Prepare-se para instalar o plug-in do SnapCenter para Microsoft SQL Server

SnapCenter Software 4.7

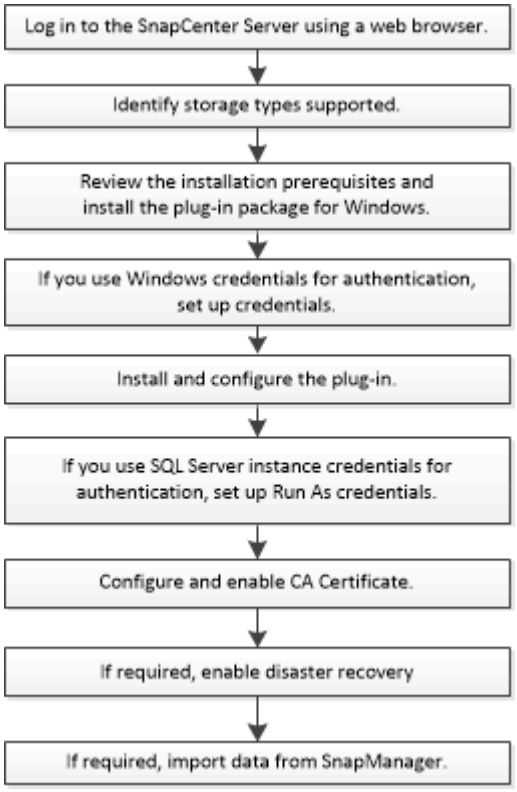
NetApp
April 02, 2025

Índice

Prepare-se para instalar o plug-in do SnapCenter para Microsoft SQL Server

Fluxo de trabalho de instalação para o plug-in SnapCenter para Microsoft SQL Server

Você deve instalar e configurar o plug-in do SnapCenter para o Microsoft SQL Server se quiser proteger bancos de dados do SQL Server.



Pré-requisitos para adicionar hosts e instalar o plug-in do SnapCenter para Microsoft SQL Server

Antes de adicionar um host e instalar os pacotes de plug-ins, você deve completar todos os requisitos.

- Se estiver a utilizar iSCSI, o serviço iSCSI tem de estar em execução.
- Você deve ter um usuário com Privileges de administrador local com permissões de login local no host remoto.
- Se você gerenciar nós de cluster no SnapCenter, precisará ter um usuário com Privileges administrativo para todos os nós do cluster.
- Você deve ter um usuário com permissões sysadmin no SQL Server.

  O plug-in do SnapCenter para Microsoft SQL Server usa o Microsoft VDI Framework, que requer acesso sysadmin.

"Artigo 2926557: As operações de backup e restauração do SQL Server VDI exigem o sysadmin Privileges"

- 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.
- Se o SnapManager for instalado, você deve ter parado ou desativado o serviço e as programações.
- O host deve ser resolvido para o nome de domínio totalmente qualificado (FQDN) do servidor.

  Se o arquivo hosts for modificado para torná-lo resoluvel e se o nome curto e o FQDN forem especificados no arquivo hosts, crie uma entrada no arquivo SnapCenter hosts no seguinte formato: <ip_address> <host_fqdn> <host_name>

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

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

Item	Requisitos
Sistemas operacionais	Microsoft Windows Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	5 GB 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 proteçãoão de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.

Item	Requisitos
Pacotes de software necessários	• Microsoft .NET Framework 4.7.2 ou posterior • Windows Management Framework (WMF) 4,0 ou posterior • PowerShell 4,0 ou posterior Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp". Para obter informações sobre solução de problemas do .NET, "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade com a Internet" consulte .

Configure credenciais para o pacote de plug-ins do SnapCenter para Windows

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

O que você vai precisar

- Você deve configurar as credenciais do Windows antes de instalar os plug-ins.
- Você deve configurar as credenciais com o Privileges de administrador, incluindo direitos de administrador no host remoto.
- Autenticação SQL em hosts Windows

  Você deve configurar credenciais SQL depois de instalar plug-ins.

  Se você estiver implantando o plug-in do SnapCenter para o Microsoft SQL Server, deverá configurar credenciais SQL após a instalação dos plug-ins. Configure uma credencial para um usuário com permissões sysadmin do SQL Server.

