Instalar o plug-in SnapCenter para Microsoft Windows

SnapCenter software

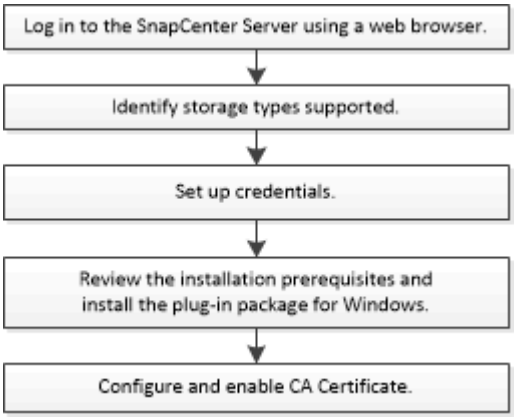
NetApp
November 06, 2025

Índice

Instalar o plug-in SnapCenter para Microsoft Windows

Fluxo de trabalho de instalação do plug-in SnapCenter para Microsoft Windows

Você deve instalar e configurar o SnapCenter Plug-in para Microsoft Windows se quiser proteger arquivos do Windows que não sejam arquivos de banco de dados.



Requisitos de instalação do plug-in SnapCenter para Microsoft Windows

Você deve estar ciente de certos requisitos de instalação antes de instalar o Plug-in para Windows.

Antes de começar a usar o Plug-in para Windows, o administrador do SnapCenter deve instalar e configurar o SnapCenter Server e executar tarefas de pré-requisito.

- Você precisa ter privilégios de administrador do SnapCenter para instalar o Plug-in para Windows.

  A função de administrador do SnapCenter deve ter privilégios de administrador.

- Você deve ter instalado e configurado o SnapCenter Server.
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.
- Você deve configurar o SnapMirror e o SnapVault se quiser replicação de backup.

Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows

Antes de instalar o pacote de plug-ins do SnapCenter para Windows, você deve estar familiarizado com alguns requisitos básicos de espaço e dimensionamento do sistema host.

Item	Requisitos
Sistemas Operacionais	Microsoft Windows Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" . Se você estiver em uma configuração de cluster do Windows, também deverá instalar e configurar o Gerenciamento Remoto do Windows (WinRM).
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	5 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	• Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) • PowerShell Core 7.4.2 Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" . Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet."

Configure suas credenciais para o Plug-in para Windows

O SnapCenter usa credenciais para autenticar usuários para operações do SnapCenter . Você deve criar credenciais para instalar plug-ins do SnapCenter e credenciais adicionais para executar operações de proteção de dados em sistemas de arquivos do Windows.

O que você vai precisar

- Você deve configurar as credenciais do Windows antes de instalar plug-ins.

- Você deve configurar as credenciais com privilégios de administrador, incluindo direitos de administrador, no host remoto.
- Se você configurar credenciais para grupos de recursos individuais e o usuário não tiver privilégios de administrador completos, será necessário atribuir pelo menos os privilégios de grupo de recursos e backup ao usuário.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credencial**.
3. Clique em **Novo**.
4. Na página Credencial, faça o seguinte:

Para este campo…	Faça isso…
Nome da credencial	Digite um nome para as credenciais.

Para este campo…	Faça isso…
Nome de usuário/Senha	Digite o nome de usuário e a senha usados para autenticação. • Administrador de domínio ou qualquer membro do grupo de administradores Especifique o administrador do domínio ou qualquer membro do grupo de administradores no sistema em que você está instalando o plug-in SnapCenter . Os formatos válidos para o campo Nome de usuário são os seguintes: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` ◦ `UserName@upn` • Administrador local (somente para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local integrado no sistema em que você está instalando o plug-in SnapCenter . Você pode especificar uma conta de usuário local que pertença ao grupo de administradores locais se a conta de usuário tiver privilégios elevados ou se o recurso de Controle de Acesso do Usuário estiver desabilitado no sistema host. O formato válido para o campo Nome de usuário é o seguinte: `UserName` Não use aspas duplas (") ou acento grave (`) nas senhas. Você não deve usar os símbolos de menor que (<) e exclamação (!) juntos em senhas. Por exemplo, menor que <! 10, menor que 10 <!, acento grave `12.
Senha	Digite a senha usada para autenticação.

