Bereiten Sie die Installation des SnapCenter-Plug-ins für Microsoft SQL Server vor

SnapCenter Software 4.7

NetApp
January 18, 2024

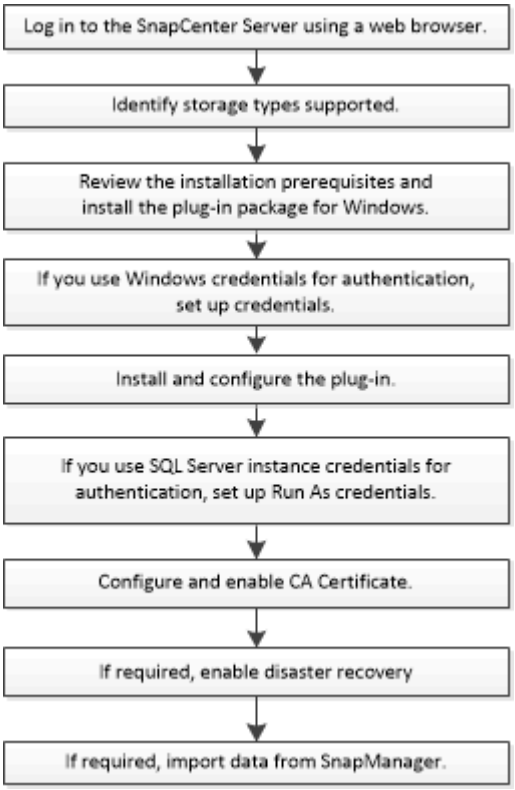
Inhalt

Bereiten Sie die Installation des SnapCenter-Plug-ins für Microsoft SQL Server vor . . . 1
Installations-Workflow für das SnapCenter Plug-in für Microsoft SQL Server . . . 1
Voraussetzungen für das Hinzufügen von Hosts und die Installation des SnapCenter-Plug-ins für Microsoft SQL Server . . . 1
Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows . . . 2
Richten Sie die Anmeldeinformationen für das SnapCenter-Plug-ins-Paket für Windows ein . . . 3
Konfigurieren von Anmeldeinformationen für eine einzelne SQL Server-Ressource . . . 5
Konfigurieren Sie gMSA unter Windows Server 2012 oder höher . . . 7
Installieren Sie das SnapCenter Plug-in für Microsoft SQL Server . . . 8
Konfigurieren Sie das CA-Zertifikat . . . 15
Konfiguration der Disaster Recovery . . . 18

Bereiten Sie die Installation des SnapCenter-Plug-ins für Microsoft SQL Server vor

Installations-Workflow für das SnapCenter Plug-in für Microsoft SQL Server

Sie sollten das SnapCenter Plug-in für Microsoft SQL Server installieren und einrichten, wenn Sie SQL Server-Datenbanken schützen möchten.



Voraussetzungen für das Hinzufügen von Hosts und die Installation des SnapCenter-Plug-ins für Microsoft SQL Server

Bevor Sie einen Host hinzufügen und die Plug-ins-Pakete installieren, müssen Sie alle Anforderungen erfüllen.

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie müssen über einen Benutzer mit lokalen Administratorrechten mit lokalen Anmeldeberechtigungen auf dem Remote-Host verfügen.
- Wenn Sie Cluster-Nodes in SnapCenter verwalten, müssen Sie einen Benutzer mit Administratorrechten für alle Nodes im Cluster besitzen.
- Sie müssen über einen Benutzer mit sysadmin-Berechtigungen auf dem SQL Server verfügen.

  Das SnapCenter Plug-in für Microsoft SQL Server verwendet Microsoft VDI Framework, für das ein

sysadmin-Zugriff erforderlich ist.

