



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

SnapCenter software

NetApp
November 06, 2025

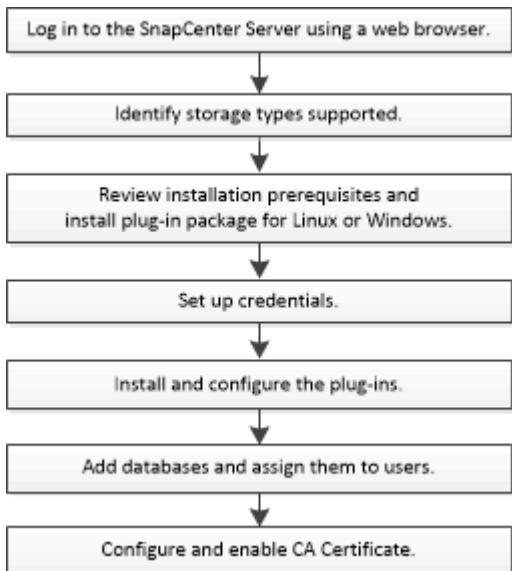
Índice

Prepare-se para instalar o plug-in SnapCenter para PostgreSQL	1
Fluxo de trabalho de instalação do plug-in SnapCenter para PostgreSQL	1
Pré-requisitos para adicionar hosts e instalar o plug-in SnapCenter para PostgreSQL	1
Hosts do Windows	2
Hosts Linux	2
Comandos suplementares	2
Configurar privilégios sudo para usuários não root para host Linux	3
Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows	4
Requisitos de host para instalar o pacote de plug-ins SnapCenter para Linux	5
Configurar credenciais para o plug-in SnapCenter para PostgreSQL	6
Configurar o gMSA no Windows Server 2016 ou posterior	9
Instalar o plug-in SnapCenter para PostgreSQL	10
Adicionar hosts e instalar pacotes de plug-ins em hosts remotos	10
Instalar pacotes de plug-in SnapCenter para Linux ou Windows em vários hosts remotos usando cmdlets	14
Instale o plug-in SnapCenter para PostgreSQL em hosts Linux usando a interface de linha de comando	14
Monitore o status da instalação do Plug-in para PostgreSQL	15
Configurar certificado CA	16
Gerar arquivo CSR de certificado CA	16
Importar certificados de CA	16
Obtenha a impressão digital do certificado CA	17
Configurar certificado CA com serviços de plug-in de host do Windows	18
Configurar o certificado CA para o serviço SnapCenter PostgreSQL Plug-ins no host Linux	18
Configurar o certificado CA para o serviço SnapCenter PostgreSQL Plug-ins no host Windows	21
Habilitar certificados CA para plug-ins	23

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

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

Você deve instalar e configurar o SnapCenter Plug-in para PostgreSQL se quiser proteger clusters PostgreSQL.



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

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

- Você deve ter instalado o Java 11 no seu host.



O IBM Java não é suportado em hosts Windows e Linux.

- No 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 PostgreSQL é instalado como administrador de domínio.
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host. O plug-in SnapCenter para Microsoft Windows será implantado por padrão com o plug-in PostgreSQL em hosts Windows.
- O SnapCenter Server deve ter acesso à porta 8145 ou personalizada do host Plug-in para PostgreSQL.

Hosts do Windows

- Você deve ter um usuário de domínio com privilégios de administrador local e permissões de login local no host remoto.
- Ao instalar o Plug-in para PostgreSQL em um host Windows, o SnapCenter Plug-in 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 no seu host Windows.

["Baixe JAVA para todos os sistemas operacionais"](#)

["Ferramenta de Matriz de Interoperabilidade da 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 no seu host Linux.

["Baixe JAVA para todos os sistemas operacionais"](#)

["Ferramenta de Matriz de Interoperabilidade da NetApp"](#)

- Para clusters PostgreSQL em execução em um host Linux, ao instalar o Plug-in para PostgreSQL, o SnapCenter Plug-in para UNIX é instalado automaticamente.
- Você deve ter **bash** como o shell padrão para instalação de plug-ins.

Comandos suplementares

Para executar um comando suplementar no SnapCenter Plug-in para PostgreSQL, você deve incluí-lo no arquivo `allowed_commands.config`.

