



Prepare-se para instalar os plug-ins personalizados do SnapCenter

SnapCenter Software 4.7

NetApp
April 02, 2025

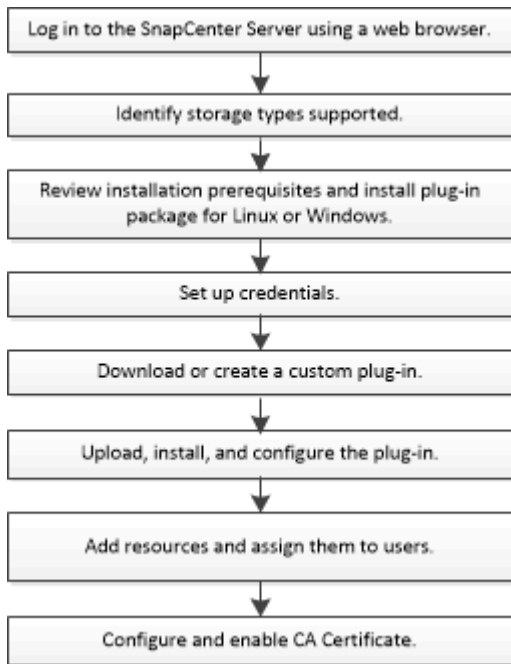
Índice

Prepare-se para instalar os plug-ins personalizados do SnapCenter	1
Fluxo de trabalho de instalação de plug-ins personalizados do SnapCenter	1
Pré-requisitos para adicionar hosts e instalar plug-ins personalizados do SnapCenter	1
Geral	2
Hash SHA512	2
Hosts do Windows	2
Hosts Linux	2
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Windows	3
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Linux	4
Configurar credenciais para plug-ins personalizados do SnapCenter	5
Configure o gMSA no Windows Server 2012 ou posterior	8
Instale os plug-ins personalizados do SnapCenter	9
Adicione hosts e instale pacotes plug-in em hosts remotos	9
Instale pacotes de plug-ins do SnapCenter para Linux ou Windows em vários hosts remotos usando cmdlets	13
Instale os plug-ins personalizados do SnapCenter em hosts Linux usando a interface de linha de comando	14
Monitore o status da instalação de plug-ins personalizados	15
Configurar certificado CA	16
Gerar arquivo CSR do certificado CA	16
Importar certificados CA	16
Obtenha a impressão digital do certificado CA	17
Configure o certificado CA com os serviços de plug-in do host do Windows	17
Configure o certificado CA para o serviço de plug-ins personalizados do SnapCenter no host Linux	18
Configure o certificado de CA para o serviço de plug-ins personalizados do SnapCenter no host do Windows	21
Ative certificados de CA para plug-ins	23

Prepare-se para instalar os plug-ins personalizados do SnapCenter

Fluxo de trabalho de instalação de plug-ins personalizados do SnapCenter

Você deve instalar e configurar plug-ins personalizados do SnapCenter se quiser proteger recursos de plug-in personalizados.



["Desenvolva um plug-in para sua aplicação"](#)

Pré-requisitos para adicionar hosts e instalar plug-ins personalizados do SnapCenter

Antes de adicionar um host e instalar os pacotes de plug-ins, você deve completar todos os requisitos. Os plug-ins personalizados podem ser usados em ambientes Windows e Linux.

- Você deve ter criado um plug-in personalizado. Para obter detalhes, consulte as informações do desenvolvedor.

["Desenvolva um plug-in para sua aplicação"](#)

- Se você quiser gerenciar aplicativos MySQL ou DB2, você deve ter baixado os plug-ins personalizados MySQL e DB2 fornecidos pelo NetApp.
- Você deve ter instalado o Java 1,8, 64 bits em seu host Linux ou Windows.
- 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.

- Os plug-ins personalizados devem estar disponíveis no host do cliente a partir do qual a operação de adição de host é executada.

Geral

Se estiver a utilizar iSCSI, o serviço iSCSI deverá estar em execução.

Hash SHA512

- Para plug-ins personalizados fornecidos pelo NetApp, você deve garantir que você adicionou o hash SHA512 do arquivo de plug-in personalizado ao arquivo *custom_plugin_checksum_list*.

