



Prepare-se para instalar o plug-in SnapCenter para MySQL

SnapCenter Software 6.0

NetApp
December 19, 2024

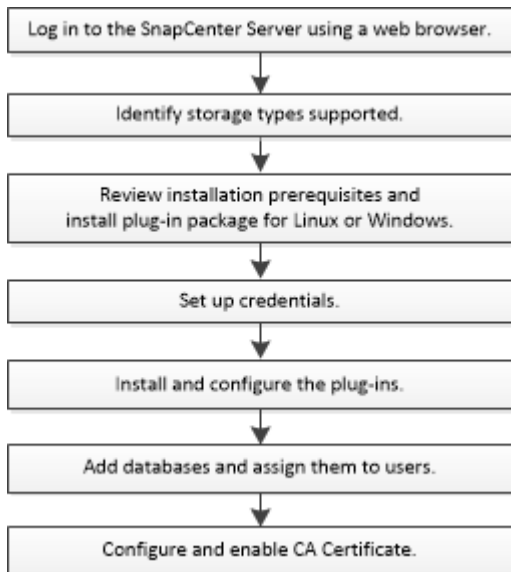
Índice

- Prepare-se para instalar o plug-in SnapCenter para MySQL 1
 - Fluxo de trabalho de instalação do plug-in SnapCenter para MySQL 1
 - Pré-requisitos para adicionar hosts e instalar o plug-in SnapCenter para MySQL 1
 - Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Windows 4
 - Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Linux 5
 - Configure credenciais para o plug-in SnapCenter para MySQL 6
 - Instale o plug-in SnapCenter para MySQL 9
 - Configurar certificado CA 14

Prepare-se para instalar o plug-in SnapCenter para MySQL

Fluxo de trabalho de instalação do plug-in SnapCenter para MySQL

Você deve instalar e configurar o plug-in SnapCenter para MySQL se quiser proteger bancos de dados MySQL.



Pré-requisitos para adicionar hosts e instalar o plug-in SnapCenter para MySQL

Antes de adicionar um host e instalar os pacotes de plug-in, você deve completar todos os requisitos. O plug-in SnapCenter para MySQL está disponível em ambientes Windows e Linux.

- Você deve ter instalado o Java 11 em seu host.



O IBM Java não é suportado.

- Para Windows, o Plug-in Creator Service deve ser executado usando o usuário do Windows "LocalSystem", que é o comportamento padrão quando o Plug-in para MySQL é instalado como administrador de domínio.
- 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 plug-in SnapCenter para Microsoft Windows será implantado por padrão com o plug-in MySQL em hosts Windows.
- O servidor SnapCenter deve ter acesso ao 8145 ou à porta personalizada do plug-in para host MySQL.
- Para o MySQL 5,7, binlog deve ser especificado no arquivo mysql config (my.cnf ou mysql-server.cnf).

Hosts do Windows

- Você deve ter um usuário de domínio com Privileges de administrador local com permissões de login local no host remoto.
- Ao instalar o plug-in para MySQL em um host Windows, o plug-in SnapCenter para Microsoft Windows é instalado automaticamente.
- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.
- Você deve ter instalado o Java 11 em seu host Windows.

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

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

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 11 em seu host Linux.

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

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

- Para bancos de dados MySQL que estão sendo executados em um host Linux, ao instalar o plug-in para MySQL, o plug-in SnapCenter para UNIX é instalado automaticamente.
- Você deve ter **bash** como o shell padrão para instalação do plug-in.

Comandos suplementares

Para executar um comando complementar no plug-in do SnapCenter para MySQL, você deve incluí-lo no arquivo *allowed_commands.config*.

- Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
- Localização padrão no host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config*

Para permitir comandos suplementares no host do plug-in, abra o arquivo *allowed_Commands.config* em um editor. Digite cada comando em uma linha separada e os comandos não são sensíveis a maiúsculas e minúsculas. Certifique-se de especificar o nome de caminho totalmente qualificado e incluir o nome de caminho entre aspas (") se ele contiver espaços.