- Local padrão no host do Windows: `C:\Arquivos de Programas\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Local 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 diferenciam maiúsculas de minúsculas. Certifique-se de especificar o caminho totalmente qualificado e coloque-o entre aspas ("") se ele contiver espaços.

Por exemplo:

comando: mount comando: umount comando: "C:\Arquivos de Programas\ NetApp\ SnapCreator commands\sdcli.exe" comando: myscript.bat

Se o arquivo `allowed_commands.config` não estiver presente, os comandos ou a execução do 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.

Configurar privilégios sudo para usuários não root para host Linux

O SnapCenter permite que um usuário não root instale o pacote de plug-ins do SnapCenter para Linux e inicie o processo de plug-in. Os processos do plug-in serão executados como um usuário não root efetivo. Você deve configurar privilégios sudo para que o usuário não root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Se a umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro dela tenham permissão de 555. Caso contrário, a instalação do plug-in poderá falhar.
- Para o usuário não root, certifique-se de que o nome do usuário não root e o nome do grupo do usuário sejam os mesmos.
- Edite o arquivo `/etc/ssh/sshd_config` para configurar os algoritmos do código de autenticação de mensagens: MACs hmac-sha2-256 e MACs hmac-sha2-512.

Reinic peace o serviço sshd após 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 privilégios sudo para que o usuário não root forneça acesso aos seguintes caminhos:

- `/home/LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin`
- `/localização_personalizada/ NetApp/snapcenter/spl/instalação/plugins/desinstalação`
- `/localização_personalizada/ NetApp/snapcenter/spl/bin/spl`