"Microsoft Support-Artikel 2926557: Für Backup- und Restore-Vorgänge für SQL Server VDI sind Sysadmin-Berechtigungen erforderlich"

- Wenn Sie ein Plug-in auf einem Windows-Host installieren, müssen Sie UAC auf dem Host deaktivieren, wenn Sie keine Anmeldedaten angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Workgroup-Benutzer gehört.
- Wenn SnapManager für Microsoft SQL Server installiert ist, müssen Sie den Service und die Zeitpläne angehalten oder deaktiviert haben.
- Der Host muss auf den vollständig qualifizierten Domänennamen (FQDN) vom Server resolable sein.

  Wenn die Host-Datei geändert wird, damit sie resolable ist, und wenn sowohl der Kurzname als auch der FQDN in der Datei Hosts angegeben sind, erstellen Sie einen Eintrag in der Datei SnapCenter Hosts im folgenden Format: <ip_Address> <Host_fqdn> <Host_Name>

Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows

Bevor Sie das SnapCenter Plug-ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatzanforderungen und Größenanforderungen für das Host-System vertraut sein.

Element	Anforderungen
Betriebssysteme	Microsoft Windows Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1 GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	5 GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.

Element	Anforderungen
Erforderliche Softwarepakete	• Microsoft .NET Framework 4.7.2 oder höher • Windows Management Framework (WMF) 4.0 oder höher • PowerShell 4.0 oder höher Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool". Informationen zur Fehlerbehebung bei .NET finden Sie unter "SnapCenter-Upgrade oder -Installation schlägt bei Legacy-Systemen ohne Internetverbindung fehl".

Richten Sie die Anmeldeinformationen für das SnapCenter-Plug-ins-Paket für Windows ein

SnapCenter verwendet Zugangsdaten, um Benutzer für SnapCenter-Vorgänge zu authentifizieren. Sie sollten Anmeldedaten für die Installation von SnapCenter-Plug-ins und zusätzliche Anmeldedaten für die Durchführung von Datenschutzvorgängen in Datenbanken oder Windows-Dateisystemen erstellen.

Was Sie brauchen

- Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-ins installieren.
- Sie müssen die Anmeldedaten mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.
- SQL-Authentifizierung auf Windows Hosts

  Nach der Installation von Plug-ins müssen Sie SQL-Anmeldedaten einrichten.

  Wenn Sie SnapCenter-Plug-in für Microsoft SQL Server bereitstellen, müssen Sie nach der Installation von Plug-ins SQL-Anmeldedaten einrichten. Richten Sie eine Anmeldedaten für einen Benutzer mit den sysadmin-Berechtigungen von SQL Server ein.

  Die SQL-Authentifizierungsmethode authentifiziert sich anhand einer SQL Server-Instanz. Das bedeutet, dass eine SQL Server-Instanz in SnapCenter erkannt werden muss. Daher müssen Sie vor dem Hinzufügen von SQL-Anmeldeinformationen einen Host hinzufügen, Plug-in-Pakete installieren und Ressourcen aktualisieren. Sie benötigen die SQL Server-Authentifizierung für Vorgänge wie Planung oder Ermittlung von Ressourcen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Credential**.
3. Klicken Sie Auf **Neu**.
4. Geben Sie auf der Seite Credential die Informationen an, die zum Konfigurieren von Anmeldeinformationen

erforderlich sind:

Für dieses Feld…	Tun Sie das…
Name der Anmeldeinformationen	Geben Sie einen Namen für die Anmeldedaten ein.
Benutzername/Passwort	Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen. • Domain-Administrator Geben Sie den Domänenadministrator auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie bei Systemen, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorengruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerungsfunktion auf dem Hostsystem deaktiviert ist. Das zulässige Format für das Feld Benutzername lautet: `UserName` Verwenden Sie keine Doppelzitate (") oder Rückkreuzzeichen (`) in den Kennwörtern. Sie sollten nicht das weniger als (<) und Ausrufezeichen (!) verwenden. Symbole in Kennwörtern. Zum Beispiel lessthan<!10, lessthan10<!, backtick`12.
Authentifizierungsmodus	Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten. Wenn Sie den SQL-Authentifizierungsmodus auswählen, müssen Sie auch die SQL-Serverinstanz und den Host angeben, auf dem sich die SQL-Instanz befindet.

