



Instale o plug-in do SnapCenter para Microsoft Windows

SnapCenter Software 6.0

NetApp
December 19, 2024

This PDF was generated from https://docs.netapp.com/pt-br/snapcenter/protect-scw/concept_install_snapcenter_plug_in_for_microsoft_windows.html on December 19, 2024. Always check docs.netapp.com for the latest.

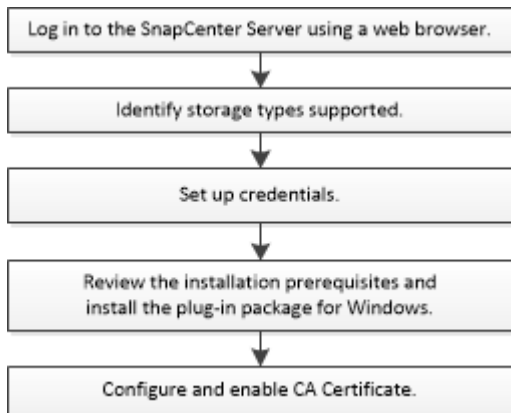
Índice

- Instale o plug-in do SnapCenter para Microsoft Windows 1
 - Fluxo de trabalho de instalação do plug-in SnapCenter para Microsoft Windows 1
 - Requisitos de instalação para o plug-in SnapCenter para Microsoft Windows 1
 - Adicione hosts e instale o plug-in do SnapCenter para Microsoft Windows 5
 - Instale o plug-in do SnapCenter para Microsoft Windows em vários hosts remotos usando cmdlets do PowerShell 9
 - Instale o plug-in do SnapCenter para Microsoft Windows silenciosamente a partir da linha de comando ... 9
 - Monitore o status da instalação do pacote de plug-in SnapCenter 11
 - Configure o certificado CA 12

Instale o plug-in do SnapCenter para Microsoft Windows

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

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



Requisitos de instalação para o 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 servidor SnapCenter e executar tarefas pré-requisitos.


- Você deve ter o SnapCenter admin Privileges para instalar o plug-in para Windows.

A função de administrador do SnapCenter deve ter admin Privileges.

- Você deve ter instalado e configurado o servidor SnapCenter.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar 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 do 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 do sistema host e requisitos de dimensionamento.

Item	Requisitos
Sistemas operacionais	<p>Microsoft Windows</p> <p>Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".</p>
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	<p>5 GB</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.</p> </div>
Pacotes de software necessários	<ul style="list-style-type: none"> • .NET Core começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • PowerShell Core 7.4.2 <p>Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".</p> <p>Para obter informações específicas de solução de problemas .NET, consulte "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conectividade com a Internet."</p>

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 a instalação de 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 os plug-ins.
- Você deve configurar as credenciais com o Privileges de administrador, incluindo direitos de administrador, no host remoto.
- Se você configurar credenciais para grupos de recursos individuais e o usuário não tiver Privileges de administrador completo, será necessário atribuir ao usuário pelo menos o grupo de recursos e Privileges

de backup.

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 (credencial), faça o seguinte:

Para este campo...	Faça isso...
Nome da credencial	Introduza um nome para as credenciais.
Nome de utilizador/Palavra-passe	<p>Introduza o nome de utilizador e a palavra-passe utilizados para autenticação.</p> <ul style="list-style-type: none">• Administrador de domínio ou qualquer membro do grupo de administradores <p>Especifique o administrador do domínio ou qualquer membro do grupo de administradores no sistema no qual você está instalando o plug-in do SnapCenter. Os formatos válidos para o campo Nome de usuário são os seguintes:</p> <ul style="list-style-type: none">◦ NetBIOS\UserName◦ Domain FQDN\UserName◦ UserName@upn <ul style="list-style-type: none">• Administrador local (apenas para grupos de trabalho) <p>Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo Nome de usuário é o seguinte: <code>UserName</code></p> <p>Não use aspas duplas (") ou backtick (`) nas senhas. Você não deve usar os símbolos menos de (>) e exclamação (!) juntos em senhas. Por exemplo, <code>lessthan!10</code>, <code>lessthan10You!</code>, <code>backtick'12</code>.</p>

Para este campo...	Faça isso...
Palavra-passe	Introduza a palavra-passe utilizada 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.

Configure o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite criar uma conta de serviço gerenciado de grupo (gMSA) que fornece gerenciamento automatizado de senha de conta de serviço a partir de uma conta de domínio gerenciado.

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 é um membro do domínio.

