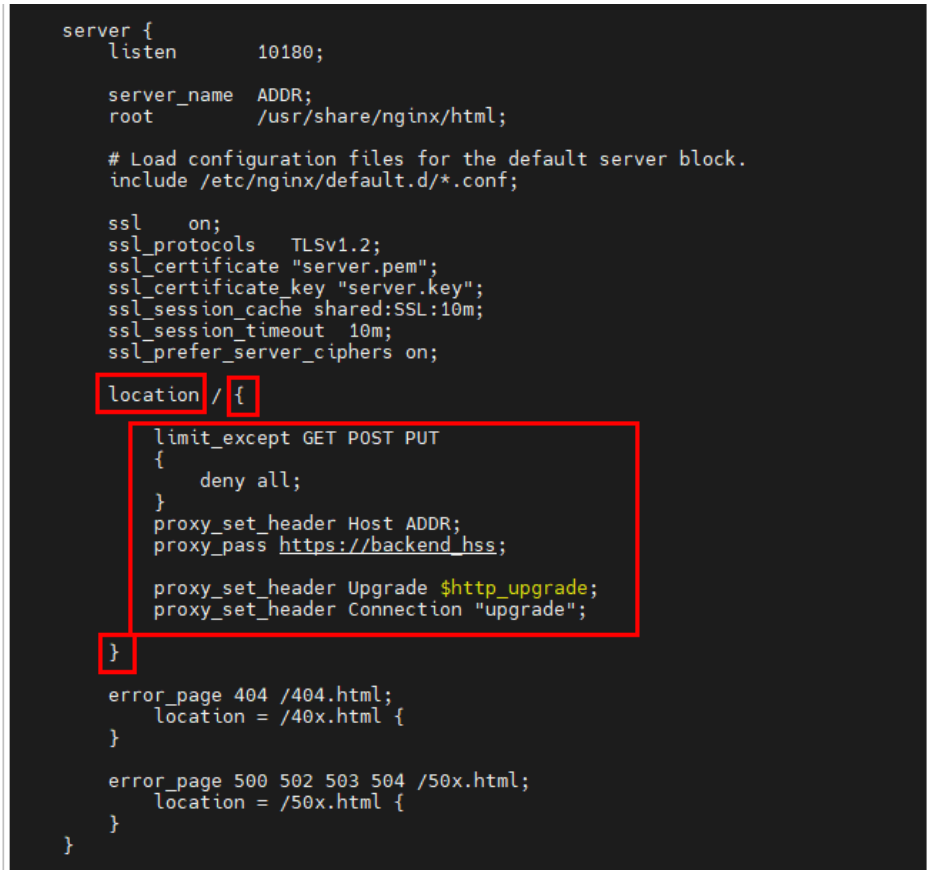
proxy_set_header Host ADDR;

proxy_pass https://backend_hss;

proxy_set_header Upgrade $http_upgrade;

proxy_set_header Connection "upgrade";

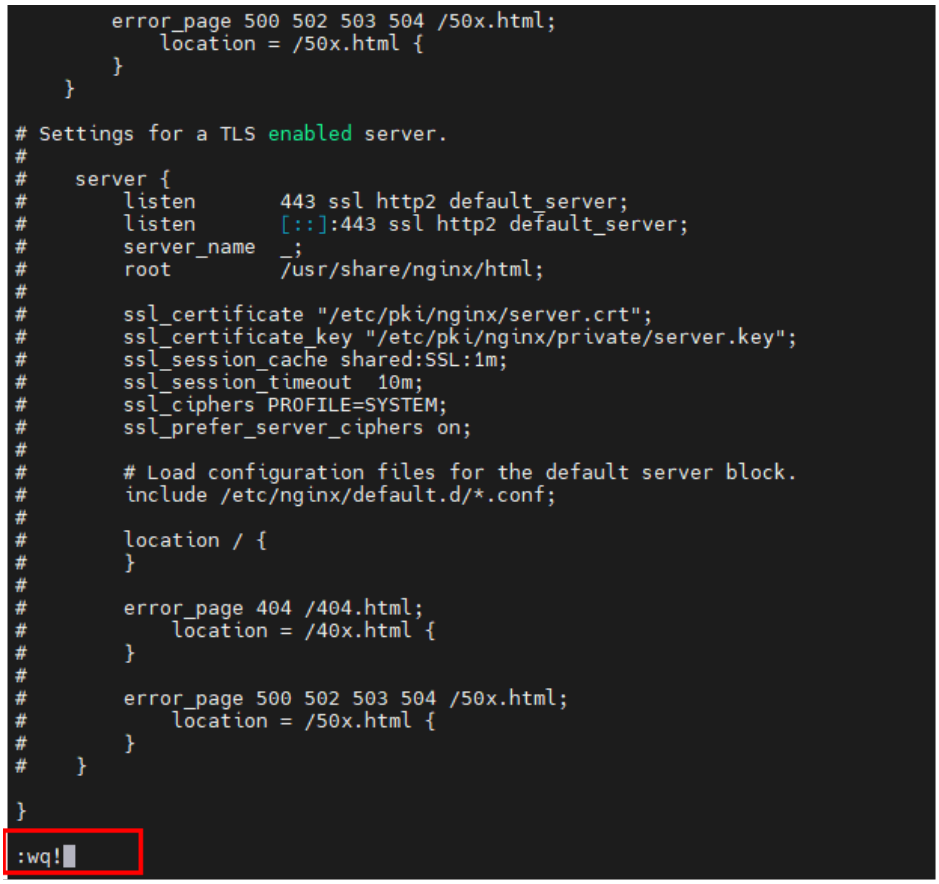
Figura 3-16 Configuração do local



Passo 8 **Opcional:** Digite **ECS**, execute o seguinte comando e pressione **Enter** para sair.

:wq!

Figura 3-17 Salvar as configurações e sair



Passo 9 Execute os seguintes comandos em sequência para iniciar o Nginx:

sed -i "s#ADDR#`cat /usr/local/hostguard/conf/connect.conf | grep master_address | cut -d '=' -f 2 | cut -d ':' -f 1`#g" nginx.conf

echo '*/10 * * * * root systemctl start nginx' >> /etc/crontab

systemctl start nginx

----Fim

3.5.4 Etapa 4: gerar um pacote/comando de instalação

Gere o comando de instalação para servidores Linux e o pacote para servidores Windows.