5. Clique em **OK**.

   Depois de concluir a configuração das credenciais, talvez você queira atribuir a manutenção de credenciais a um usuário ou grupo de usuários na página Usuário e Acesso.

Configurar o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite que você crie uma Conta de Serviço Gerenciada de grupo (gMSA) que fornece gerenciamento automatizado de senhas de contas de serviço a partir de uma conta de domínio gerenciada.

Antes de começar

- Você deve ter um controlador de domínio do Windows Server 2016 ou posterior.
- Você deve ter um host Windows Server 2016 ou posterior, que seja membro do domínio.

Passos

1. Crie uma chave raiz do KDS para gerar senhas exclusivas para cada objeto no seu gMSA.
2. Para cada domínio, execute o seguinte comando no controlador de domínio do Windows: Add-KDSRootKey -EffectiveImmediately
3. Crie e configure seu gMSA:
   a. Crie uma conta de grupo de usuários no seguinte formato:

```
 domainName\accountName$
.. Adicione objetos de computador ao grupo.
.. Use o grupo de usuários que você acabou de criar para criar o
gMSA.
```

   Por exemplo,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Correr `Get-ADServiceAccount` comando para verificar a conta de
serviço.
```

4. Configure o gMSA em seus hosts:
   a. Habilite o módulo do Active Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

   Para fazer isso, execute o seguinte comando no PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                            Name                Install State
------------                            ----                -------------
[ ] Active Directory Domain Services    AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. Reinicie seu host.

b. Instale o gMSA no seu host executando o seguinte comando no prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua privilégios administrativos ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no SnapCenter Server.

   O SnapCenter Server instalará os plug-ins selecionados no host e o gMSA especificado será usado como a conta de logon de serviço durante a instalação do plug-in.

Adicionar hosts e instalar o plug-in SnapCenter para Microsoft Windows

Você pode usar a página Adicionar Host do SnapCenter para adicionar hosts do Windows. O plug-in SnapCenter para Microsoft Windows é instalado automaticamente no host especificado. Este é o método recomendado para instalar plug-ins. Você pode adicionar um host e instalar um plug-in para um host individual ou um cluster.

Antes de começar

- Se o sistema operacional do host do SnapCenter Server for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deverá executar o seguinte:
  - Atualize para o Windows Server 2019 (versão do sistema operacional 17763.5936) ou posterior
  - Atualize para o Windows Server 2022 (versão do sistema operacional 20348.2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha permissões de instalação e desinstalação de plug-ins, como a função de administrador do SnapCenter .
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada

ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.

- O usuário do SnapCenter deve ser adicionado à função “Fazer logon como um serviço” do Windows Server.
- Você deve garantir que o serviço de enfileiramento de mensagens esteja em execução.
- Se estiver usando uma conta de serviço gerenciada em grupo (gMSA), você deverá configurar a gMSA com privilégios administrativos.

  "Configurar conta de serviço gerenciada de grupo no Windows Server 2016 ou posterior para o sistema de arquivos do Windows"

Sobre esta tarefa

- Não é possível adicionar um SnapCenter Server como um host de plug-in a outro SnapCenter Server.
- Plug-ins do Windows
  - Microsoft Windows
  - Servidor Microsoft Exchange
  - Servidor Microsoft SQL
  - SAP HANA
- Instalando plug-ins em um cluster

  Se você instalar plug-ins em um cluster (WSFC, Oracle RAC ou Exchange DAG), eles serão instalados em todos os nós do cluster.

- Armazenamento da série E

  Não é possível instalar o Plug-in para Windows em um host Windows conectado ao armazenamento da série E.

O SnapCenter não oferece suporte à adição do mesmo host (host de plug-in) ao SnapCenter se o host já fizer parte de um grupo de trabalho e tiver sido alterado para outro domínio ou vice-versa. Se quiser adicionar o mesmo host, você deve removê-lo do SnapCenter e adicioná-lo novamente.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Certifique-se de que **Hosts gerenciados** esteja selecionado na parte superior.