  O método de autenticação SQL é autenticado em uma instância do SQL Server. Isso significa que uma instância do SQL Server deve ser descoberta no SnapCenter. Portanto, antes de adicionar uma credencial SQL, você deve adicionar um host, instalar pacotes de plug-in e atualizar recursos. Você precisa de autenticação do SQL Server para executar operações como agendamento ou descoberta de recursos.

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 a credencial.
Nome de utilizador/Palavra-passe	Introduza o nome de utilizador e a palavra-passe a utilizar para a autenticação. • Administrador de domínio Especifique o administrador de domínio no sistema no qual você está instalando o plug-in SnapCenter. Os formatos válidos para o campo Nome de usuário são: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • Administrador local (apenas para grupos de trabalho) 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: `UserName` Não use aspas duplas (") ou backtick (') nas senhas. Você não deve usar os símbolos menos de (>) e exclamação (!) juntos em senhas. Por exemplo, lessthan!10, lessthan10You!, backtick'12.
Modo de autenticação	Selecione o modo de autenticação que pretende utilizar. Se você selecionar o modo de autenticação SQL, você também deve especificar a instância do servidor SQL e o host onde a instância SQL está localizada.

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 credenciais para um recurso do SQL Server individual

Você pode configurar credenciais para executar tarefas de proteção de dados em recursos individuais do SQL Server para cada usuário. Embora você possa configurar as credenciais globalmente, talvez você queira fazer isso apenas para um recurso específico.

Sobre esta tarefa

- Se você estiver usando credenciais do Windows para autenticação, você deve configurar sua credencial antes de instalar plug-ins.

  No entanto, se você estiver usando uma instância do SQL Server para autenticação, você deve adicionar a credencial após a instalação de plug-ins.

- Se você ativou a autenticação SQL durante a configuração das credenciais, a instância descoberta ou o banco de dados será exibida com um ícone de cadeado de cor vermelha.

  Se o ícone de cadeado aparecer, você deve especificar as credenciais da instância ou do banco de dados para adicionar com êxito a instância ou o banco de dados a um grupo de recursos.

- Você deve atribuir a credencial a um usuário de controle de acesso baseado em função (RBAC) sem acesso sysadmin quando as seguintes condições forem atendidas:
  - A credencial é atribuída a uma instância SQL.
  - A instância ou host SQL é atribuída a um usuário RBAC.

    O usuário deve ter o grupo de recursos e o Privileges de backup

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credential**.
3. Para adicionar uma nova credencial, clique em **novo**.
4. Na página Credential (credencial), configure as credenciais:

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

Para este campo…	Faça isso…
Nome de usuário	Introduza o nome de utilizador utilizado para a autenticação do SQL Server. • O administrador de domínio ou qualquer membro do grupo de administradores especificam o administrador do domínio ou qualquer membro do grupo de administradores no sistema no qual você está instalando o plug-in do SnapCenter. Os formatos válidos para o campo **Nome de usuário** são: ◦ *NetBIOS_username* ◦ *Domain FQDN_username* • Administrador local (somente para grupos de trabalho) para sistemas que pertencem a um grupo de trabalho, especifique o administrador local interno 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 **Username** é: *Username*
Senha	Introduza a palavra-passe utilizada para autenticação.
Modo de autenticação	Selecione o modo de autenticação do SQL Server. Você também pode escolher a autenticação do Windows se o usuário do Windows tiver sysadmin Privileges no servidor SQL.
Anfitrião	Selecione o host.
Instância do SQL Server	Selecione a instância do SQL Server.

5. Clique em **OK** para adicionar a credencial.
6. No painel de navegação esquerdo, clique em **Resources**.
7. Na página recursos, selecione **Instância** na lista **Exibir**.
   a. Clique em e selecione o nome do host para filtrar as instâncias.
   b. Clique em para fechar o painel de filtro.
8. Na página proteção de instância, proteja a instância e, se necessário, clique em **Configurar credenciais**.

   Se o usuário que está conetado ao servidor SnapCenter não tiver acesso ao plug-in do SnapCenter para Microsoft SQL Server, o usuário terá que configurar as credenciais.