Geração do comando de instalação para servidores Linux

Passo 1 Execute o seguinte comando para acessar o diretório **/tmp**:

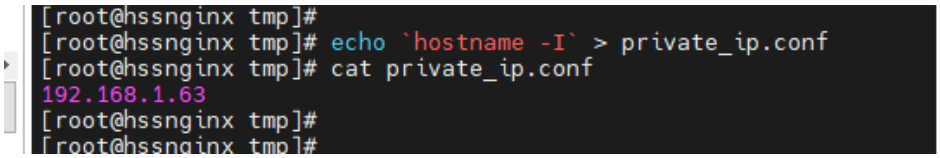
cd /tmp

Passo 2 Execute os seguintes comandos em sequência para verificar se o endereço IP em **private_ip.conf** está disponível:

echo `hostname -I` > private_ip.conf

cat private_ip.conf

Figura 3-18 Verificação do endereço IP



AVISO

- Verifique se o endereço IP em **private_ip.conf** está disponível para o servidor proxy. Certifique-se de que o endereço IP possa ser conectado por servidores fora da nuvem.
- Se o endereço IP não estiver disponível, altere-o manualmente.

Passo 3 Depois de confirmar que o endereço IP está disponível, execute os seguintes comandos em sequência para gerar o comando de instalação:

- Imagem do pacote de software x86 RPM:

  echo -e "# for Liunx x86 CentOS EulerOS OpenSUSE Fedora\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/x86/hostguard.x86_64.rpm' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && rpm -ivh hostguard.x86_64.rpm && rm -f hostguard_setup_config.conf && rm -f hostguard*.rpm" > x86_rpm_install.sh

- Imagem do pacote de software x86 deb:

  echo -e "# for Liunx x86 Ubuntu Debian\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/x86/hostguard.x86_64.deb' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && dpkg -i hostguard.x86_64.deb && rm -f hostguard_setup_config.conf && rm -f hostguard*.deb" > x86_deb_install.sh

- Imagem do pacote de software ARM RPM:

  echo -e "# for Liunx ARM CentOS EulerOS OpenSUSE Fedora UOS Kylin\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/arm/hostguard.aarch64.rpm' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && rpm -ivh hostguard.aarch64.rpm && rm -f hostguard_setup_config.conf && rm -f hostguard*.rpm" > arm_rpm_install.sh

- Imagem do pacote de software ARM deb:

  echo -e "# for Liunx ARM Ubuntu Debian\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/arm/hostguard.aarch64.deb' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && dpkg -i hostguard.aarch64.deb && rm -f hostguard_setup_config.conf && rm -f hostguard*.deb" > arm_deb_install.sh

- Altere para um endereço IP disponível:

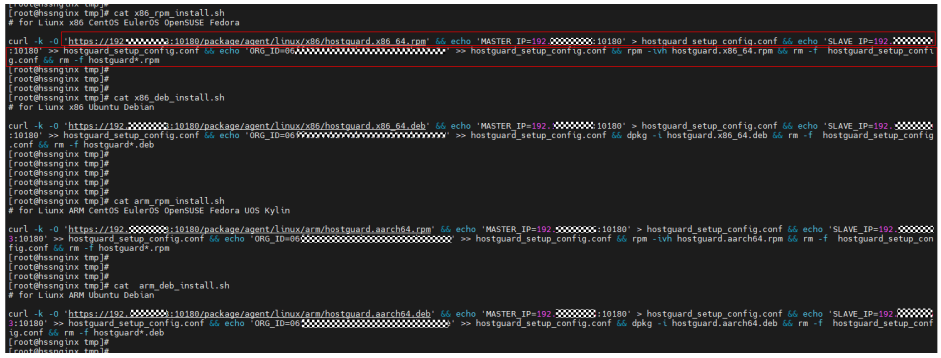
sed -i "s#private_ip#`cat private_ip.conf`#g" *install.sh && sed -i "s#project_id#`cat /usr/local/hostguard/run/metadata.conf | grep -v enterprise_project_id | grep project_id | cut -d ":" -f 2 | cut -d " " -f 2`#g" *install.sh

NOTA

- Todos os cinco comandos devem ser executados. O último comando que é usado para mudar para um endereço IP disponível deve ser executado finalmente.
- Os comandos de instalação em **x86_rpm_install.sh** são adequados para imagens gerenciadas pelo pacote de software RPM na arquitetura x86, como CentOS, EulerOS, OpenSUSE e Fedora.
- Os comandos de instalação em **x86_deb_install.sh** são adequados para imagens gerenciadas pelo pacote de software .deb na arquitetura x86, como Ubuntu e Debian.
- Os comandos de instalação em **arm_rpm_install.sh** são adequados para imagens gerenciadas pelo pacote de software RPM na arquitetura ARM, como CentOS, EulerOS, OpenSUSE, Fedora, UOS e Kylin.
- Os comandos de instalação em **arm_deb_install.sh** são adequados para imagens gerenciadas pelo pacote de software .deb na arquitetura ARM, como Ubuntu e Debian.

Passo 4 Veja o comando de instalação gerado, que será usado para instalar agentes nos servidores Linux fora da nuvem.