Passos

1. Efetue 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 SCCCMDEXECUTOR =checksum_value==  
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor  
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,  
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD  
Defaults: LINUX_USER env_keep += "IATEMPDIR"  
Defaults: LINUX_USER env_keep += "JAVA_HOME"  
Defaults: LINUX_USER !visiblepw  
Defaults: LINUX_USER !requiretty
```

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**, localizado em:

- *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* _ se o SnapCenter Server estiver instalado no host Windows.
- */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* _ se o SnapCenter Server 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 SnapCenter para Windows

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

Item	Requisitos
Sistemas Operacionais	<p>Microsoft Windows</p> <p>Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .</p>
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	<p>5 GB</p> <p></p> <p>Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.</p>
Pacotes de software necessários	<ul style="list-style-type: none"> Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) PowerShell Core 7.4.2 <p>Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .</p> <p>Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet."</p>

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

Antes de instalar o pacote de plug-ins 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 • Servidor SUSE Linux Enterprise (SLES) <p>Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .</p>
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	<p>2 GB</p> <p></p> <p>Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.</p>
Pacotes de software necessários	<p>Java 11 Oracle Java e OpenJDK</p> <p>Se você atualizou o JAVA para a versão mais recente, certifique-se de que a opção JAVA_HOME localizada em /var/opt/snapcenter/spl/etc/spl.properties esteja definida para a versão correta do JAVA e o caminho correto.</p> <p>Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .</p>

Configurar credenciais para o plug-in SnapCenter para PostgreSQL

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 clusters 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 root ou para um usuário não root que tenha privilégios sudo para instalar e iniciar o processo do plug-in.

Melhores práticas: embora você tenha permissão para criar credenciais para o Linux após implantar hosts e instalar plug-ins, a melhor prática é criar credenciais depois de adicionar SVMs, antes de implantar hosts e instalar plug-ins.

- Hosts do Windows

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

Você deve configurar as credenciais com privilégios de administrador, incluindo direitos de administrador no host remoto.

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

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credencial**.
3. Clique em **Novo**.
4. Na página Credencial, especifique as informações necessárias para configurar as credenciais:

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

Para este campo...	Faça isso...
Nome de usuário	<p>Digite o nome de usuário e a senha que serão usados para autenticação.</p> <ul style="list-style-type: none"> Administrador de domínio ou qualquer membro do grupo de administradores <p>Especifique o administrador do domínio ou qualquer membro do grupo de administradores no sistema em que você está instalando o plug-in SnapCenter . Os formatos válidos para o campo Nome de usuário são:</p> <ul style="list-style-type: none"> NetBIOS\Nome do Usuário FQDN do domínio\Nome do usuário <ul style="list-style-type: none"> Administrador local (somente para grupos de trabalho) <p>Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local integrado no sistema em que você está instalando o plug-in SnapCenter . Você pode especificar uma conta de usuário local que pertença ao grupo de administradores locais se a conta de usuário tiver privilégios elevados ou se o recurso de Controle de Acesso do Usuário estiver desabilitado no sistema host. O formato válido para o campo Nome de usuário é: <i>UserName</i></p> <p>Não use aspas duplas ("") ou acento grave (`) nas senhas. Você não deve usar os símbolos de menor que (<) e exclamação (!) juntos em senhas. Por exemplo, menor que <! 10, menor que 10 <!, acento grave `12.</p>
Senha	Digite a senha usada para autenticação.
Modo de autenticação	Selecione o modo de autenticação que você deseja usar.
Use privilégios sudo	<p>Marque a caixa de seleção Usar privilégios sudo se estiver criando credenciais para um usuário não root.</p> <p> Aplicável somente a usuários do 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.

Configurar o gMSA no Windows Server 2016 ou posterior

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

Antes de começar

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

Passos

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

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

Por exemplo,

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

4. Configure o gMSA em seus hosts:

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

Para fazer isso, execute o seguinte comando no PowerShell:

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

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

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

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

- a. Reinicie seu host.
- b. Instale o gMSA no seu host executando o seguinte comando no prompt de comando do PowerShell:
`Install-AdServiceAccount <gMSA>`
- c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua privilégios administrativos ao gMSA configurado no host.

6. Adicione o host do Windows especificando a conta gMSA configurada no SnapCenter Server.

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

Instalar o plug-in SnapCenter para PostgreSQL

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

- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.
- Você deve garantir que o serviço de enfileiramento de mensagens esteja em execução.
- A documentação de administração contém informações sobre o gerenciamento de hosts.
- Se estiver usando uma conta de serviço gerenciada em grupo (gMSA), você deverá configurar a gMSA com privilégios administrativos.

["Configurar conta de serviço gerenciada de grupo no Windows Server 2016 ou posterior para PostgreSQL"](#)

Sobre esta tarefa

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

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Verifique se a aba **Hosts Gerenciados** está selecionada na parte superior.
3. Clique em **Adicionar**.
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> O plug-in para PostgreSQL é instalado no host do cliente PostgreSQL, e esse host pode estar em um sistema Windows ou Linux.</p>
Nome do host	<p>Digite o nome do host de comunicação. Digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração correta do DNS. Portanto, a melhor prática é inserir o FQDN.</p>