Passos

1. Crie uma chave raiz KDS para gerar senhas exclusivas para cada objeto em seu gMSA.
2. Para cada domínio, execute o seguinte comando do 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,...>  
.. Execute `Get-ADServiceAccount` o comando para verificar a conta de  
serviço.
```

4. Configure o gMSA em seus hosts:

- a. Ative o módulo do Active Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

Para fazer isso, execute o seguinte comando do 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 o host.
- b. Instale o gMSA em seu host executando o seguinte comando a partir do prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`
- c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`
5. Atribua o Privileges administrativo ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no servidor SnapCenter.

O servidor SnapCenter 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.

Adicione hosts e instale o plug-in do SnapCenter para Microsoft Windows

Você pode usar a página Adicionar host do SnapCenter para adicionar hosts do Windows. O plug-in do 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 para um cluster.

Antes de começar

- Se o sistema operacional do host do servidor SnapCenter for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deve executar o seguinte:
 - Atualize para o Windows Server 2019 (versão de SO 17763,5936) ou posterior
 - Atualize para o Windows Server 2022 (versão de SO 20348,2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.

- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o UAC no host.
- O usuário do SnapCenter deve ser adicionado à função "Iniciar sessão como um serviço" do Windows Server.
- Você deve garantir que o serviço de enfileiramento de mensagens esteja no estado em execução.
- Se você estiver usando a conta de serviço gerenciado de grupo (gMSA), você deve configurar o gMSA com Privileges administrativo.

["Configure a conta de serviço gerenciado de grupo no Windows Server 2016 ou posterior para o sistema de arquivos do Windows"](#)

Sobre esta tarefa

- Não é possível adicionar um servidor SnapCenter como um host plug-in a outro servidor SnapCenter.
- Plug-ins do Windows
 - Microsoft Windows
 - Microsoft Exchange Server
 - Microsoft SQL Server
 - SAP HANA
 - Plug-ins personalizados
- Instalar 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 e-Series


Não é possível instalar o plug-in para Windows em um host do Windows conectado ao armazenamento do e-Series.



O SnapCenter não suporta a adição do mesmo host (host plug-in) ao SnapCenter se o host já faz parte de um grupo de trabalho e foi alterado para outro domínio ou vice-versa. Se você quiser adicionar o mesmo host, remova o host do SnapCenter e adicione-o 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 **Add**.
4. Na página hosts, faça o seguinte:

Para este campo...	Faça isso...
Tipo de host	<p>Selecione o tipo de host Windows.</p> <p>O servidor SnapCenter adiciona o host e, em seguida, instala o plug-in para Windows se ele ainda não estiver instalado no host.</p>
Nome do host	<p>Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host.</p> <p>O SnapCenter depende da configuração adequada do DNS. Portanto, a melhor prática é inserir o nome de domínio totalmente qualificado (FQDN).</p> <p>Você pode inserir os endereços IP ou FQDN de um dos seguintes:</p> <ul style="list-style-type: none"> • Anfitrião independente • Cluster de failover do Windows Server (WSFC) <p>Se você estiver adicionando um host usando o SnapCenter e fizer parte de um subdomínio, você deverá fornecer o FQDN.</p>
Credenciais	<p>Selecione o nome da credencial que você criou ou crie as novas credenciais.</p> <p>A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte informações sobre como criar uma credencial.</p> <p>Os detalhes sobre as credenciais, incluindo o nome de usuário, domínio e tipo de host, são exibidos colocando o cursor sobre o nome da credencial fornecida.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>O modo de autenticação é determinado pelo tipo de host especificado no assistente Adicionar host.</p> </div>

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

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

6. (Opcional) clique em **mais opções**.

Para este campo...	Faça isso...
Porta	<p>Guarde o número da porta padrão ou especifique o número da porta.</p> <p>O número da porta padrão é 8145. Se o servidor SnapCenter tiver sido instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Se você instalou manualmente os plug-ins e especificou uma porta personalizada, você deve especificar a mesma porta. Caso contrário, a operação falha.</p> </div>
Caminho de instalação	<p>O caminho padrão é C: Arquivos de programas / NetApp / SnapCenter.</p> <p>Opcionalmente, você pode personalizar o caminho. Para o pacote de plug-ins do SnapCenter para Windows, o caminho padrão é C: Arquivos de programas/NetApp/SnapCenter. No entanto, se quiser, você pode personalizar o caminho padrão.</p>
Adicione todos os hosts no cluster	<p>Marque essa caixa de seleção para adicionar todos os nós de cluster em um WSFC.</p>
Ignorar as verificações de pré-instalação	<p>Marque essa caixa de seleção se você já instalou os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.</p>
Use a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in	<p>Marque essa caixa de seleção se quiser usar a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in.</p> <p>Forneça o nome gMSA no seguinte formato: _Domainname</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>O gMSA será usado como uma conta de serviço de logon apenas para o serviço SnapCenter Plug-in para Windows.</p> </div>

7. Clique em **Enviar**.

Se você não selecionou 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 o local são validados de acordo com os requisitos mínimos. Se os requisitos mínimos não forem cumpridos, são apresentadas mensagens de erro ou de aviso adequadas.

Se o erro estiver relacionado ao espaço em disco ou à RAM, você poderá atualizar o arquivo `web.config` localizado no `C:\Program Files\NetApp\SnapCenter\WebApp` para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deve corrigir o problema.



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

8. Monitorize o progresso da instalação.

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