Figura 3-19 Comandos de instalação do Linux



----Fim

Geração do pacote de instalação para servidores Windows

Passo 1 Execute o seguinte comando para acessar o diretório **/tmp**:

cd /tmp

Passo 2 Execute os seguintes comandos em sequência para gerar o pacote de instalação do agente para servidores Windows:

curl -k -O https://`cat private_ip.conf`:10180/package/agent/windows/hostguard_setup.exe && echo '[system]' > hostguard_setup_config.ini && echo 'master='`cat private_ip.conf`':10180' >> hostguard_setup_config.ini && echo 'slave='`cat private_ip.conf`':10180' >> hostguard_setup_config.ini && echo 'orgid='`cat /usr/local/hostguard/run/metadata.conf | grep -v enterprise_project_id | grep project_id | cut -d ":" -f 2 | cut -d " " -f 2` >> hostguard_setup_config.ini

zip hostguard_setup.zip hostguard_setup.exe hostguard_setup_config.ini

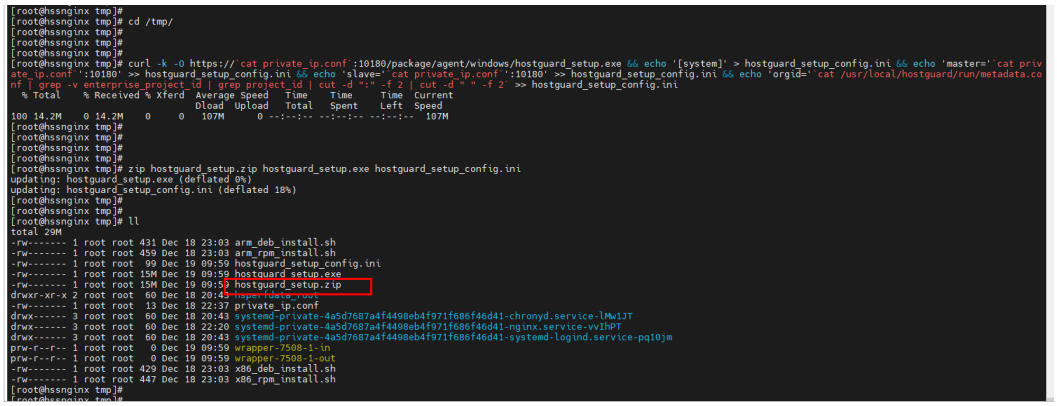
NOTA

Se o servidor proxy não tiver comandos zip, execute o seguinte comando para instalar o plug-in zip:

yum install -y zip

Passo 3 Visualize o pacote de instalação gerado, que será usado para instalar agentes nos servidores Windows fora da nuvem.

Figura 3-20 Pacote de instalação do Windows



----Fim

3.5.5 Etapa 5: instalar agentes em servidores fora da nuvem

Instale agentes em servidores fora da nuvem e gerencie os servidores no HSS de maneira unificada.

Instalação de agentes em servidores Linux fora da nuvem

Faça logon em um servidor fora da nuvem e copie o comando gerado em **Geração de comandos de instalação para servidores Linux** para o servidor para instalar um agente.

Para obter detalhes, consulte a etapa 8 em **Instalação de um agente no Linux**.

Instalação de agentes em servidores Windows fora da nuvem

Copie o pacote **hostguard_setup.zip** gerado em **Geração de pacotes de instalação para servidores Linux** para o PC local e carregue-o em um servidor Windows fora da nuvem para instalar o agente. Descompacte o pacote de instalação e clique duas vezes em **hostguard_setup.exe** para instalar o agente.

AVISO

Depois que o pacote de instalação .zip gerado for copiado para o PC local, você deverá descompactar o pacote antes de instalar o software. Caso contrário, a instalação falhará.

4 Melhores práticas para defesa contra ransomware

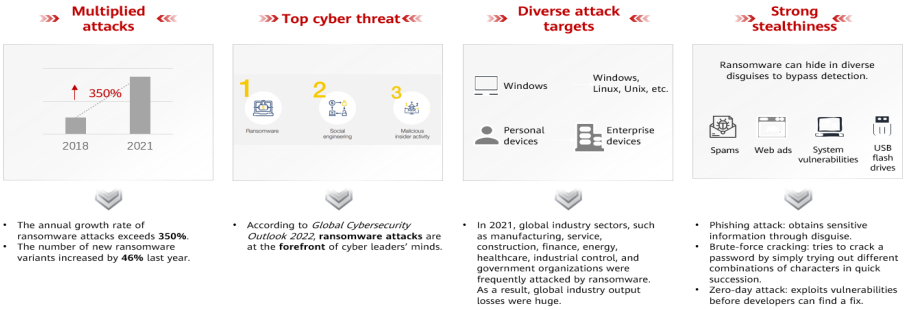
4.1 O que é um ataque de ransomware?

Os ataques de ransomware se tornaram um dos maiores desafios de segurança enfrentados pelas empresas atualmente. Ransomware é um tipo de ataque de malware em que o invasor bloqueia os dados ou dispositivos de ativos da vítima e, em seguida, exige um pagamento para desbloquear os dados. Às vezes, os invasores podem não desbloquear os dados, mesmo depois de receber o resgate.

Ataques de ransomware podem causar a interrupção de seus serviços e o vazamento ou a perda de informações e dados críticos. Como resultado, a operação, a economia e a reputação da sua empresa podem ser muito afetadas e problemas de segurança podem prejudicar o desenvolvimento da sua empresa.

Com os ataques de ransomware aumentando nos últimos anos, esse malware está evoluindo para se tornar mais furtivo, mais rápido e mais impactante. A defesa contra ataques de ransomware é agora uma tarefa importante e urgente para as empresas.

Figura 4-1 Visão geral de ransomware



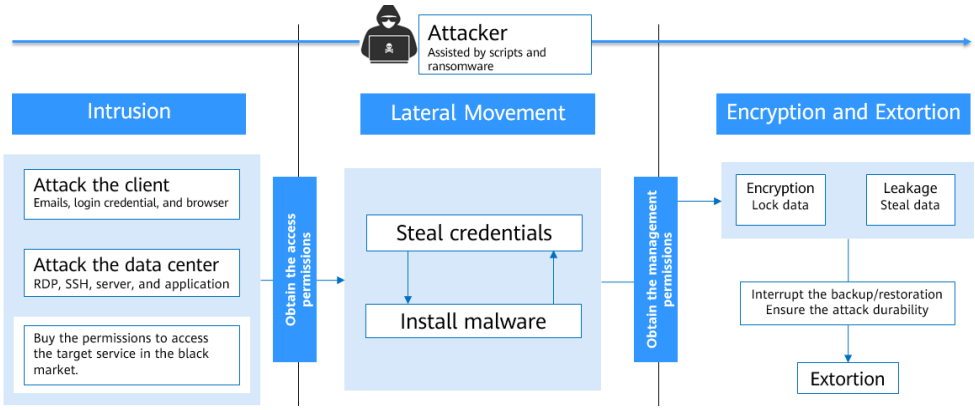
4.2 Processo de ataques de ransomware

Ao atacar a infraestrutura de nuvem, os invasores geralmente atacam vários recursos na tentativa de obter acesso a dados de clientes ou segredos da empresa. O processo de um

ataque de ransomware pode ser dividido em três etapas: investigação e detecção, intrusão e movimentação lateral e extorsão.