A opção credencial não se aplica a bancos de dados e grupos de disponibilidade.

9. Clique em **Atualizar recursos**.

Configure o gMSA no Windows Server 2012 ou posterior

O Windows Server 2012 ou posterior permite criar uma conta de serviço gerenciado de grupo (gMSA) que fornece gerenciamento automatizado de senha de conta de serviço a partir de uma conta de domínio gerenciado.

O que você vai precisar

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

Passos

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

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

   Por exemplo,

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

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

   Para fazer isso, execute o seguinte comando do PowerShell:

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

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


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

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

a. Reinicie o host.

b. Instale o gMSA em seu host executando o seguinte comando a partir do prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

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

5. Atribua o Privileges administrativo ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no servidor SnapCenter.

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

Instale o plug-in do SnapCenter para Microsoft SQL Server

Adicione hosts e instale o pacote de plug-ins do SnapCenter para Windows

Você deve usar a página SnapCenter **Adicionar host** para adicionar hosts e instalar o pacote de plug-ins. Os plug-ins são instalados automaticamente nos hosts remotos.

O que você vai precisar

- Você deve ser um usuário atribuído a uma função que tenha as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não esteja integrada, desative o UAC no host.
- Você deve garantir que o serviço de enfileiramento de mensagens esteja no estado em execução.
- Se você estiver usando a conta de serviço gerenciado de grupo (gMSA), você deve configurar o gMSA com Privileges administrativo.

  "Configurar conta de serviço gerenciado de grupo no Windows Server 2012 ou posterior para SQL"

Sobre esta tarefa

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

Você pode adicionar um host e instalar os pacotes de plug-in para um host individual ou para um cluster. Se você estiver instalando os plug-ins em um cluster ou no WSFC (Windows Server failover Clustering), os plug-ins serão instalados em todos os nós do cluster.

Para obter informações sobre como gerenciar hosts, "Gerenciar hosts"consulte .

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, faça o seguinte:

Para este campo…	Faça isso…
Tipo de host	Selecione Windows como o tipo de host. O servidor SnapCenter adiciona o host e, em seguida, instala o plug-in para Windows se o plug-in ainda não estiver instalado no host. Se você selecionar a opção Microsoft SQL Server na página Plug-ins, o servidor SnapCenter instala o plug-in para SQL Server.
Nome do host	Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O endereço IP é suportado para hosts de domínio não confiáveis somente se for resolvido para o FQDN. O SnapCenter depende da configuração adequada do DNS. Portanto, a melhor prática é entrar no FQDN. Você pode inserir os endereços IP ou FQDN de um dos seguintes: • Anfitrião independente • WSFC se você estiver adicionando um host usando o SnapCenter e o host fizer parte de um subdomínio, você deverá fornecer o FQDN.

Para este campo…	Faça isso…
Credenciais	Selecione o nome da credencial que você criou ou crie novas credenciais. A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte as informações sobre como criar credenciais. Você pode exibir detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você especificou. O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar host.

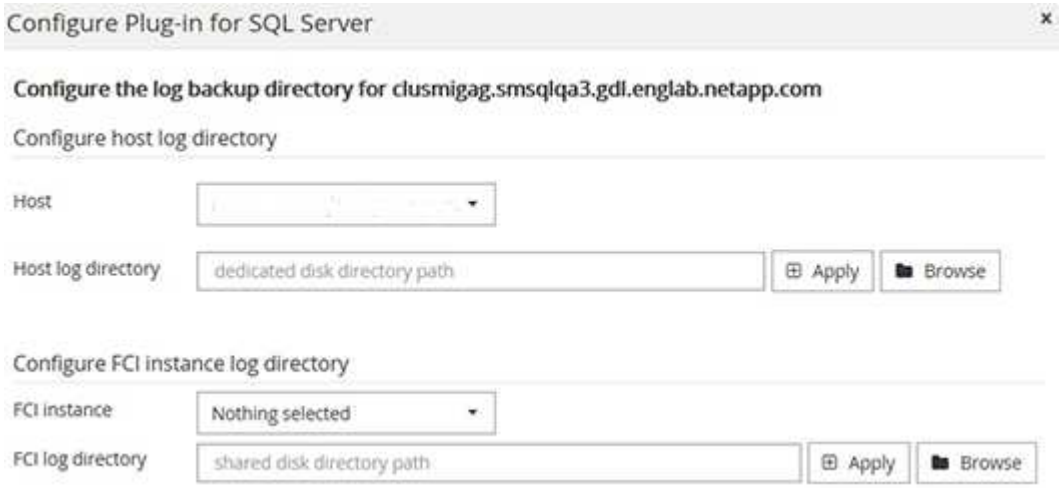
5. Na seção **Select Plug-ins to Install**, selecione os plug-ins a instalar.
6. Clique em **mais opções**.