Por exemplo:

Comando: Comando de montagem: Comando umount: Comando "C: Arquivos de programas/NetApp comandos do SnapCreator" comando: mysript.bat

Se o arquivo *allowed_commands.config* não estiver presente, os comandos ou a execução de script serão bloqueados e o fluxo de trabalho falhará com o seguinte erro:

"[/mnt/mount -a] execução não permitida. Autorize adicionando o comando no arquivo %s no host do plugin."

Se o comando ou script não estiver presente no *allowed_Commands.config*, a execução do comando ou script será bloqueada e o fluxo de trabalho falhará com o seguinte erro:

"[/mnt/mount -a] execução não permitida. Autorize adicionando o comando no arquivo %s no host do plugin."



Você não deve usar uma entrada curinga (*) para permitir todos os comandos.

Configure sudo Privileges para usuários não-root para host Linux

O SnapCenter 2,0 e versões posteriores permitem que um usuário não root instale o pacote de plug-ins do SnapCenter para Linux e inicie o processo de plug-in. Os processos de plug-in serão executados como um usuário não-root eficaz. Você deve configurar o sudo Privileges para que o usuário não-root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Se o umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro devem ter permissão de 555. Caso contrário, a instalação do plug-in pode falhar.
- Para o usuário não-root, certifique-se de que o nome do usuário não-root e do grupo do usuário devem ser os mesmos.
- Edite o arquivo `/etc/ssh/sshd_config` para configurar os algoritmos de código de autenticação de mensagem: Macs hmac-SHA2-256 e MACs hmac-SHA2-512.

Reinicie o serviço sshd depois de atualizar o arquivo de configuração.

Exemplo:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

Sobre esta tarefa

Você deve configurar o sudo Privileges para que o usuário não-root forneça acesso aos seguintes caminhos:

- `/Home/Linux_USER/SC_NetApp/SnapCenter_linux_host_plugin.bin`
- `/Custom_location/NetApp/SnapCenter/spl/installation/plugins/uninstall`
- `/Custom_location/NetApp/SnapCenter/spl/bin/spl`