- **Intrusion**: os invasores coletam informações básicas, procuram vetores de ataque, entram no ambiente e estabelecem uma base de apoio interna.
- **Lateral movement**: os invasores implementam recursos de ataque, detectam ativos de rede, elevam as permissões de acesso, roubam credenciais, implementam ransomware, danificam o mecanismo de detecção e defesa e expandem o escopo do ataque.
- **Encryption extortion**: os invasores roubam dados confidenciais, criptografam dados importantes, carregam informações de ransomware e pedem resgate.

Figura 4-2 Processo de extorsão



4.3 Proteção contra ransomware (ações gerais)

Medidas pré-evento

É difícil descriptografar os dados que foram criptografados pelo ransomware ou rastrear os invasores com base em suas transações em moeda digital. A maneira mais eficaz de combater ataques de ransomware é melhorar as capacidades anti-ataques.

É aconselhável realizar as seguintes operações para proteger seus servidores contra ransomware:

- **Minimize o escopo exposto à Internet**: verifique periodicamente as portas externas e certifique-se de que apenas as portas necessárias estejam ativadas.
- **Reduza os riscos do sistema**: verifique periodicamente as vulnerabilidades e os parâmetros de configuração de risco do sistema para corrigir vulnerabilidades e riscos em tempo hábil. Além disso, preste atenção às informações de vulnerabilidade de segurança e às informações de patch divulgadas pelos fornecedores de software e gerencie e corrija vulnerabilidades em tempo hábil.
- **Melhore o controle de acesso à rede**: defina claramente as zonas de segurança da rede e as regras de controle de acesso, minimize os direitos de acesso e atualize as regras de controle de acesso em tempo hábil.
- **Faça backup de dados importantes**: o backup confiável de dados pode minimizar a perda causada pelo ransomware. Criptografe o armazenamento e faça backups periódicos de dados críticos de serviço e defina regras de retenção de backup adequadas para garantir que cópias válidas possam ser usadas para restaurar dados após serem atacados.

- **Melhore o controle de permissões de conta**: atribua contas e permissões a diferentes funções com base em regras de controle de acesso, como gerenciamento de identidade e controle de permissão refinado. Melhore a segurança das contas privilegiadas. Defina e salve corretamente contas e senhas para os principais ativos de serviço da sua empresa. Configure a autenticação de dois fatores para identificar o pessoal que acessa os principais ativos e reduzir os riscos de quebra por força bruta.
- **Estabeleça uma arquitetura de serviço de alta confiabilidade**: implemente serviços de nuvem no modo de cluster. Se ocorrer uma emergência em um nó, os serviços serão alternados para o nó em espera, melhorando a confiabilidade e evitando a perda de dados. Se você tiver recursos suficientes, poderá criar sistemas de backup e DR remotos ou dentro da cidade. Se o sistema primário for atacado por ransomware, seus serviços podem ser rapidamente alternados para o sistema de backup e não serão interrompidos.
- **Desenvolva planos de emergência para incidentes de segurança**: estabeleça uma organização de emergência e um mecanismo de gerenciamento para lidar com incidentes de segurança cibernética, como ataques de ransomware, e especifique os princípios de trabalho, a divisão de responsabilidades, os processos de tratamento de emergência e as principais medidas. Depois que seu serviço for atacado por ransomware, inicie imediatamente o plano interno de emergência de segurança cibernética e realize o tratamento de emergência padronizado para mitigar e eliminar o impacto do ataque de ransomware.
- **Melhore a conscientização de segurança dos funcionários**: melhore a conscientização sobre segurança cibernética dos funcionários por meio de treinamentos e simulações. Certifique-se de que os funcionários entendam as leis e regulamentos nacionais de segurança cibernética e os regulamentos de segurança cibernética da Huawei, possam identificar ataques comuns de segurança cibernética, como phishing, tenham determinados recursos de tratamento de incidentes e conheçam as consequências e os impactos dos incidentes de segurança.

Medidas durante o evento

Quando um intruso ignora o mecanismo de defesa, se você puder detectar e bloquear o intruso em tempo hábil, um desastre poderá ser evitado.

Você é aconselhado a executar as seguintes operações depois de ser atacado por ransomware:

- **Isole rapidamente os dispositivos infectados**: depois de ser atacado, desconecte imediatamente a rede ou desligue o sistema para evitar a propagação do ataque de ransomware. Altere as senhas de dispositivos infectados e outros dispositivos na mesma LAN em tempo hábil.
- **Lide rapidamente com os eventos de intrusão**: execute uma verificação de segurança em tempo real nos recursos do serviço, isole e bloqueie o ransomware, bloqueie os endereços IP de origem do ransomware e os endereços IP suspeitos de ataques de força bruta e bloqueie a execução, a comunicação e a conexão do ransomware.

Medidas pós-evento

Atualmente, os ataques de ransomware se desenvolvem rapidamente e nenhuma ferramenta pode fornecer 100% de proteção. Depois de ser atacado, restaure seus serviços em tempo hábil e fortaleça a segurança da rede para reduzir o impacto dos ataques de ransomware.

Recomenda-se que você execute as seguintes operações de restauração:

- **Use dados de backup para restaurar serviços**: determine o escopo, a sequência e a versão de backup da restauração de dados com base no status de backup do dispositivo atacado e use os dados de backup para restaurar os serviços.
- **Verifique e corrija os riscos da rede**: identifique as vulnerabilidades do sistema com base nos caminhos de ataque do ransomware. Verifique e corrija as vulnerabilidades do sistema.