Para este campo…	Faça isso…
Porta	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. Se você instalou manualmente os plug-ins e especificou uma porta personalizada, você deve especificar a mesma porta. Caso contrário, a operação falha.
Caminho de instalação	O caminho padrão é C: Arquivos de programas / NetApp / SnapCenter. Opcionalmente, você pode personalizar o caminho.
Adicione todos os hosts no cluster	Marque essa caixa de seleção para adicionar todos os nós de cluster em um WSFC ou um SQL Availability Group. Você deve adicionar todos os nós de cluster selecionando a caixa de seleção de cluster apropriada na GUI se quiser gerenciar e identificar vários grupos de disponibilidade SQL disponíveis em um cluster.
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.

Para este campo…	Faça isso…
Use a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in	Marque essa caixa de seleção se quiser usar a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in. Forneça o nome do gMSA no seguinte formato: Se o host for adicionado com gMSA e se o gMSA tiver login e sys admin Privileges, o gMSA será usado para se conetar à instância SQL.

7. Clique em **Enviar**.
8. Para o SQL Plug-in, selecione o host para configurar o diretório de log.
   a. Clique em **Configure log Directory** e, na página Configurar diretório de log do host, clique em **Browse** e execute as seguintes etapas:

      Apenas os LUNs (unidades) NetApp são listados para seleção. O SnapCenter faz o backup e replica o diretório de log do host como parte da operação de backup.



      i. Selecione a letra da unidade ou ponto de montagem no host onde o log do host será armazenado.
      ii. Escolha um subdiretório, se necessário.
      iii. Clique em **Salvar**.
9. Clique em **Enviar**.

Se você não selecionou a caixa de seleção **Ignorar pré-verificações**, o host será validado para verificar se atende aos requisitos para a instalação do plug-in. O espaço em disco, a RAM, a versão do PowerShell, a versão .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.

10. Monitorize o progresso da instalação.

Instale o plug-in do SnapCenter para Microsoft SQL Server em vários hosts remotos usando cmdlets

Você pode instalar o plug-in do SnapCenter para Microsoft SQL Server em vários hosts simultaneamente usando o cmdlet Install-SmHostPackage PowerShell.

O que você vai precisar

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 do SnapCenter para Microsoft SQL Server em vários hosts remotos 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 já 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 do SnapCenter para Microsoft SQL Server silenciosamente a partir da linha de comando

Você deve instalar o plug-in do SnapCenter para Microsoft SQL Server a partir da interface de usuário do SnapCenter. No entanto, se você não puder por algum motivo, você pode executar o Plug-in para o programa de instalação do SQL Server sem supervisão no modo silencioso a partir da linha de comando do Windows.

O que você vai precisar

- Você deve excluir a versão anterior do plug-in do SnapCenter para Microsoft SQL Server antes de instalar.

  Para obter mais informações, "Como instalar um plug-in do SnapCenter manualmente e diretamente do host do plug-in"consulte .

Passos

1. Valide se a pasta C: /Temp existe no host do plug-in e o usuário conetado tem acesso total a ela.

2. Faça o download do plug-in para o software do SQL Server a partir do repositório C:/ProgramData/NetApp/SnapCenter/Package.

   Este caminho é acessível a partir do host onde o servidor SnapCenter está instalado.