3. Clique em **Adicionar**.
4. Na página Hosts, faça o seguinte:

Para este campo…	Faça isso…
Tipo de host	Selecione o tipo de host **Windows**. O SnapCenter Server adiciona o host e instala o Plug-in para Windows, caso ele ainda não esteja instalado no host.

Para este campo…	Faça isso…
Nome do host	Digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração correta do DNS. Portanto, a melhor prática é inserir o nome de domínio totalmente qualificado (FQDN). Você pode inserir os endereços IP ou FQDN de um dos seguintes: • Host autônomo • Cluster de Failover do Windows Server (WSFC) Se você estiver adicionando um host usando o SnapCenter e ele fizer parte de um subdomínio, você deverá fornecer o FQDN.
Credenciais	Selecione o nome da credencial que você criou ou crie novas credenciais. A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte informações sobre como criar uma credencial. Detalhes sobre credenciais, incluindo nome de usuário, domínio e tipo de host, são exibidos colocando o cursor sobre o nome da credencial fornecido. O modo de autenticação é determinado pelo tipo de host especificado no assistente Adicionar Host.

5. Na seção Selecionar plug-ins para instalar, selecione os plug-ins a serem instalados.

   Para novas implantações, nenhum pacote de plug-in é listado.

6. (Opcional) Clique em **Mais opções**.

Para este campo…	Faça isso…
Porta	Mantenha o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o SnapCenter Server foi instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão. Se você instalou manualmente os plug-ins e especificou uma porta personalizada, deverá especificar a mesma porta. Caso contrário, a operação falhará.
Caminho de instalação	O caminho padrão é C:\Arquivos de Programas\ NetApp\ SnapCenter. Opcionalmente, você pode personalizar o caminho. Para o pacote de plug-ins SnapCenter para Windows, o caminho padrão é C:\Arquivos de Programas\ NetApp\ SnapCenter. No entanto, se desejar, você pode personalizar o caminho padrão.
Adicionar todos os hosts no cluster	Marque esta caixa de seleção para adicionar todos os nós do cluster em um WSFC.
Ignorar verificações de pré-instalação	Marque esta caixa de seleção se você já instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.
Use a conta de serviço gerenciada em grupo (gMSA) para executar os serviços do plug-in	Marque esta caixa de seleção se desejar usar a Conta de Serviço Gerenciada em Grupo (gMSA) para executar os serviços do plug-in. Forneça o nome do gMSA no seguinte formato: *domainName\accountName$*. O gMSA será usado como uma conta de serviço de logon somente para o serviço SnapCenter Plug-in para Windows.

7. Clique em **Enviar**.

Se você não tiver marcado a caixa de seleção **Ignorar pré-verificações**, o host será validado para verificar se atende aos requisitos para instalar o plug-in. O espaço em disco, a RAM, a versão do PowerShell, a versão do .NET e a localização são validados em relação aos requisitos mínimos. Se os requisitos mínimos não forem atendidos, mensagens de erro ou aviso apropriadas serão exibidas.

Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado em `C:\Program Files\NetApp\SnapCenter` WebApp para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deverá corrigir o problema.

> Em uma configuração de HA, se você estiver atualizando o arquivo web.config, deverá atualizar o arquivo em ambos os nós.

8. Monitore o progresso da instalação.

Instalar o plug-in SnapCenter para Microsoft Windows em vários hosts remotos usando cmdlets do PowerShell

Se você deseja instalar o SnapCenter Plug-in para Microsoft Windows em vários hosts ao mesmo tempo, você pode fazer isso usando o `Install-SmHostPackage` Cmdlet do PowerShell.

Você deve ter efetuado login no SnapCenter como um usuário de domínio com direitos de administrador local em cada host no qual deseja instalar plug-ins.

Passos

1. Inicie o PowerShell.
2. No host do SnapCenter Server, estabeleça uma sessão usando o `Open-SmConnection` cmdlet e insira suas credenciais.
3. Adicione o host autônomo ou o cluster ao SnapCenter usando o `Add-SmHost` cmdlet e os parâmetros necessários.

   As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

4. Instale o plug-in em vários hosts usando o `Install-SmHostPackage` cmdlet e os parâmetros necessários.

   Você pode usar o `-skipprecheck` opção quando você instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.