4.4 Solução de prevenção de ransomware da Huawei Cloud (HSS+CBR)

4.4.1 Visão geral

Além das ações gerais de proteção contra ransomware (**Proteção contra ransomware (ações gerais)**), tanto o HSS quanto o CBR podem melhorar sua capacidade abrangente de defesa contra ransomware.

Atualmente, o ransomware é frequentemente atualizado e evoluído. O HSS pode detectar ransomware e identificar riscos do sistema, mas não pode fornecer proteção contra 100% dos vírus existentes. Você pode usar o CBR para melhorar os recursos de prevenção de ransomware e reduzir o impacto de ataques de ransomware. Se apenas o CBR estiver configurado, o sistema pode falhar ao restaurar os dados gerados entre o último backup e o ataque do ransomware. Você pode usar o HSS para detectar ransomware em tempo real e minimizar a perda de dados. Portanto, é aconselhável usar o HSS e o CBR para proteger as empresas antes, durante e após os ataques de ransomware.

- **Pré-evento: detecte e resolva rapidamente ataques de ransomware**

  Para mais detalhes, consulte **Identificação e correção de ransomware**.
- **Durante o evento: detecte, isole e bloqueie ataques de ransomware em tempo real**

  Para mais detalhes, consulte **Ativação da prevenção de ransomware e do backup**.
- **Pós-evento: minimize as perdas e recupere rapidamente os serviços**

  Para mais detalhes, consulte **Restauração de dados do servidor**.

Configuração da proteção contra ransomware

De acordo com as estatísticas de eventos de segurança da Huawei Cloud, o uso de HSS e CBR juntos pode melhorar muito seus recursos abrangentes de defesa contra ransomware. Para fornecer uma proteção contra ransomware mais forte com esses serviços, é aconselhável ativar a política de proteção contra ransomware da edição premium do HSS e ativar e configurar o backup CBR permanente em nível de hora.

Host Security Service (HSS)	Cloud Backup and Recovery (CBR)	Probabilidade de criptografia	Probabilidade de recuperação	Classificação de proteção contra ransomware (0-100)

Edição	Política de proteção contra ransomware	Status da configuração	Período de backup mais curto (recomendado)			
-	-	-	-	Alta (90%)	0%	0
Edição básica	Não suportada	-	-	Alta (90%)	0%	0
Edição empresarial	Não suportada	-	-	Alta (85%)	0%	10
Edição premium	Não configurada	-	-	Média (50%)	0%	15
Edição básica/não ativada	Não suportada	Configurado	Dia	Alta (90%)	50%	20
Edição empresarial	Não suportada	Configurado	Dia	Alta (85%)	50%	30
Edição básica/não ativada	Não suportada	Configurado	Hora	Alta (90%)	90%	30
Edição premium	Não configurada	Configurado	Dia	Média (50%)	50%	35
Edição empresarial	Não suportada	Configurado	Hora	Alta (85%)	90%	40
Edição premium	Não configurada	Configurado	Hora	Média (50%)	90%	45
Edição premium	Configurada	-	-	Baixa (< 10%)	0%	60
Edição premium	Configurada	Configurado	Dia	Baixa (< 10%)	50%	80

Edição premium	Configurada	Configurado	Hora	Baixa (< 10%)	90%	90
Edição premium	**Configurada**	**Configurado**	**Hora (backup permanente)**	**Baixa (< 10%)**	**90%**	**99 (recomendada)**

4.4.2 Identificação e correção de ransomware

Depois de sermos atacados por ransomware, precisamos identificar e isolar o ransomware e fazer backup e restaurar os dados do serviço em tempo hábil. O HSS da Huawei Cloud usa mecanismos de detecção de ransomware e potes de mel dinâmicos para impedir que o ransomware invada seu sistema, criptografe dados ou se espalhe para outros dispositivos. O HSS pode detectar e remover ransomware em segundos, fazer backup e recuperar dados de serviço em minutos e fornecer recursos de prevenção e controle de ransomware líderes do setor.

De acordo com as estatísticas da Huawei Cloud sobre eventos de intrusão de segurança, 90% dos ataques de ransomware são resultados de senhas fracas, explorações de vulnerabilidades e configurações de linha de base inseguras. A identificação e a correção de riscos antes de intrusões reais podem melhorar significativamente a segurança do sistema. O HSS da Huawei Cloud ajuda você a identificar rapidamente os riscos e fornece reparo com um clique para reduzir os custos de O&M da empresa.

Aumento da força da senha

O HSS verifica automaticamente os servidores todas as manhãs cedo em busca de senhas fracas comuns e **das senhas que você baniu**. Em seguida, você pode pedir aos usuários com senhas fracas que definam senhas mais fortes. O HSS pode detectar senhas fracas em SSH, FTP e MySQL.

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** > **HSS**.

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

Passo 4 Clique na guia **Common Weak Password Detection** para visualizar as senhas fracas do servidor.

Passo 5 Faça logon nos servidores para fortalecer senhas fracas com base nos nomes de servidores, nomes de contas e tipos de contas correspondentes às senhas fracas detectadas.

Depois de fortalecer senhas fracas, é aconselhável realizar a **verificação manual** imediatamente.

----Fim

Fortalecimento das configurações de linha de base

O HSS verifica o seu software para configurações inseguras todas as manhãs cedo e fornece sugestões. Você pode modificar suas configurações adequadamente para aumentar a segurança do servidor.

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

Passo 2 No painel de navegação à esquerda, escolha **Prediction** > **Baseline Checks**.

Passo 3 Clique na guia **Unsafe Configurations** para visualizar as configurações não seguras do servidor.

Passo 4 Clique no nome da linha de base de destino. A página de detalhes da linha de base é exibida.

Passo 5 Clique na guia **Check Items** e clique em **Failed** para visualizar itens de risco de linha de base.

Passo 6 Clique em **View Details** na coluna **Operation** de um item de verificação para visualizar as sugestões de modificação e os servidores afetados.

Passo 7 Faça logon no servidor afetado e fortaleça a configuração com base nas sugestões de modificação.

Passo 8 Depois de fortalecer uma configuração, clique em **Verify** na coluna **Operation** para verificar o resultado do fortalecimento.