- Para o host Linux, o hash SHA512 está localizado em */var/opt/SnapCenter/scc/custom_plugin_checksum_list.txt*
- Para o host do Windows, o hash SHA512 está localizado em *C:/arquivos de programas/NetApp/SnapCenter Plug-in Creator/custom_plugin_checksum_list.txt*

Para o caminho de instalação personalizado, o hash SHA512 está localizado em *<custom path>/NetApp/SnapCenter/SnapCenter Plug-in Creator/custom_plugin_checksum_list.txt*

O *custom_plugin_checksum_list* faz parte da instalação de plug-in personalizada no host pelo SnapCenter.

- Para plug-ins personalizados criados para o seu aplicativo, você deve ter executado as seguintes etapas:

- a. Gerou o hash SHA512 do arquivo zip do plug-in.

Você pode usar ferramentas on-line como "[Hash SHA512](#)".

- b. Adicionado o hash SHA512 gerado ao arquivo *custom_plugin_checksum_list* em uma nova linha.

Os comentários começam com o símbolo *nº* para identificar o plug-in ao qual o hash pertence.

A seguir está um exemplo de uma entrada de hash SHA512 no arquivo de checksum:

```
#ORASCPM
03721f567a1e4a1cb5569066b9a58af619ee12b1f8713108f81b696cfbdb81c25232fa63
d6e6777a2b2a1ec068bb0a93a59a8ade71587182f8bccbe81f7e0ba6
```

Hosts do Windows

- Você deve ter um usuário de domínio com Privileges de administrador local com permissões de login local no host remoto.
- Se você gerenciar nós de cluster no SnapCenter, precisará ter um usuário com Privileges administrativo para todos os nós do cluster.

Hosts Linux

- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.

- Você deve ter instalado o Java 1,8 64-bit, em seu host Linux.

Se você estiver usando o Windows 2019 ou o Windows 2016 para o host do servidor SnapCenter, instale o Java 1,8 de 64 bits. A ferramenta de Matriz de interoperabilidade (IMT) contém as informações mais recentes sobre os requisitos.

["Downloads Java para todos os sistemas operacionais"](#)

["Ferramenta de Matriz de interoperabilidade do NetApp"](#)


- Você deve configurar o sudo Privileges para que o usuário não-root forneça acesso a vários caminhos. Adicione as seguintes linhas ao arquivo /etc/sudoers usando o utilitário visudo Linux. Por exemplo,

```
Cmnd_Alias SCCMD = /opt/NetApp/snapcenter/scc/bin/scc <non_root_user>
ALL=(ALL) NOPASSWD:SETENV: SCCMD
```

non_root_user é o nome do usuário não-root que você criou.

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	Microsoft Windows Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	5 GB <div style="display: flex; align-items: center;">  <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>

Item	Requisitos
Pacotes de software necessários	<ul style="list-style-type: none"> • Microsoft .NET Framework 4.7.2 ou posterior • Windows Management Framework (WMF) 4,0 ou posterior • PowerShell 4,0 ou posterior <p>Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".</p> <p>Para obter informações sobre solução de problemas do .NET, "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conectividade com a Internet" consulte .</p>

Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Linux

Você deve garantir que o host atenda aos requisitos antes de instalar o pacote de plug-ins do SnapCenter para Linux.

Item	Requisitos
Sistemas operacionais	<ul style="list-style-type: none"> • Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
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>2 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>

Item	Requisitos
Pacotes de software necessários	<p>Java 1,8 (64-bit) Oracle Java ou OpenJDK sabores</p> <p>Se você atualizou O JAVA para a versão mais recente, você deve garantir que a opção JAVA_HOME localizada em /var/opt/SnapCenter/spl/etc/spl.properties esteja definida para a versão JAVA correta e o caminho correto.</p>

Para obter as informações mais recentes sobre versões suportadas, consulte a. ["Ferramenta de Matriz de interoperabilidade do NetApp"](#)

Configurar credenciais para plug-ins personalizados do SnapCenter

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 bancos de dados ou sistemas de arquivos do Windows.

O que você vai precisar

- Hosts Linux

Você deve configurar credenciais para instalar plug-ins em hosts Linux.

Você deve configurar as credenciais para o usuário raiz ou para um usuário não-root que tenha sudo Privileges para instalar e iniciar o processo de plug-in.

Prática recomendada: embora você tenha permissão para criar credenciais para Linux após implantar hosts e instalar plug-ins, a prática recomendada é criar credenciais após adicionar SVMs, antes de implantar hosts e instalar plug-ins.