3. Copie o arquivo de instalação para o host no qual você deseja instalar o plug-in.
4. Em um prompt de comando do Windows no host local, navegue até o diretório para o qual você salvou os arquivos de instalação do plug-in.
5. Instale o plug-in para o software SQL Server:

   ```
   "snapcenter_windows_host_plugin.exe"/silent /debuglog"Debug_Log_Path"
   /log"Log_Path" BI_SNAPCENTER_PORT=Num
   SUITE_INSTALLDIR="Install_Directory_Path"
   BI_SERVICEACCOUNT=domain\\administrator BI_SERVICEPWD=password
   ISFeatureInstall=SCW,SCSQL
   ```

   Substitua os valores do marcador de posição pelos dados

   - Debug_Log_Path é o nome e a localização do arquivo de log do instalador do pacote.
   - Log_Path é o local dos logs de instalação dos componentes do plug-in (SCW, SCSQL e SMCore).
   - Num é a porta na qual o SnapCenter se comunica com o SMCore
   - Install_Directory_Path é o diretório de instalação do pacote de plug-in do host.
   - Domínio/administrador é a conta do serviço Web do SnapCenter Plug-in para Microsoft Windows.
   - Senha é a senha para a conta de serviço da Web do SnapCenter Plug-in para Microsoft Windows. E `"snapcenter_windows_host_plugin.exe"/silent /debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145 SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter" BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password ISFeatureInstall=SCW,SCSQL`

   Todos os parâmetros passados durante a instalação do Plug-in para SQL Server são sensíveis a maiúsculas e minúsculas.

6. Monitore o agendador de tarefas do Windows, o arquivo de log de instalação principal C: Installdebug.log e os arquivos de instalação adicionais em C: Temp.
7. Monitore o diretório %temp% para verificar se os instaladores do msiexe.exe estão instalando o software sem erros.

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

Monitore o status da instalação do Plug-in para SQL Server

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

Sobre esta tarefa

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

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

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **trabalhos**.
3. Na página trabalhos, para filtrar a lista de modo a que apenas as operações de instalação de plug-in sejam listadas, faça o seguinte:
   a. Clique em **filtro**.
   b. Opcional: Especifique a data de início e fim.
   c. No menu suspenso tipo, selecione **Instalação Plug-in**.
   d. No menu suspenso Status, selecione o status da instalação.
   e. Clique em **aplicar**.
4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página Detalhes da tarefa, clique em **Exibir logs**.

Configurar certificado CA

Gerar arquivo CSR do certificado CA

Você pode gerar uma solicitação de assinatura de certificado (CSR) e importar o certificado que pode ser obtido de uma autoridade de certificação (CA) usando a CSR gerada. O certificado terá uma chave privada associada a ele.

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

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

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

Para configurações de cluster, o nome do cluster (FQDN de cluster virtual) e os respetivos 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 carateres hexadecimais da caixa.

e. Remova os espaços entre os números hexadecimais.

   Por exemplo, se a impressão digital for: "A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 B0 0d 42 77 A3 2a 7b", depois de remover os espaços, será: "A909502d82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:

   a. Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o certificado instalado recentemente pelo nome do assunto.

      Get-ChildItem -Path Cert: LocalMachine/My

   b. Copie a impressão digital.

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

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

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

Passos

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

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

   Por exemplo:

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

   ```
   > $cert = "<certificate thumbprint>"

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
   appid="$guid"
   ```