NOTA

É aconselhável repetir as etapas anteriores para corrigir todas as configurações de alto risco.

----Fim

Correção de vulnerabilidades

Por padrão, o HSS realiza automaticamente uma detecção abrangente de vulnerabilidades todas as semanas e fornece sugestões de correção. Você pode corrigir as vulnerabilidades com base nas sugestões. Você também pode configurar o período de detecção automática de vulnerabilidades. Para obter detalhes, consulte **Verificação automática de vulnerabilidades**.

NOTA

Existem quatro níveis de prioridade de correção de vulnerabilidades: crítico, alto, médio e baixo. É aconselhável corrigir prontamente as vulnerabilidades dos níveis crítico e alto e corrigir as vulnerabilidades dos níveis médio e baixo com base nos requisitos do serviço.

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

Passo 2 No painel de navegação à esquerda, escolha **Prediction** > **Vulnerabilities**. A página de gerenciamento de vulnerabilidades é exibida.

Passo 3 Clique nas guias **Linux Vulnerabilities**, **Windows Vulnerabilities**, **Web-CMS Vulnerabilities** e **Application Vulnerabilities** para visualizar as vulnerabilidades do servidor.

Passo 4 Corrija vulnerabilidades com base nos tipos de vulnerabilidades.

- Vulnerabilidades do Linux e do Windows

  Na linha da vulnerabilidade que você deseja corrigir, clique em **Fix** na coluna **Operation**.

Você também pode selecionar várias vulnerabilidades e clicar em **Fix** no canto superior esquerdo da lista de vulnerabilidades para corrigi-las em lotes.

- Vulnerabilidades de Web-CMS e vulnerabilidades de aplicações

  a. Clique em um nome de vulnerabilidade para visualizar as sugestões de correção de vulnerabilidades.

  b. Faça logon no servidor afetado pela vulnerabilidade e corrija manualmente a vulnerabilidade.

     A correção de vulnerabilidades pode afetar a estabilidade do serviço. Você é aconselhado a usar um dos seguintes métodos para evitar tais impactos:

     - Método 1: criar uma nova VM para corrigir a vulnerabilidade.

       1) Crie uma imagem para que o ECS seja corrigido.

          Para obter detalhes, consulte **Criação de uma imagem de ECS completo a partir de um ECS**.

       2) Use a imagem para criar um ECS.

          Para obter detalhes, consulte **Criação de um ECS a partir de uma imagem**.

       3) Corrija a vulnerabilidade no novo ECS e verifique o resultado.

       4) Mude os serviços para o novo ECS e verifique se eles estão funcionando de forma estável.

       5) 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.

       1) Crie um backup para que o ECS seja corrigido.

          Para obter detalhes, consulte **Criação de um backup do CSBS**.

       2) Corrija vulnerabilidades no servidor atual.

       3) 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.

     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 alternância 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.

  c. Depois que uma vulnerabilidade for corrigida, clique no nome da vulnerabilidade para acessar a página de detalhes da vulnerabilidade.

  d. Clique na guia **Affected** e escolha **More** > **Verify** na coluna **Operation** de um ativo ou endereço IP afetado para verificar o resultado da correção da vulnerabilidade.

----Fim

4.4.3 Ativação da prevenção de ransomware e do backup

Depois de sermos atacados por ransomware, precisamos identificar e isolar o ransomware e fazer backup e restaurar os dados do serviço em tempo hábil. O HSS usa mecanismos de detecção de ransomware e potes de mel dinâmicos para impedir que o ransomware invada seu sistema, criptografe dados ou se espalhe para outros dispositivos. O HSS pode detectar e remover ransomware em segundos, fazer backup e recuperar dados de serviço em minutos e fornecer recursos de prevenção e controle de ransomware líderes do setor.

Você pode ativar a prevenção de ransomware e o backup para se defender contra ataques de ransomware e reduzir os riscos de perda de serviço, aprimorando os recursos de prevenção de ransomware.

Etapa 1: ativar a prevenção de ransomware

Se a versão do agente instalado no servidor Linux for 3.2.8 ou posterior ou se a versão do agente instalado no servidor Windows for 4.0.16 ou posterior, a prevenção de ransomware será ativada automaticamente com a edição premium, WTP ou de container do HSS. Se a versão do agente não suportar a ativação automática da prevenção de ransomware, você poderá ativá-la manualmente.

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

Passo 2 Escolha **Prevention** > **Ransomware Prevention**.

Passo 3 Clique na guia **Protected Servers**.

Passo 4 Na coluna **Ransomware Prevention 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 5 Na caixa de diálogo **Enable Ransomware Prevention**, confirme as informações do servidor e selecione uma política de proteção.

Passo 6 Clique em **OK**.

Se o **Ransomware Prevention Status** do servidor for alterado para **Enabled**, a proteção de ransomware será ativada com sucesso.

----Fim

Etapa 2: configurar uma política de prevenção de ransomware

Configure os diretórios de arquivos do pote de mel, os diretórios excluídos e os tipos de arquivos protegidos com base nos requisitos do serviço.

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

Passo 2 Escolha **Prevention** > **Ransomware Prevention**.

Passo 3 Clique na guia **Protected Servers**.

Passo 4 Na linha do servidor de destino, clique no nome da política na coluna **Policy**. A página **Edit Policy** é exibida.

Passo 5 Configure as informações de política referindo-se a **Tabela 4-1**.

Tabela 4-1 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**
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 Confirme as informações da política e clique em **OK**.

----Fim

Etapa 3: ativar o backup

Para evitar a perda de serviço causada por ataques de ransomware, ative a função de backup para que seus servidores façam backup periódico dos dados de serviço.

NOTA

Se você não tiver cofres disponíveis, adquira um consultando **Compra de um cofre de backup do servidor** e ative a função de backup.