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie einem Benutzer oder einer Gruppe von Benutzern auf der Seite Benutzer und Zugriff die Wartung der Anmeldeinformationen zuweisen.

Konfigurieren von Anmeldeinformationen für eine einzelne SQL Server-Ressource

Sie können Anmeldedaten für die Durchführung von Datensicherungsjobs für einzelne SQL Server-Ressourcen für jeden Benutzer konfigurieren. Sie können die Anmeldeinformationen zwar global konfigurieren, aber dies ist möglicherweise nur für eine bestimmte Ressource erforderlich.

Über diese Aufgabe

- Wenn Sie Windows-Anmeldeinformationen zur Authentifizierung verwenden, müssen Sie vor der Installation von Plug-ins die Anmeldedaten einrichten.

  Wenn Sie jedoch eine SQL Server-Instanz zur Authentifizierung verwenden, müssen Sie nach der Installation von Plug-ins die Anmeldeinformationen hinzufügen.

- Wenn Sie die SQL-Authentifizierung beim Einrichten der Anmeldeinformationen aktiviert haben, wird die erkannte Instanz oder Datenbank mit einem roten Farbvorhängeschloss-Symbol angezeigt.

  Wenn das Vorhängeschloss-Symbol angezeigt wird, müssen Sie die Instanz oder die Datenbankanmeldeinformationen angeben, um die Instanz oder Datenbank einer Ressourcengruppe erfolgreich hinzuzufügen.

- Sie müssen die Anmeldedaten einem Benutzer mit rollenbasierter Zugriffssteuerung (Role-Based Access Control, RBAC) ohne sysadmin-Zugriff zuweisen, wenn die folgenden Bedingungen erfüllt sind:
  - Die Anmeldeinformationen werden einer SQL-Instanz zugewiesen.
  - Die SQL Instanz oder der Host wird einem RBAC-Benutzer zugewiesen.

    Der Benutzer muss sowohl über die Ressourcengruppe als auch über die Sicherungsrechte verfügen

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Credential**.
3. Klicken Sie zum Hinzufügen einer neuen Anmeldedaten auf **Neu**.
4. Konfigurieren Sie auf der Seite Anmeldeinformationen:

Für dieses Feld…	Tun Sie das…
Anmeldeinformationsname	Geben Sie einen Namen für die Anmeldedaten ein.

Für dieses Feld…	Tun Sie das…
Benutzername	Geben Sie den Benutzernamen ein, der für die SQL Server-Authentifizierung verwendet wird. • Domänenadministrator oder ein Mitglied der Administratorgruppe Geben Sie den Domänenadministrator oder ein Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld **Benutzername** sind: ◦ *NetBIOS\Benutzername* ◦ *Domain FQDN\Benutzername* • Lokaler Administrator (nur für Arbeitsgruppen) für Systeme, die zu einer Arbeitsgruppe gehören, geben Sie den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorengruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerungsfunktion auf dem Hostsystem deaktiviert ist. Das zulässige Format für das Feld **Benutzername** lautet: *Username*
Passwort	Geben Sie das für die Authentifizierung verwendete Passwort ein.
Authentifizierungsmodus	Wählen Sie den SQL Server-Authentifizierungsmodus aus. Sie können auch die Windows-Authentifizierung auswählen, wenn der Windows-Benutzer sysadmin-Berechtigungen auf dem SQL-Server hat.
Gastgeber	Wählen Sie den Host aus.
SQL Server-Instanz	Wählen Sie die SQL Server-Instanz aus.

5. Klicken Sie auf **OK**, um die Anmeldedaten hinzuzufügen.
6. Klicken Sie im linken Navigationsbereich auf **Ressourcen**.
7. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Instanz** aus.
   a. Klicken Sie Auf Und wählen Sie dann den Hostnamen aus, um die Instanzen zu filtern.
   b. Klicken Sie Auf Um den Filterbereich zu schließen.
8. Schützen Sie die Instanz auf der Seite Schützen, und klicken Sie bei Bedarf auf **Anmeldeinformationen konfigurieren**.