Passos

1. Faça login no host Linux no qual você deseja instalar o pacote de plug-ins do SnapCenter para Linux.

2. Adicione as seguintes linhas ao arquivo `/etc/sudoers` usando o utilitário visudo Linux.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/  
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,  
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,  
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc  
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/  
LINUX_USER/.sc_netapp/Linux_Prechecks.sh  
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config  
_Check.sh  
Cmnd_Alias SCCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/bin/sc_command_executor  
Cmnd_Alias SCCMDEXECUTOR =checksum_value==  
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor  
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,  
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD  
Defaults: LINUX_USER !visiblepw  
Defaults: LINUX_USER !requiretty
```



Se você estiver tendo uma configuração RAC, juntamente com os outros comandos permitidos, você deve adicionar o seguinte ao arquivo `/etc/sudoers`:
`'/<crs_home>/bin/olsnodes'`

Você pode obter o valor de `crs_Home` do arquivo `/etc/oracle/olr.loc`.

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

Você pode obter o `checksum_value` do arquivo **SC_unix_plugins_checksum.txt**, que está localizado em:


- `_C: /ProgramData/NetApp/SnapCenter/Repositório de pacotes/sc_unix_plugins_checksum.txt` _ se o servidor SnapCenter estiver instalado no host do Windows.
- `./opt/NetApp/SnapCenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` _ se o servidor SnapCenter estiver instalado no host Linux.



O exemplo deve ser usado apenas como referência para criar seus próprios dados.


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"> • DOTNET 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>

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

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

Item	Requisitos
Sistemas operacionais	<ul style="list-style-type: none"> • Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) <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>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>
Pacotes de software necessários	<p>Java 11 Oracle Java e OpenJDK</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> <p>Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".</p>

Configure credenciais para o plug-in SnapCenter para MySQL

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.

Sobre esta tarefa

- 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.

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**.
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> <p>Não use aspas duplas (") ou backtick (`) nas senhas. Você não deve usar os símbolos menos de (>) e exclamação (!) juntos em senhas. Por exemplo, <i>lessthan!10</i>, <i>lessthan10You!</i>, <i>backtick'12</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.

Instale o plug-in SnapCenter para MySQL

Adicione hosts e instale pacotes plug-in em hosts remotos

Você deve usar a página Adicionar host do SnapCenter para adicionar hosts e, em seguida, instalar os pacotes de plug-ins. Os plug-ins são instalados automaticamente nos hosts remotos. Você pode adicionar o host e instalar pacotes de plug-in para um host individual.

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.
- Você deve garantir que o serviço de enfileiramento de mensagens esteja em execução.
- A documentação de administração contém informações sobre o gerenciamento de hosts.


Sobre esta tarefa

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

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	Selecione o tipo de host: <ul style="list-style-type: none">• Windows• Linux <div style="display: flex; align-items: center;"><p>O Plug-in para MySQL tem que ser instalado no servidor de banco de dados MySQL.</p></div>

Para este campo...	Faça isso...
Nome do host	Insira o nome do host de comunicação. Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração adequada do DNS. Portanto, a melhor prática é entrar no FQDN.
Credenciais	<p>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 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 forneceu.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar host. </div>

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

Ao usar a API REST para instalar o Plug-in para MySQL, você deve passar a versão como 3,0. Por exemplo, MySQL:3,0

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. 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;">  Se você instalou manualmente os plug-ins e especificou uma porta personalizada, você deve especificar a mesma porta. Caso contrário, a operação falha. </div>

Para este campo...	Faça isso...
Caminho de instalação	<p>O Plug-in para MySQL é instalado no host cliente MySQL, e este host pode estar 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. Opcionalmente, você pode personalizar o caminho. • Para o pacote de plug-ins do SnapCenter para Linux, o caminho padrão é /opt/NetApp/SnapCenter. Opcionalmente, você pode personalizar o caminho.
Ignorar as verificações de pré-instalação	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.
Adicione todos os hosts no cluster	Não aplicável.
Use a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in	Não aplicável.

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**.

Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós no cluster.



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.

- Para o plug-in do Windows, os logs de instalação e atualização estão localizados em: *C: Plug-in do Windows SnapCenter<JOBID>_*

- Para o plug-in Linux, os logs de instalação estão localizados em: `/var/opt/SnapCenter/logs/SnapCenter_Linux_Host_Plug-in_Install<JOBID>.log_` e os logs de atualização estão localizados em: `/var/opt/SnapCenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade<JOBID>.log_`

Depois de terminar

Se você quiser atualizar para a versão do SnapCenter 6,0, o plug-in baseado EM PERL existente para MySQL será desinstalado do servidor de plug-in remoto.

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.

Antes de começar

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

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 o plug-in SnapCenter para MySQL em hosts Linux usando a interface de linha de comando

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

Antes de começar

- Você deve instalar o Plug-in para MySQL Database em cada um dos hosts Linux onde a instância MySQL deve ser protegida.
- O host Linux no qual você está instalando o plug-in SnapCenter para banco de dados MySQL deve atender aos requisitos de software, banco de dados e sistema operacional dependentes.

A ferramenta de Matriz de interoperabilidade (IMT) contém as informações mais recentes sobre as

configurações suportadas.

"Ferramenta de Matriz de interoperabilidade do NetApp"

- O plug-in do SnapCenter para banco de dados MySQL faz parte do pacote de plug-ins do SnapCenter para Linux. Antes de instalar o pacote de plug-ins do SnapCenter para Linux, você já deve ter instalado o SnapCenter em um host do Windows.

Passos

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

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. Edite o arquivo `/<installation directory>/NetApp/SnapCenter/scc/etc/SC_SMS_Services.properties` e, em seguida, adicione o parâmetro `PLUGINS_ENABLED: MySQL:3,0`.
5. 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"](#).

Monitore o status da instalação do Plug-in para MySQL

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**.

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.



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: "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.

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"
```

Configure o certificado CA para o serviço de plug-ins MySQL 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 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  
intermédios 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  
carateres 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 CA para o serviço de plug-ins MySQL do SnapCenter no host 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 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.

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.