Instale o plug-in SnapCenter para Microsoft Windows silenciosamente a partir da linha de comando

Você pode instalar o SnapCenter Plug-in para Microsoft Windows localmente em um host Windows se não conseguir instalar o plug-in remotamente a partir da GUI do SnapCenter . Você pode executar o programa de instalação do SnapCenter Plug-in para Microsoft Windows sem supervisão, no modo silencioso, a partir da linha de comando do Windows.

Antes de começar

- Você deve ter instalado o ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) Hosting Bundle.

- Você deve ter instalado o PowerShell 7.4.2 ou posterior.
- Você deve ser um administrador local no host.

Passos

1. Baixe o plug-in SnapCenter para Microsoft Windows do seu local de instalação.

   Por exemplo, o caminho de instalação padrão é C:\ProgramData\ NetApp\ SnapCenter\Package Repository.

   Este caminho pode ser acessado a partir do host onde o SnapCenter Server está instalado.

2. Copie o arquivo de instalação para o host no qual você deseja instalar o plug-in.
3. No prompt de comando, navegue até o diretório onde você baixou o arquivo de instalação.
4. Digite o seguinte comando, substituindo as variáveis pelos seus dados:

   ```
   "snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""
   BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=
   ISFeatureInstall=SCW
   ```

   Por exemplo:

   ```
   `"C:\ProgramData\NetApp\SnapCenter\Package Repository
   \snapcenter_windows_host_plugin.exe"/silent /debuglog"C:
   \HPPW_SCW_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
   SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
   BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
   ISFeatureInstall=SCW`
   ```

   Todos os parâmetros passados durante a instalação do Plug-in para Windows diferenciam maiúsculas de minúsculas.

   Insira os valores para as seguintes variáveis:

Variável	Valor
/debuglog"<Caminho_do_Log_de_Depuração>	Especifique o nome e o local do arquivo de log do instalador do pacote, como no exemplo a seguir: Setup.exe /debuglog"C:\PathToLog\setupexe.log".
PORTA_BI_SNAPCENTER	Especifique a porta na qual o SnapCenter se comunica com o SMCore.
SUITE_INSTALLDIR	Especifique o diretório de instalação do pacote de plug-in do host.
CONTA_DE_SERVIÇO_BI	Especifique o plug-in SnapCenter para a conta de serviço web do Microsoft Windows.

Variável	Valor
BI_SERVICEPWD	Especifique a senha para a conta de serviço web do SnapCenter Plug-in para Microsoft Windows.
Instalação do ISFeature	Especifique a solução a ser implantada pelo SnapCenter no host remoto.

O parâmetro *debuglog* inclui o caminho do arquivo de log do SnapCenter. Gravar neste arquivo de log é o método preferencial para obter informações de solução de problemas, porque o arquivo contém os resultados das verificações que a instalação executa para pré-requisitos de plug-in.

Se necessário, você pode encontrar informações adicionais sobre solução de problemas no arquivo de log do pacote SnapCenter para Windows. Os arquivos de log do pacote são listados (os mais antigos primeiro) na pasta *%Temp%*, por exemplo, *C:\temp*.

A instalação do Plug-in para Windows registra o plug-in no host e não no SnapCenter Server. Você pode registrar o plug-in no SnapCenter Server adicionando o host usando a GUI do SnapCenter ou o cmdlet do PowerShell. Depois que o host é adicionado, o plug-in é descoberto automaticamente.

Monitorar o status de instalação do pacote de plug-in SnapCenter

Você pode monitorar o progresso da instalação do pacote de plug-in SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento da instalação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Trabalhos**, para filtrar a lista de modo que apenas as operações de instalação de plug-ins sejam listadas, faça o seguinte:
   a. Clique em **Filtrar**.
   b. Opcional: especifique a data de início e término.

c. No menu suspenso Tipo, selecione **Instalação de plug-in**.

d. No menu suspenso Status, selecione o status da instalação.

e. Clique em **Aplicar**.

4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

Configurar certificado CA

Gerar arquivo CSR de certificado CA

Você pode gerar uma Solicitação de Assinatura de Certificado (CSR) e importar o certificado que pode ser obtido de uma Autoridade de Certificação (CA) usando o CSR gerado. O certificado terá uma chave privada associada a ele.