Wenn der beim SnapCenter-Server angemeldete Benutzer keinen Zugriff auf das SnapCenter-Plugin für Microsoft SQL-Server hat, muss der Benutzer die Anmeldeinformationen konfigurieren.

> Die Anmeldeinformationsoption gilt nicht für Datenbanken und Verfügbarkeitsgruppen.

9. Klicken Sie Auf **Ressourcen Aktualisieren**.

Konfigurieren Sie gMSA unter Windows Server 2012 oder höher

Mit Windows Server 2012 oder höher können Sie ein Group Managed Service Account (gMSA) erstellen, das über ein verwaltetes Domain-Konto eine automatisierte Verwaltung von Service-Konten ermöglicht.

Was Sie brauchen

- Sie sollten einen Windows Server 2012 oder höher Domänencontroller haben.
- Sie sollten einen Windows Server 2012 oder höher-Host haben, der Mitglied der Domain ist.

Schritte

1. Erstellen Sie einen KDS-Stammschlüssel, um eindeutige Passwörter für jedes Objekt in Ihrem gMSA zu generieren.
2. Führen Sie für jede Domäne den folgenden Befehl vom Windows Domain Controller aus: Add-KDSRootKey -EffectiveImmediately
3. Erstellen und Konfigurieren des gMSA:
   a. Erstellen Sie ein Benutzerkonto in folgendem Format:

   ```
    domainName\accountName$
   .. Fügen Sie der Gruppe Computerobjekte hinzu.
   .. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu
   erstellen.
   ```

   Beispiel:

   ```
    New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
   -PrincipalsAllowedToRetrieveManagedPassword <group>
   -ServicePrincipalNames <SPN1,SPN2,…>
   .. Laufen `Get-ADServiceAccount` Befehl zum Überprüfen des
   Dienstkontos.
   ```

4. Konfigurieren Sie das gMSA auf Ihren Hosts:
   a. Aktivieren Sie das Active Directory-Modul für Windows PowerShell auf dem Host, auf dem Sie das gMSA-Konto verwenden möchten.

   Um dies zu tun, führen Sie den folgenden Befehl aus 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. Starten Sie den Host neu.

b. Installieren Sie das gMSA auf Ihrem Host, indem Sie den folgenden Befehl über die PowerShell-Eingabeaufforderung ausführen: `Install-AdServiceAccount <gMSA>`

c. Überprüfen Sie Ihr gMSA-Konto, indem Sie folgenden Befehl ausführen: `Test-AdServiceAccount <gMSA>`

5. Weisen Sie dem konfigurierten gMSA auf dem Host die Administratorrechte zu.
6. Fügen Sie den Windows-Host hinzu, indem Sie das konfigurierte gMSA-Konto im SnapCenter-Server angeben.

   SnapCenter-Server installiert die ausgewählten Plug-ins auf dem Host, und das angegebene gMSA wird während der Plug-in-Installation als Service-Login-Konto verwendet.

Installieren Sie das SnapCenter Plug-in für Microsoft SQL Server

Fügen Sie Hosts hinzu, und installieren Sie das SnapCenter-Plug-ins-Paket für Windows

Sie müssen die Seite SnapCenter **Add Host** verwenden, um Hosts hinzuzufügen und das Plug-ins-Paket zu installieren. Die Plug-ins werden automatisch auf den Remote-Hosts installiert.

Was Sie brauchen

- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen für die Plug-in-Installation und -Deinstallation verfügt, wie z. B. die Rolle „SnapCenter-Administrator“.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, sollten Sie UAC auf dem Host deaktivieren, wenn Sie keine integrierten Anmeldeinformationen angeben.