   Por exemplo:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
   appid="$guid"
   ```

Ative certificados de CA para plug-ins

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

O que você vai precisar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet RUN *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando as *Get-SmCertificateSettings*.

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

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **hosts gerenciados**.
3. Selecione um ou vários hosts de plug-in.
4. Clique em **mais opções**.
5. Selecione **Ativar Validação de certificado**.

Depois de terminar

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

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

> Quando o status é amarelo ou verde, as operações de proteção de dados são concluídas com êxito.

Configurar a recuperação de desastres

Recuperação de desastres do plug-in SnapCenter para SQL Server

Quando o plug-in do SnapCenter estiver inativo, mude para um host SQL diferente e recupere os dados executando algumas etapas.

O que você vai precisar

- O host secundário deve ter o mesmo sistema operacional, aplicativo e nome de host que o host principal.
- Envie o plug-in do SnapCenter para SQL Server para um host alternativo usando a página **Adicionar host** ou **Modificar host**.

"Gerenciar hosts"

Passos

1. Selecione o host na página **hosts** para modificar e instalar o plug-in do SnapCenter para SQL Server.
2. (Opcional) substitua o plug-in do SnapCenter para arquivos de configuração do SQL Server do backup de recuperação de desastres (DR) para a nova máquina.
3. Importe programações do Windows e SQL da pasta do plug-in do SnapCenter para SQL Server do backup de DR.

Para obter mais informações, consulte o "APIs de recuperação de desastres" vídeo.

Recuperação de desastres de storage (DR) para plug-in SnapCenter para SQL Server

Você pode recuperar o plug-in do SnapCenter para armazenamento do SQL Server habilitando o modo DR para armazenamento na página Configurações globais.

O que você vai precisar

- Certifique-se de que os plug-ins estão no modo de manutenção.
- Quebre a relação SnapMirror/SnapVault. "Quebrando relacionamentos SnapMirror"
- Conete o LUN do secundário à máquina host com a mesma letra de unidade.
- Certifique-se de que todos os discos estejam conetados usando as mesmas letras de unidade usadas antes do DR.
- Reinicie o serviço de servidor MSSQL.
- Certifique-se de que os recursos SQL estão novamente online.

Sobre esta tarefa

A recuperação de desastres (DR) não é compatível com configurações VMDK e RDM.

Passos

1. Na página Configurações, navegue até **Configurações** > **Configurações globais** > **recuperação de desastres**.
2. Selecione **Ativar recuperação de desastres**.
3. Clique em **aplicar**.
4. Verifique se a tarefa DR está ativada ou não clicando em **Monitor** > **jobs**.

Depois de terminar

- Se novos bancos de dados forem criados após o failover, os bancos de dados estarão no modo não DR.

  Os novos bancos de dados continuarão operando como antes do failover.

- Os novos backups criados no modo DR serão listados em SnapMirror ou SnapVault (secundário) na página topologia.

Um ícone "i" é exibido ao lado dos novos backups para indicar que esses backups foram criados durante o modo DR.

- Você pode excluir o plug-in do SnapCenter para backups do SQL Server criados durante o failover usando a IU ou o cmdlet a seguir: `Remove-SmBackup`
- Após o failover, se você quiser que alguns dos recursos estejam em modo não DR, use o seguinte cmdlet: `Remove-SmResourceDRMode`

  Para obter mais informações, consulte "Guia de referência de cmdlet do software SnapCenter".

- O servidor SnapCenter gerenciará os recursos de storage individuais (bancos de dados SQL) que estão no modo DR ou não DR, mas não o grupo de recursos com recursos de storage que estão no modo DR ou no modo não DR.

Failback do plug-in do SnapCenter para storage secundário do SQL Server para storage primário

Depois que o plug-in do SnapCenter para o armazenamento primário do SQL Server estiver novamente on-line, você deve fazer o failback para o storage primário.

O que você vai precisar

- Coloque o plug-in do SnapCenter para SQL Server no modo **Manutenção** na página hosts gerenciados.
- Desconete o storage secundário do host e conete-se ao storage primário.
- Para fazer o failback para o storage primário, verifique se a direção da relação permanece a mesma antes do failover executando a operação de ressincronização reversa.

  Para manter as funções de armazenamento primário e secundário após a operação de ressincronização reversa, execute novamente a operação de ressincronização reversa.

  Para obter mais informações, consulte "Reverter a ressincronização das relações de espelho"

- Reinicie o serviço de servidor MSSQL.
- Certifique-se de que os recursos SQL estão novamente online.

> Durante o failover ou failback do plug-in, o status geral do plug-in não é atualizado imediatamente. O status geral do host e do plug-in é atualizado durante a operação de atualização subsequente do host.

Passos

1. Na página Configurações, navegue até **Configurações** > **Configurações globais** > **recuperação de desastres**.
2. Desmarque **Ativar recuperação de desastres**.
3. Clique em **aplicar**.
4. Verifique se a tarefa DR está ativada ou não clicando em **Monitor** > **jobs**.

Depois de terminar

- Você pode excluir o plug-in do SnapCenter para backups do SQL Server criados durante o failover usando

a IU ou o cmdlet a seguir: `Remove-SmDRFailoverBackups`

Informações sobre direitos autorais

Informações sobre marcas comerciais