- Hosts do Windows

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.

- Aplicativos de plug-ins personalizados

O plug-in usa as credenciais selecionadas ou criadas ao adicionar um recurso. Se um recurso não exigir credenciais durante operações de proteção de dados, você pode definir as credenciais como **Nenhuma**.

Sobre esta tarefa

Se você configurar credenciais para grupos de recursos individuais e o nome de usuário não tiver Privileges de administrador completo, será necessário atribuir pelo menos o grupo de recursos e Privileges de backup ao

nome de usuário.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credential**.
3. Clique em **novo**.

Credential

Provide information for the Credential you want to add

Credential Name

Username i

Password


Authentication

Use sudo privileges i

Cancel OK

4. Na página Credential (credencial), especifique as informações necessárias para configurar credenciais:

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

Para este campo...	Faça isso...
Nome de utilizador	<p>Introduza o nome de utilizador e a palavra-passe a utilizar para a 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. Formatos válidos para o campo Nome de usuário são:</p> <ul style="list-style-type: none"> <i>NetBIOS_username</i> <i>Domain FQDN_username</i> <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: <i>Nome de usuário</i></p>
Palavra-passe	Introduza a palavra-passe utilizada para autenticação.
Modo de autenticação	Selecione o modo de autenticação que pretende utilizar.
Use sudo Privileges	<p>Marque a caixa de seleção Use sudo Privileges se estiver criando credenciais para um usuário que não seja root.</p> <p> Aplicável apenas a usuários Linux.</p>

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 2012 ou posterior

O Windows Server 2012 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.

O que você vai precisar

- Você deve ter um controlador de domínio do Windows Server 2012 ou posterior.
- Você deve ter um host Windows Server 2012 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.

Instale os plug-ins personalizados do SnapCenter

Adicione hosts e instale pacotes plug-in em hosts remotos

Você deve usar a página SnapCenterAdd Host para adicionar hosts e, em seguida, instalar os pacotes de plug-in. Os plug-ins são instalados automaticamente nos hosts remotos. Você pode adicionar um host e instalar os pacotes de plug-in para um host individual ou para um cluster.

O que você vai precisar

- 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.
- Você deve garantir que o serviço de enfileiramento de mensagens esteja 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 2012 ou posterior para aplicativos](#)


Sobre esta tarefa


Não é possível adicionar um servidor SnapCenter como um host plug-in a outro servidor SnapCenter.

Se você instalar plug-ins em um cluster (WSFC), os plug-ins serão instalados em todos os nós do cluster.

Passos


1. No painel de navegação esquerdo, clique em **hosts**.
2. Verifique se a guia **hosts gerenciados** está selecionada na parte superior.
3. Clique em **Add**.
4. Na página hosts, execute as seguintes ações:

Para este campo...	Faça isso...
Tipo de host	<p>Selecione o tipo de host:</p> <ul style="list-style-type: none">• Windows• Linux <p> Os plug-ins personalizados podem ser usados em ambientes Windows e Linux.</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 entrar no FQDN.</p> <p>Para ambientes Windows, o endereço IP é suportado para hosts de domínio não confiáveis somente se for resolvido para o FQDN.</p> <p>Você pode inserir os endereços IP ou FQDN de um host autônomo.</p> <p>Se você estiver adicionando um host usando o SnapCenter e o host fizer parte de um subdomínio, você deverá fornecer o FQDN.</p>



Para este campo...	Faça isso...
Credenciais	<p>Selecione o nome da credencial que você criou ou crie novas credenciais.</p> <p>As credenciais devem ter direitos administrativos no host remoto. Para obter detalhes, consulte as informações sobre como criar credenciais.</p> <p>Você pode exibir detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você especificou.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar host.</p> </div>