Se você quiser instalar o plug-in do SnapCenter para Microsoft Windows em vários hosts ao mesmo tempo, use o `Install-SmHostPackage` cmdlet do PowerShell.

Você deve ter feito 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 servidor SnapCenter, estabeleça uma sessão usando `Open-SmConnection` o cmdlet e insira suas credenciais.
3. Adicione o host autônomo ou o cluster ao SnapCenter usando `Add-SmHost` o 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`. Em alternativa, pode também consultar o "[Guia de referência de cmdlet do software SnapCenter](#)".

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

Você pode usar a `-skipprecheck` opção quando tiver instalado os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.

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

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

Antes de começar

- Você deve ter instalado o Microsoft .Net 4.7.2 ou posterior.
- Você deve ter instalado o PowerShell 7.4.2 ou posterior.

- Você deve ter ativado o enfileiramento de mensagens do Windows.
- Você deve ser um administrador local no host.

Passos

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

Por exemplo, o caminho de instalação padrão é C:/ProgramData/NetApp/SnapCenter/Repositório de pacotes.

Este caminho é acessível a partir do host onde o servidor SnapCenter 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 variáveis por 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 são sensíveis a maiúsculas e minúsculas.

Insira os valores para as seguintes variáveis:

Variável	Valor
/debuglog"<Debug_Log_Path>	Especifique o nome e o local do arquivo de log do instalador do pacote, como no exemplo a seguir: setup.exe /debuglog"C:
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.
BI_SERVICEACCOUNT	Especifique o plug-in do SnapCenter para a conta de serviço da Web do Microsoft Windows.

Variável	Valor
BI_SERVICEPWD	Especifique a senha do plug-in do SnapCenter para a conta do serviço da Web do Microsoft Windows.
ISFeatureInstall	Especifique a solução a ser implantada pelo SnapCenter em host remoto.

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

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








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

Monitore o status da instalação do pacote de plug-in SnapCenter

Pode monitorizar o progresso da instalação do pacote de plug-ins do SnapCenter utilizando a página trabalhos. Você pode querer verificar o andamento da instalação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

-  Em curso
-  Concluído com êxito
-  Falha
-  Preenchido com avisos ou não foi possível iniciar devido a avisos
-  Em fila de espera

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, para filtrar a lista de modo a que apenas as operações de instalação de plug-in sejam listadas, faça o seguinte:
 - a. Clique em **filtro**.
 - b. Opcional: Especifique a data de início e fim.

- c. No menu suspenso tipo, selecione **Instalação 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 **Visualizar logs**.

Configure o certificado CA

Gerar arquivo CSR do 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 a CSR gerada. O certificado terá uma chave privada associada a ele.

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



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

Para obter informações sobre como gerar um CSR, "[Como gerar o arquivo CSR do certificado CA](#)" consulte .



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

Para configurações de cluster, o nome do cluster (FQDN de 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 (SAN) do assunto antes de adquirir o certificado. Para um certificado Wild card (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados CA

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

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File > Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola > certificados – computador local > autoridades de Certificação raiz fidedignas > certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" 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 Yes , importe a chave privada e clique em Next .
Importar formato de ficheiro	Não faça alterações; clique em seguinte .
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em Avançar .
Concluir o Assistente de importação de certificados	Revise o resumo e clique em Finish para iniciar a importação.



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

7. Repita o passo 5 para a pasta "Pessoal".

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma cadeia 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 **thumbprint**.
 - 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", depois de remover os espaços, será: "A909502d82ae41433e6f83886b00d4277a32a7b".

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.

Configure o certificado CA com os serviços de plug-in do host do Windows

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

Execute as etapas a seguir no servidor SnapCenter e em todos os hosts de plug-in em que os certificados de CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão SMCore 8145, 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"
```

Ative certificados de CA para plug-ins

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

Antes de começar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet `RUN Set-SmCertificateSettings`.
- Você pode exibir o status do certificado para os plug-ins usando as `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`. Em alternativa, pode também consultar o ["Guia de referência de cmdlet do software SnapCenter"](#).





Passos

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

3. Selecione um ou vários hosts de plug-in.
4. Clique em **mais opções**.
5. Selecione **Ativar Validação de certificado**.

Depois de terminar

O host de guia hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o servidor SnapCenter e o host do plug-in.

-  ** Indica que o certificado da CA não está habilitado nem atribuído ao host do plug-in.
-  ** Indica que o certificado da CA foi validado com êxito.
-  ** Indica que o certificado da 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 são concluídas com êxito.

Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.