Para este campo...	Faça isso...
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 visualizar detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial fornecida.</p> <p> O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar Host.</p>

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

Ao usar a API REST para instalar o Plug-in para PostgreSQL, você deve passar a versão como 3.0. Por exemplo, PostgreSQL:3.0

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

Para este campo...	Faça isso...
Porta	<p>Mantenha o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o SnapCenter Server foi instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão.</p> <p> Se você instalou manualmente os plug-ins e especificou uma porta personalizada, deverá especificar a mesma porta. Caso contrário, a operação falhará.</p>
Caminho de instalação	<p>O plug-in para PostgreSQL é instalado no host do cliente PostgreSQL, e esse host pode estar em um sistema Windows ou Linux.</p> <ul style="list-style-type: none"> Para o pacote de plug-ins 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 SnapCenter para Linux, o caminho padrão é /opt/ NetApp/snapcenter. Opcionalmente, você pode personalizar o caminho.

Para este campo...	Faça isso...
Ignorar verificações de pré-instalação	Marque esta caixa de seleção se você já instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.
Adicionar todos os hosts no cluster	Marque esta caixa de seleção para adicionar todos os nós do cluster.
Use a conta de serviço gerenciada em grupo (gMSA) para executar os serviços do plug-in	<p>Para o host Windows, marque esta caixa de seleção se desejar usar a Conta de Serviço Gerenciada em Grupo (gMSA) para executar os serviços do plug-in.</p> <p> Forneça o nome do gMSA no seguinte formato: domainName\accountName\$.</p> <p> O gMSA será usado como uma conta de serviço de logon somente para o serviço SnapCenter Plug-in para Windows.</p>

7. Clique em **Enviar**.

Se você não tiver marcado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar se ele 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 do Java (para plug-ins do Linux) são validados em relação aos requisitos mínimos. Se os requisitos mínimos não forem atendidos, mensagens de erro ou aviso apropriadas serão exibidas.

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



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

8. Se o tipo de host for Linux, verifique a impressão digital e clique em **Confirmar e Enviar**.

Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós do cluster.



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

9. Monitore o progresso da instalação.

- Para o plug-in do Windows, os logs de instalação e atualização estão localizados em: *C:\Windows\SnapCenter plugin\Install<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_Plugin_Upgrade<JOBID>.log`

Instalar pacotes de plug-in 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` do PowerShell.

Antes de começar

Você deve ter efetuado 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 SnapCenter Server, 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`. Alternativamente, você também pode consultar o "[Guia de referência do 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 PostgreSQL em hosts Linux usando a interface de linha de comando

Você deve instalar o plug-in SnapCenter para cluster PostgreSQL usando a interface de usuário (IU) do SnapCenter. Se o seu ambiente não permitir a instalação remota do plug-in pela interface do usuário do SnapCenter, você poderá instalar o cluster do Plug-in para PostgreSQL no modo de console ou no modo silencioso usando a interface de linha de comando (CLI).

Antes de começar

- Você deve instalar o cluster Plug-in para PostgreSQL em cada host Linux onde o cliente PostgreSQL reside.
- O host Linux no qual você está instalando o plug-in SnapCenter para cluster PostgreSQL deve atender aos requisitos de software, cluster 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 da NetApp"](#)

- O plug-in SnapCenter para cluster PostgreSQL faz parte do pacote de plug-ins SnapCenter para Linux. Antes de instalar o SnapCenter Plug-ins Package para Linux, você já deve ter instalado o SnapCenter em um host Windows.

Passos

1. Copie o arquivo de instalação do pacote de plug-ins do SnapCenter para Linux (snapcenter_linux_host_plugin.bin) de C:\ProgramData\ NetApp\ SnapCenter\Package Repository para o host onde você deseja instalar o plug-in para PostgreSQL.

Você pode acessar esse caminho a partir do host onde o SnapCenter Server 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 do SMCore.
 - -DSERVER_IP especifica o endereço IP do SnapCenter Server.
 - -DSERVER_HTTPS_PORT especifica a porta HTTPS do SnapCenter Server.
 - -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 /<diretório de instalação>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties e adicione o parâmetro `PLUGINS_ENABLED = PostgreSQL:3.0`.
5. Adicione o host ao SnapCenter Server 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`. Alternativamente, você também pode consultar o "[Guia de referência do cmdlet do software SnapCenter](#)".

Monitore o status da instalação do Plug-in para PostgreSQL

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

Sobre esta tarefa

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

- Em andamento
- Concluído com sucesso
- Fracassado

-  Concluído com avisos ou não pode ser iniciado devido a avisos
-  Na fila

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Trabalhos**, para filtrar a lista de modo que apenas as operações de instalação de plug-ins sejam listadas, faça o seguinte:
 - a. Clique em **Filtrar**.
 - b. Opcional: especifique a data de início e término.
 - c. No menu suspenso **Tipo**, selecione **Instalação de plug-in**.
 - d. No menu suspenso **Status**, selecione o status da instalação.
 - e. Clique em **Aplicar**.
4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

Configurar certificado CA

Gerar arquivo CSR de certificado CA

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

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



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

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



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

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

Importar certificados de CA

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

Passos

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

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



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

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

Obtenha a impressão digital do certificado CA

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

Passos

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

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

2. Execute o seguinte no PowerShell:

- 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
```