- Stellen Sie sicher, dass der Nachrichtenwarteschlange in Betrieb ist.
- Wenn Sie Group Managed Service Account (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

  "Konfigurieren Sie das Gruppenkonto für Managed Services unter Windows Server 2012 oder höher für SQL"

Über diese Aufgabe

Sie können einen SnapCenter-Server nicht als Plug-in-Host zu einem anderen SnapCenter-Server hinzufügen.

Sie können einen Host hinzufügen und die Plug-in-Pakete entweder für einen einzelnen Host oder für einen Cluster installieren. Wenn Sie die Plug-ins auf einem Cluster oder Windows Server Failover Clustering (WSFC) installieren, werden die Plug-ins auf allen Knoten des Clusters installiert.

Informationen zum Verwalten von Hosts finden Sie unter "Management von Hosts".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Überprüfen Sie, ob die Registerkarte **verwaltete Hosts** oben ausgewählt ist.
3. Klicken Sie Auf **Hinzufügen**.
4. Gehen Sie auf der Seite Hosts wie folgt vor:

Für dieses Feld…	Tun Sie das…
Host-Typ	Wählen Sie Windows als Hosttyp aus. Der SnapCenter-Server fügt den Host hinzu und installiert dann das Plug-in für Windows, wenn das Plug-in nicht bereits auf dem Host installiert ist. Wenn Sie auf der Seite Plug-ins die Option Microsoft SQL Server auswählen, installiert der SnapCenter-Server das Plug-in für SQL Server.

Für dieses Feld…	Tun Sie das…
Host-Name	Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. Die IP-Adresse wird nur für nicht vertrauenswürdige Domänenhosts unterstützt, wenn sie auf den FQDN auflöst. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den FQDN einzugeben. Sie können die IP-Adressen oder FQDN einer der folgenden Adressen eingeben: • Eigenständiger Host • WSFC Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Subdomain ist, müssen Sie den FQDN angeben.
Anmeldedaten	Wählen Sie den Anmeldeinformationsnamen aus, den Sie erstellt haben oder neue Anmeldeinformationen erstellen. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Weitere Informationen finden Sie unter Informationen zum Erstellen von Anmeldeinformationen. Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen positionieren. Der Authentifizierungsmodus für die Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten zum Hinzufügen von Hosts angeben.

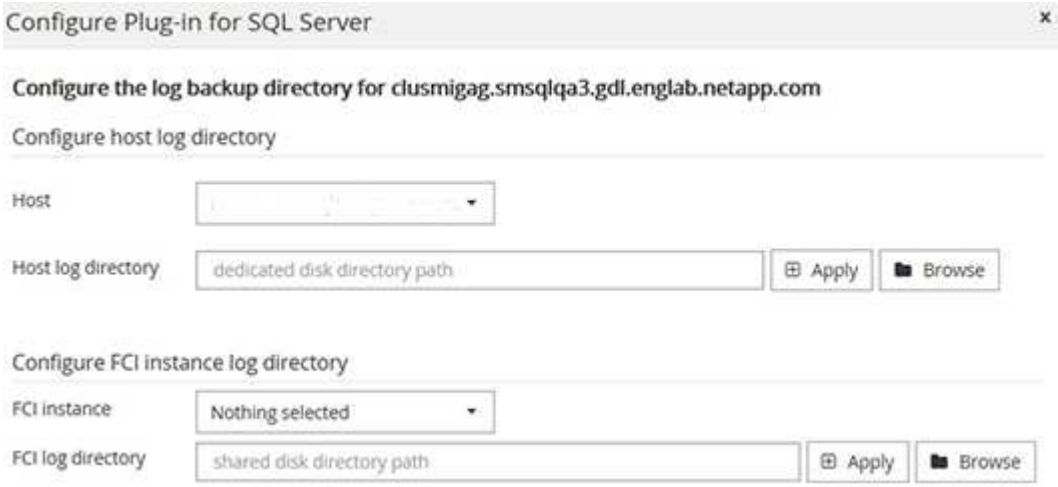
5. Wählen Sie im Abschnitt **Plug-ins zur Installation auswählen** die zu installierenden Plug-ins aus.
6. Klicken Sie Auf **Weitere Optionen**.