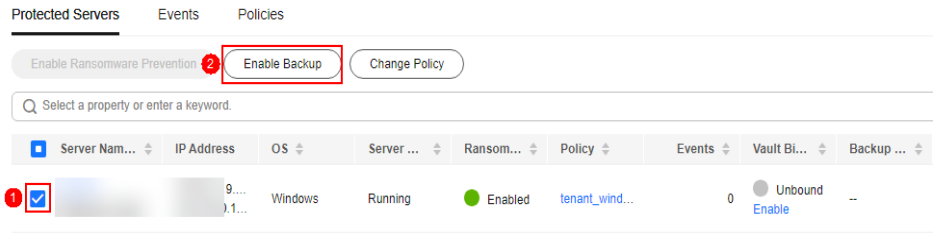
Passo 1 **Faça logon no console de gerenciamento**.

Passo 2 Escolha **Prevention** > **Ransomware Prevention**.

Passo 3 Clique na guia **Protected Servers**.

Passo 4 Selecione um servidor e clique em **Enable Backup** na parte superior da lista de servidores.

Figura 4-3 Ativação do backup



Passo 5 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 6 Clique em **OK**.

----Fim

4.4.4 Restauração de dados do servidor

Atualmente, os ataques de ransomware se desenvolvem rapidamente e nenhuma ferramenta pode fornecer 100% de proteção. Backup e recuperação podem ajudá-lo a minimizar a perda após ataques de ransomware. O CBR da Huawei Cloud pode restaurar rapidamente seus serviços e garantir a execução segura do serviço.

Antes de usar os dados de backup para restaurar os dados de serviço de um servidor, verifique se o backup está disponível. Se o backup estiver disponível, restaure primeiro o sistema de serviço principal.

Procedimento

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

Passo 2 No painel de navegação à esquerda, escolha **Prevention** > **Ransomware Prevention**. A página de prevenção de ransomware é exibida.

Passo 3 Clique na guia **Protected Servers**.

Passo 4 Na coluna **Operation** do servidor de destino, clique em **More** > **Restore Data**.

Passo 5 Na página **Backups** exibida, selecione os dados de backup que você deseja restaurar.

Passo 6 Na coluna **Operation** dos dados de backup de destino, clique em **Restore Data**.

Passo 7 Na página de diálogo exibida, confirme as informações do servidor e configure parâmetros como o disco para armazenar dados.

- **Restart the server immediately after restoration**: se você selecionar essa opção, o servidor será reiniciado automaticamente durante a restauração de dados.
- **Disk Backup**: especifique um disco de armazenamento para a fonte de dados que você deseja fazer backup.

Passo 8 Clique em **OK**.

----Fim

5 Instalação do agente de HSS usando o CBH

Cenário

Se você comprou a edição profissional do Cloud Bastion Host (CBH) da Huawei Cloud, poderá usar o CBH para instalar o agente do HSS em seu servidor. Você não precisa obter a conta e a senha do servidor ou executar comandos de instalação complexos. Você pode instalar facilmente o agente em um ou mais servidores.

Pré-requisitos

- Você adquiriu a edição profissional do CBH e os recursos de servidor gerenciados por meio do CBH.

  Para obter detalhes, consulte **Compra de uma instância do CBH** e **Gerenciamento de recursos do host usando o CBH**.
- O servidor onde o agente será instalado é um servidor Linux do tipo de protocolo SSH e a conexão de rede do servidor é normal.
- Você obteve a conta de administrador do sistema do CBH.

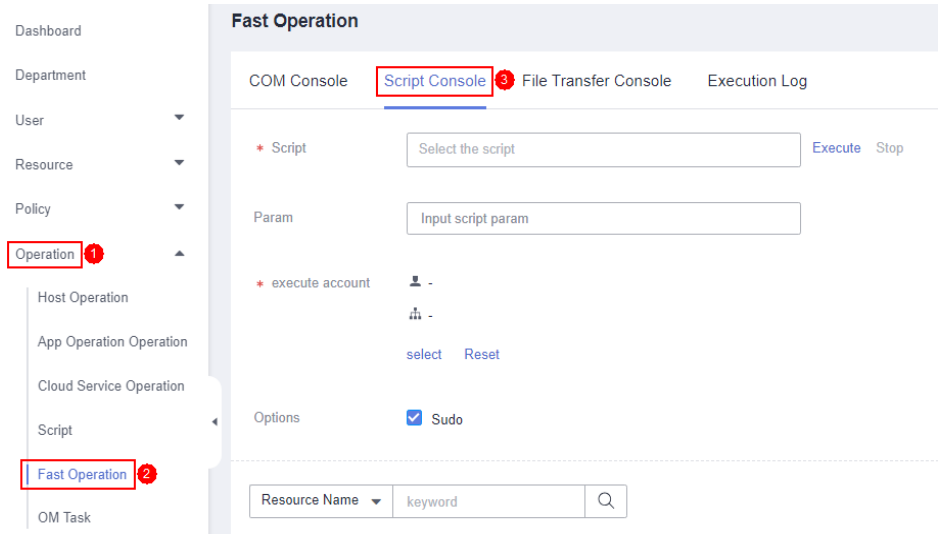
Procedimento

Passo 1 Use a conta de administrador do sistema para **fazer logon no sistema do CBH**.

Passo 2 Na árvore de navegação à esquerda, escolha **Operation** > **Fast Operation**. A página **Fast Operation** é exibida.

Passo 3 Clique na guia **Script Console**.

Figura 5-1 Acesso ao console de script



Passo 4 Configure as informações de O&M do script. **Os parâmetros de O&M de script** descrevem os parâmetros.