CSR é um bloco de texto codificado que é fornecido a um fornecedor de certificado autorizado para obter o certificado de CA assinado.

O comprimento mínimo da chave RSA do certificado CA deve ser de 3072 bits.

Para obter informações sobre como gerar um CSR, consulte "Como gerar um arquivo CSR de certificado CA" .

Se você possui o certificado CA para seu domínio (*.domain.company.com) ou seu sistema (machine1.domain.company.com), você pode pular a geração do arquivo CSR do certificado CA. Você pode implantar o certificado CA existente com o SnapCenter.

Para configurações de cluster, o nome do cluster (FQDN do cluster virtual) e os respectivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome Alternativo do Assunto (SAN) antes de adquirir o certificado. Para um certificado curinga (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados de CA

Você deve importar os certificados de CA para o SnapCenter Server e os plug-ins do host do Windows usando o console de gerenciamento da Microsoft (MMC).

Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados – Computador local** > **Autoridades de certificação raiz confiáveis** > **Certificados**.
5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” e selecione **Todas as Tarefas** > **Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente…	Faça o seguinte…
Importar chave privada	Selecione a opção **Sim**, importe a chave privada e clique em **Avançar**.
Formato de arquivo de importação	Não faça alterações; clique em **Avançar**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluindo o Assistente de Importação de Certificados	Revise o resumo e clique em **Concluir** para iniciar a importação.

O certificado de importação deve ser agrupado com a chave privada (os formatos suportados são: *.pfx, *.p12 e *.p7b).

7. Repita a Etapa 5 para a pasta “Pessoal”.

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma sequência hexadecimal que identifica um certificado. Uma impressão digital é calculada a partir do conteúdo do certificado usando um algoritmo de impressão digital.

Passos

1. Execute o seguinte na GUI:
   a. Clique duas vezes no certificado.
   b. Na caixa de diálogo Certificado, clique na guia **Detalhes**.
   c. Percorra a lista de campos e clique em **Impressão digital**.
   d. Copie os caracteres hexadecimais da caixa.
   e. Remova os espaços entre os números hexadecimais.

      Por exemplo, se a impressão digital for: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", após remover os espaços, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:
   a. Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o certificado instalado recentemente pelo nome do assunto.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Copie a impressão digital.

Configurar certificado CA com serviços de plug-in de host do Windows

Você deve configurar o certificado CA com os serviços de plug-in do host do Windows para ativar o certificado digital instalado.

Execute as seguintes etapas no SnapCenter Server e em todos os hosts de plug-in onde os certificados CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão 8145 do SMCore, executando o seguinte comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Por exemplo:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Vincule o certificado recém-instalado aos serviços de plug-in do host
   do Windows, executando os seguintes comandos:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Por exemplo:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

Habilitar certificados CA para plug-ins

Você deve configurar os certificados CA e implantá-los no SnapCenter Server e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet run *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando *Get-SmCertificateSettings*.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.

3. Selecione hosts de plug-in únicos ou múltiplos.
4. Clique em **Mais opções**.
5. Selecione **Ativar validação de certificado**.

Depois que você terminar

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- *  * indica que o certificado CA não está habilitado nem atribuído ao host do plug-in.
- *  * indica que o certificado CA foi validado com sucesso.
- *  * indica que o certificado CA não pôde ser validado.
- *  * indica que as informações de conexão não puderam ser recuperadas.

Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

Informações sobre direitos autorais

Informações sobre marcas comerciais