5. Na seção **Select Plug-ins to Install**, selecione os plug-ins a instalar.

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>

Para este campo...	Faça isso...
Caminho de instalação	<p>Os plug-ins personalizados podem ser instalados em um sistema Windows ou em um sistema Linux.</p> <ul style="list-style-type: none"> • Para o pacote de plug-ins do SnapCenter para Windows, o caminho padrão é C: Arquivos de programas/NetApp/SnapCenter. <p>Opcionalmente, você pode personalizar o caminho.</p> <ul style="list-style-type: none"> • Para o pacote de plug-ins do SnapCenter para Linux, o caminho padrão é /opt/NetApp/SnapCenter. <p>Opcionalmente, você pode personalizar o caminho.</p> <ul style="list-style-type: none"> • Para os plug-ins personalizados do SnapCenter: <ul style="list-style-type: none"> i. Na seção Plug-ins personalizados, clique em Procurar e selecione a pasta plug-in personalizado zipado. <p>A pasta zipada contém o código de plug-in personalizado e o arquivo .xml do descritor.</p> <p>Para o plug-in de armazenamento, navegue até <i>C:/ProgramData/NetApp/SnapCenter/Package Repository</i> e <i>Storage.zip</i> selecione a pasta.</p> ii. Clique em Upload. <p>O arquivo .xml do descritor na pasta de plug-in personalizado zipado é validado antes que o pacote seja carregado.</p> <p>Os plug-ins personalizados que são carregados para o servidor SnapCenter são listados.</p> <p>Se você quiser gerenciar aplicativos MySQL ou DB2, você pode usar os plug-ins personalizados MySQL e DB2 fornecidos pelo NetApp.</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>

Para este campo...	Faça isso...
Use a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in	<p>Para o host Windows, marque essa caixa de seleção se desejar usar a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in.</p> <p> Forneça o nome do gMSA no seguinte formato:</p> <p> O gMSA será usado como uma conta de serviço de logon apenas para o serviço SnapCenter Plug-in para Windows.</p>

7. Clique em **Enviar**.

Se você não tiver selecionado a caixa de seleção **Ignorar pré-verificações**, o host será validado para verificar se o host atende aos requisitos para a instalação do plug-in. O espaço em disco, a RAM, a versão do PowerShell, a versão do .NET, a localização (para plug-ins do Windows) e a versão Java (para plug-ins do Linux) 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 pode atualizar o arquivo web.config localizado no NetApp SnapCenter 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. Se o tipo de host for Linux, verifique a impressão digital e clique em **Confirm and Submit**.



A verificação de impressões digitais é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitorize o progresso da instalação.

Os arquivos de log específicos da instalação estão localizados em /custom_location/SnapCenter/logs.

Instale pacotes de plug-ins do SnapCenter para Linux ou Windows em vários hosts remotos usando cmdlets

Você pode instalar os Pacotes de plug-in do SnapCenter para Linux ou Windows em vários hosts simultaneamente usando o cmdlet Install-SmHostPackage PowerShell.

O que você vai precisar

O usuário que adiciona um host deve ter os direitos administrativos no host.

Passos

1. Inicie o PowerShell.
2. No host do servidor SnapCenter, estabeleça uma sessão usando o cmdlet `Open-SmConnection` e insira suas credenciais.
3. Instale o plug-in em vários hosts usando o cmdlet `Install-SmHostPackage` 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"](#).

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

4. Insira suas credenciais para instalação remota.

Instale os plug-ins personalizados do SnapCenter em hosts Linux usando a interface de linha de comando

Você deve instalar os plug-ins personalizados do SnapCenter usando a interface de usuário (UI) do SnapCenter. Se o seu ambiente não permitir a instalação remota do plug-in a partir da IU do SnapCenter, você pode instalar os plug-ins personalizados no modo console ou no modo silencioso usando a interface de linha de comando (CLI).

Passos

1. Copie o pacote de plug-ins do SnapCenter para o arquivo de instalação do Linux (`SnapCenter_linux_host_plugin.bin`) do repositório de pacotes `C: NetApp/SnapCenter` para o host onde você deseja instalar os plug-ins personalizados.

Você pode acessar esse caminho a partir do host onde o servidor SnapCenter está instalado.

2. No prompt de comando, navegue até o diretório onde você copiou o arquivo de instalação.
3. Instale o plug-in: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`
 - `-DPORT` especifica a porta de comunicação HTTPS SMCORE.
 - `-DSERVER_IP` especifica o endereço IP do servidor SnapCenter.
 - `-DSERVER_HTTPS_PORT` especifica a porta HTTPS do servidor SnapCenter.
 - `-DUSER_INSTALL_DIR` especifica o diretório onde você deseja instalar o pacote de plug-ins do SnapCenter para Linux.
 - `DINSTALL_LOG_NAME` especifica o nome do arquivo de log.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```


4. Adicione o host ao servidor SnapCenter usando o cmdlet Add-Smhost e os parâmetros necessários.

As informações sobre os parâmetros que podem ser usados com o comando 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](#)".