Figura 5-2 Configuração de informações de O&M do script

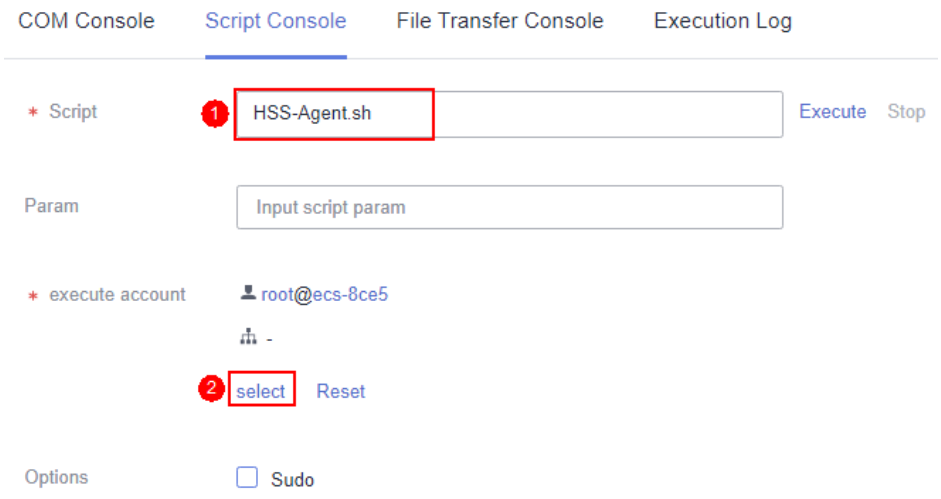


Tabela 5-1 Parâmetros de O&M de script

Parâmetro	Descrição
Script	Selecione o script **HSS-Agent.sh**.
Param	Deixe este parâmetro em branco.
execute account	Clique em **select** e selecione a conta ou o grupo de contas do servidor em que o agente será instalado.
Options	Este parâmetro é opcional. Por padrão, a tarefa de script é executada no arquivo Sudoers no servidor. Se a conta do servidor não tiver a permissão de execução no arquivo, selecione **Sudo**.

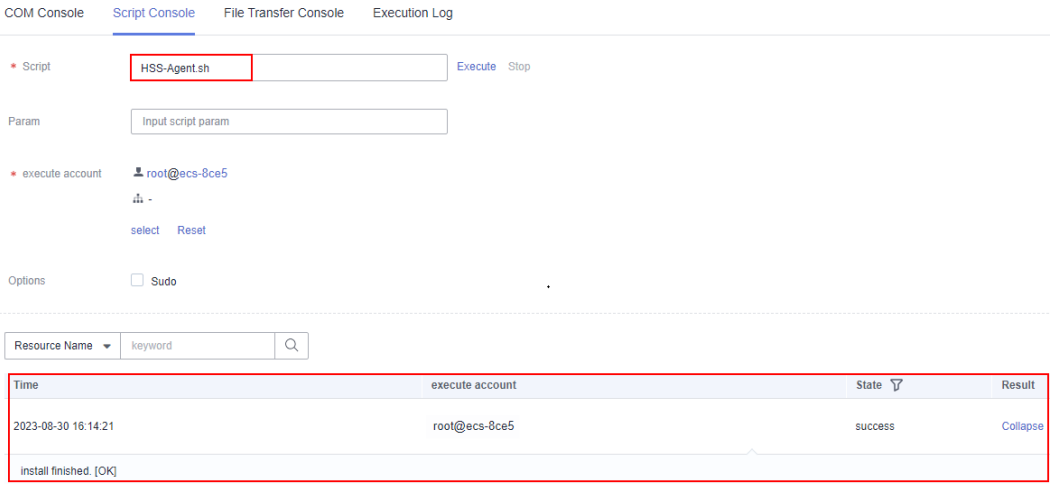
Passo 5 Clique em **Execute**.

Figura 5-3 Execução de uma tarefa de script

Passo 6 Depois que a tarefa de script for executada com sucesso, clique em **Collapse** na coluna **Result** para expandir o resultado da execução.

Se **install finished.[OK]** for exibido, o agente será instalado com sucesso.

Figura 5-4 Execução bem-sucedida de uma tarefa de script

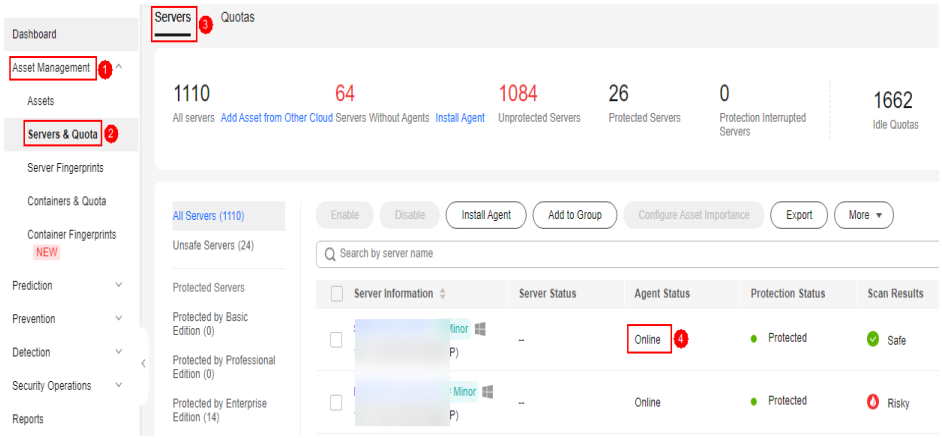


Passo 7 No console do HSS, confirme o resultado da instalação do agente.

1. Faça logon no console de HSS.
2. Na árvore de navegação à esquerda, escolha **Asset Management** > **Servers & Quota**.
3. Na página de guia **Servers**, verifique o status do agente do servidor de destino, conforme mostrado em **Verificação do status do agente**.

   Se o status do agente for **Online**, o agente será instalado com sucesso.

Figura 5-5 Verificação do status do agente



----Fim

A Histórico de alterações

Lançado em	Descrição
17/11/2023	Esta edição é o 7º lançamento oficial. Otimização de: Adição da descrição sobre operações de configuração de proteção em **Melhores práticas para defesa contra ransomware**.
27/10/2023	Esta edição é o 6º lançamento oficial.
10/10/2023	Esta edição é o 5º lançamento oficial. Adição de: **Instalação do agente de HSS usando o CBH**
18/01/2023	Esta edição é o 4º lançamento oficial. Adição de: **Gerenciamento e implementação de várias nuvens do HSS** **Melhores práticas para defesa contra ransomware**
10/12/2022	Esta edição é o 3º lançamento oficial. Modificação das melhores práticas de prevenção de ransomware.
20/10/2022	Esta edição é o 2º lançamento oficial. Adição de **Melhores práticas de reforço da segurança de logon**.
15/06/2022	Esta edição é o 1º lançamento oficial.