- Copie a impressão digital.

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

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

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

Passos

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

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

Por exemplo:

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

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

Por exemplo:

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

Configurar o certificado CA para o serviço SnapCenter PostgreSQL Plug-ins no host Linux

Você deve gerenciar a senha do keystore do plug-in e seu certificado, configurar o certificado da CA, configurar certificados raiz ou intermediários para o trust-store do plug-

in e configurar o par de chaves assinadas pela CA para o trust-store do plug-in com o serviço de plug-ins do SnapCenter para ativar o certificado digital instalado.

Os plug-ins usam o arquivo 'keystore.jks', que está localizado em `/opt/NetApp/snapcenter/scc/etc` como seu armazenamento confiável e armazenamento de chaves.

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

Passos

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

É o valor correspondente à chave 'KEYSTORE_PASS'.

2. Alterar a senha do keystore:

```
keytool -storepasswd -keystore keystore.jks
. Altere a senha de 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 após alterar a senha.



A senha para o keystore do plug-in e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para plug-in trust-store

Você deve configurar os certificados raiz ou intermediários sem a chave privada para conectar o trust-store.

Passos

1. Navegue até a pasta que contém o keystore do plug-in: `/opt/NetApp/snapcenter/scc/etc`.
2. Localize o arquivo 'keystore.jks'.
3. Listar 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 após configurar os certificados raiz ou
intermediários para conectar o trust-store.
```



Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Configurar o par de chaves assinadas pela CA para plug-in trust-store

Você deve configurar o par de chaves assinadas pela CA para o trust-store do plug-in.

Passos

1. Navegue até a pasta que contém o keystore do plug-in /opt/NetApp/snapcenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar 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. Listar os certificados adicionados no keystore.

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

6. Verifique se o keystore contém o alias correspondente ao novo certificado CA, que foi adicionado ao keystore.

7. Altere a senha da chave privada adicionada para o certificado CA para a senha do keystore.

A senha padrão do keystore do plug-in 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 espaços  
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 em relação à chave SCC_CERTIFICATE_ALIAS.

8. Reinicie o serviço após configurar o par de chaves assinadas pela CA para plug-in trust-store.

Configurar lista de revogação de certificados (CRL) para plug-ins

Sobre esta tarefa

- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.

- O diretório padrão para os arquivos CRL dos plug-ins do SnapCenter é ' opt/NetApp/snapcenter/scc/etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo `agent.properties` em relação à chave `CRL_PATH`.

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

Configurar o certificado CA para o serviço SnapCenter PostgreSQL Plug-ins no host Windows

Você deve gerenciar a senha do keystore do plug-in e seu certificado, configurar o certificado da CA, configurar certificados raiz ou intermediários para o trust-store do plug-in e configurar o par de chaves assinadas pela CA para o trust-store do plug-in com o serviço de plug-ins do SnapCenter para ativar o certificado digital instalado.

Os plug-ins usam o arquivo `keystore.jks`, que está localizado em `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc` como seu armazenamento confiável e armazenamento de chaves.

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

Passos

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

É o valor correspondente à chave `KEYSTORE_PASS`.

2. Alterar 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 pelo seu caminho completo.

```
C:\Arquivos de Programas\Java\<versão_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

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

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

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

4. Reinicie o serviço após alterar a senha.



A senha para o keystore do plug-in e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para plug-in trust-store

Você deve configurar os certificados raiz ou intermediários sem a chave privada para conectar o trust-store.

Passos

1. Navegue até a pasta que contém o keystore do plug-in C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc
2. Localize o arquivo 'keystore.jks'.
3. Listar 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 após configurar os certificados raiz ou intermediários para conectar o trust-store.



Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Configurar o par de chaves assinadas pela CA para plug-in trust-store

Você deve configurar o par de chaves assinadas pela CA para o trust-store do plug-in.

Passos

1. Navegue até a pasta que contém o keystore do plug-in C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc
2. Localize o arquivo keystore.jks.
3. Listar 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. Listar os certificados adicionados no keystore.

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

6. Verifique se o keystore contém o alias correspondente ao novo certificado CA, que foi adicionado ao keystore.

7. Altere a senha da chave privada adicionada para o certificado CA para a senha do keystore.

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

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

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

Atualize este valor em relação à chave SCC_CERTIFICATE_ALIAS.

9. Reinicie o serviço após configurar o par de chaves assinadas pela CA para plug-in trust-store.

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

Sobre esta tarefa

- Para baixar o arquivo CRL mais recente para o certificado CA relacionado, consulte ["Como atualizar o arquivo de lista de revogação de certificados no SnapCenter CA Certificate"](#) .
- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL dos plug-ins 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` em relação à chave `CRL_PATH`.
2. Você pode colocar mais de um arquivo CRL neste diretório.

Os certificados recebidos serão verificados em relação a cada CRL.

Habilitar certificados CA para plug-ins

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

Antes de começar

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

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

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Selecione hosts de plug-in únicos ou múltiplos.
4. Clique em **Mais opções**.
5. Selecione **Ativar validação de certificado**.

Depois que você terminar

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

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



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

Informações sobre direitos autorais

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 DESTE DOCUMENTO. 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 SOBRESSAENTES; 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 DESTE SOFTWARE, 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.