5. Faça login no SnapCenter e faça o upload do plug-in personalizado a partir da IU ou usando cmdlets do PowerShell.

Pode carregar o plug-in personalizado a partir da IU consultando "[Adicione hosts e instale pacotes plug-in em hosts remotos](#)" a secção.

A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm mais informações sobre cmdlets do PowerShell.






["Guia de referência de cmdlet do software SnapCenter"](#).

Monitore o status da instalação de plug-ins personalizados

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 **trabalhos**.
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 da tarefa, clique em **Exibir logs**.

Configurar 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.

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 .

Nesta janela do assistente...	Faça o seguinte...
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"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid"
```

Configure o certificado CA para o serviço de plug-ins personalizados do SnapCenter no host Linux

Você deve gerenciar a senha do armazenamento de chaves de plug-ins personalizados e seu certificado, configurar o certificado de CA, configurar certificados raiz ou intermediários para o armazenamento de confiança de plug-ins personalizados e configurar o par de chaves assinadas de CA para armazenamento de confiança de plug-ins personalizados personalizados com o serviço de plug-ins personalizados SnapCenter para ativar o certificado digital instalado.

Plug-ins personalizados usam o arquivo 'keystore.jks', que está localizado em `/opt/NetApp/SnapCenter/scc/etc` tanto como seu armazenamento de confiança e armazenamento de chaves.

Gerenciar senha para armazenamento de chaves plug-in personalizado e alias do par de chaves assinadas CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in personalizado do arquivo de propriedade do agente do plug-in personalizado.

É o valor correspondente à chave 'KEYSTORE_PASS'.

2. Altere a senha do keystore:

```
keytool -storepasswd -keystore keystore.jks  
. Altere a senha para todos os aliases de entradas de chave privada no  
keystore para a mesma senha usada para o keystore:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Atualize o mesmo para a chave `KEYSTORE_PASS` no arquivo *agent.properties*.

3. Reinicie o serviço depois de alterar a senha.



A palavra-passe para o armazenamento de chaves plug-in personalizado e para todas as palavras-passe de alias associadas da chave privada deve ser a mesma.

Configure certificados raiz ou intermediários para armazenamento de confiança de plug-in personalizado

Você deve configurar os certificados raiz ou intermediários sem a chave privada para armazenamento de confiança de plug-in personalizado.

Passos

1. Navegue até a pasta que contém o keystore de plug-in personalizado: `/Opt/NetApp/SnapCenter/scc/etc`.
2. Localize o arquivo 'keystore.jks'.
3. Liste os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione um certificado raiz ou intermediário:

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. Reinicie o serviço depois de configurar os certificados raiz ou  
intermediários para o armazenamento de confiança de plug-in personalizado.
```



Você deve adicionar o certificado de CA raiz e, em seguida, os certificados de CA intermediários.

Configure o par de chaves assinadas da CA para o armazenamento de confiança de plug-in personalizado

Você deve configurar o par de chaves assinadas da CA para o armazenamento de confiança do plug-in personalizado.

Passos

1. Navegue até a pasta que contém o keystore de plug-in personalizado `/opt/NetApp/SnapCenter/scc/etc`.

2. Localize o arquivo 'keystore.jks'.
3. Liste os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione o certificado da CA com chave privada e pública.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Liste os certificados adicionados no keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da CA para a senha do keystore.

A senha padrão do keystore do plug-in personalizado é o valor da chave KEYSTORE_PASS no arquivo agent.properties.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

. Se o nome do alias no certificado da CA for longo e contiver espaço ou caracteres especiais ("*", ",", " "), altere o nome do alias para um nome simples:

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. Configure o nome do alias do certificado CA no arquivo agent.properties.

Atualize este valor com a chave SCC_CERTIFICATE_ALIAS.

8. Reinicie o serviço depois de configurar o par de chaves assinadas pela CA para o armazenamento de confiança de plug-in personalizado.

Configurar a lista de revogação de certificados (CRL) para plug-ins personalizados do SnapCenter

Sobre esta tarefa

- Os plug-ins personalizados do SnapCenter pesquisarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL para plug-ins personalizados do SnapCenter é 'opt/NetApp/SnapCenter/scc/etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo agent.properties contra a chave CRL_PATH.

Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Configure o certificado de CA para o serviço de plug-ins personalizados do SnapCenter no host do Windows

Você deve gerenciar a senha do armazenamento de chaves de plug-ins personalizados e seu certificado, configurar o certificado de CA, configurar certificados raiz ou intermediários para o armazenamento de confiança de plug-ins personalizados e configurar o par de chaves assinadas de CA para armazenamento de confiança de plug-ins personalizados com o serviço de plug-ins personalizados SnapCenter para ativar o certificado digital instalado.

Plug-ins personalizados usam o arquivo *keystore.jks*, que está localizado em `_C: Arquivos de programas, NetApp, SnapCenter, SnapCenter Plug-in Creator`, tanto como seu armazenamento de confiança e armazenamento de chaves.

Gerenciar senha para armazenamento de chaves plug-in personalizado e alias do par de chaves assinadas CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in personalizado do arquivo de propriedade do agente do plug-in personalizado.

É o valor correspondente à chave `KEYSTORE_PASS`.

2. Altere a senha do keystore:

```
keytool -storepasswd -keystore keystore.jks
```



Se o comando "keytool" não for reconhecido no prompt de comando do Windows, substitua o comando keytool por seu caminho completo.

```
C: Arquivos de programas/<jdk_version>/keytool.exe" -storepasswd -keystore keystore.jks
```

3. Altere a senha para todos os aliases de entradas de chave privada no keystore para a mesma senha usada para o keystore:

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Atualize o mesmo para a chave `KEYSTORE_PASS` no arquivo *agent.properties*.

4. Reinicie o serviço depois de alterar a senha.



A palavra-passe para o armazenamento de chaves plug-in personalizado e para todas as palavras-passe de alias associadas da chave privada deve ser a mesma.

Configure certificados raiz ou intermediários para armazenamento de confiança de plug-in personalizado

Você deve configurar os certificados raiz ou intermediários sem a chave privada para armazenamento de confiança de plug-in personalizado.

Passos

1. Navegue até a pasta que contém o armazenamento de chaves de plug-in personalizado *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc*
2. Localize o arquivo 'keystore.jks'.
3. Liste os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione um certificado raiz ou intermediário:

```
Keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_root.cer -keystore keystore.jks
```

5. Reinicie o serviço depois de configurar os certificados raiz ou intermediários para o armazenamento de confiança de plug-in personalizado.



Você deve adicionar o certificado de CA raiz e, em seguida, os certificados de CA intermediários.

Configure o par de chaves assinadas da CA para o armazenamento de confiança de plug-in personalizado

Você deve configurar o par de chaves assinadas da CA para o armazenamento de confiança do plug-in personalizado.

Passos

1. Navegue até a pasta que contém o armazenamento de chaves de plug-in personalizado *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc*
2. Localize o arquivo *keystore.jks*.
3. Liste os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione o certificado da CA com chave privada e pública.

```
Keytool -importkeystore -srckeystore /root/SnapCenter.ssl.test.NetApp.com.pfx -srcstoretype PKCS12 -destkeystore keystore.jks -deststoretype JKS
```

5. Liste os certificados adicionados no keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da CA para a senha do keystore.

A senha padrão do keystore do plug-in personalizado é o valor da chave `KEYSTORE_PASS` no arquivo `agent.properties`.

```
Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore keystore.jks
```

8. Configure o nome do alias do certificado CA no arquivo `agent.properties`.

Atualize este valor com a chave `SCC_CERTIFICATE_ALIAS`.

9. Reinicie o serviço depois de configurar o par de chaves assinadas pela CA para o armazenamento de confiança de plug-in personalizado.

Configurar a lista de revogação de certificados (CRL) para plug-ins personalizados do SnapCenter

Sobre esta tarefa

- Para transferir o ficheiro CRL mais recente para o certificado CA relacionado, "[Como atualizar o arquivo de lista de revogação de certificados no certificado da CA do SnapCenter](#)" consulte .
- Os plug-ins personalizados do SnapCenter pesquisarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL para os plug-ins personalizados do SnapCenter é '`C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator etc/crl`'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo `agent.properties` contra a chave `CRL_PATH`.
2. Você pode colocar mais de um arquivo CRL neste diretório.

Os certificados recebidos serão verificados em relação a cada CRL.

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.

O que você vai precisar

- 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 © 2025 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.