Für dieses Feld…	Tun Sie das…
Port	Behalten Sie die Standard-Port-Nummer bei oder geben Sie die Port-Nummer an. Die Standardanschlussnummer ist 8145. Wenn der SnapCenter-Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt. Wenn Sie die Plug-ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.
Installationspfad	Der Standardpfad ist C:\Programmdateien\NetApp\SnapCenter. Optional können Sie den Pfad anpassen.
Fügen Sie alle Hosts im Cluster hinzu	Aktivieren Sie dieses Kontrollkästchen, um alle Clusterknoten in einer WSFC- oder SQL-Verfügbarkeitsgruppe hinzuzufügen. Sie sollten alle Cluster-Knoten hinzufügen, indem Sie das entsprechende Kontrollkästchen Cluster in der GUI aktivieren, wenn Sie mehrere verfügbare SQL-Verfügbarkeitsgruppen in einem Cluster verwalten und identifizieren möchten.
Überspringen Sie die Prüfungen vor der Installation	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.
Verwenden Sie Group Managed Service Account (gMSA), um die Plug-in-Dienste auszuführen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-in-Dienste über das Group Managed Service Account (gMSA) ausführen möchten. Geben Sie den gMSA-Namen in folgendem Format an: Domainname\AccountName€. Wenn der Host mit gMSA hinzugefügt wird und der gMSA über Login- und sys Admin-Berechtigungen verfügt, wird das gMSA verwendet, um eine Verbindung zur SQL-Instanz herzustellen.

7. Klicken Sie Auf **Absenden**.

8. Wählen Sie für das SQL-Plug-in den Host aus, um das Protokollverzeichnis zu konfigurieren.
   a. Klicken Sie auf **Logverzeichnis konfigurieren** und klicken Sie auf der Seite Hostprotokollverzeichnis konfigurieren auf **Durchsuchen** und führen Sie die folgenden Schritte aus:

      Nur NetApp LUNs (Laufwerke) werden zur Auswahl aufgeführt. SnapCenter sichert und repliziert im Rahmen des Backup-Vorgangs das Host-Protokollverzeichnis.



      i. Wählen Sie den Laufwerksbuchstaben oder den Bereitstellungspunkt auf dem Host aus, auf dem das Hostprotokoll gespeichert werden soll.
      ii. Wählen Sie ggf. ein Unterverzeichnis aus.
      iii. Klicken Sie Auf **Speichern**.
9. Klicken Sie Auf **Absenden**.

   Wenn Sie das Kontrollkästchen **Vorabprüfungen** nicht aktiviert haben, wird der Host validiert, um zu überprüfen, ob er die Anforderungen für die Installation des Plug-ins erfüllt. Der Festplattenspeicher, der RAM, die PowerShell-Version, die .NET-Version, der Speicherort (für Windows-Plug-ins) und die Java-Version (für Linux-Plug-ins) werden anhand der Mindestanforderungen validiert. Wenn die Mindestanforderungen nicht erfüllt werden, werden entsprechende Fehler- oder Warnmeldungen angezeigt.

   Wenn der Fehler mit dem Festplattenspeicher oder RAM zusammenhängt, können Sie die Datei Web.config unter C:\Programme\NetApp\SnapCenter WebApp aktualisieren, um die Standardwerte zu ändern. Wenn der Fehler mit anderen Parametern zusammenhängt, müssen Sie das Problem beheben.

   > Wenn Sie in einem HA-Setup die Datei „Web.config“ aktualisieren, müssen Sie die Datei auf beiden Knoten aktualisieren.

10. Überwachen Sie den Installationsfortschritt.

Installieren Sie das SnapCenter Plug-in für Microsoft SQL Server mithilfe von Cmdlets auf mehreren Remote Hosts

Sie können das SnapCenter-Plug-in für Microsoft SQL Server auf mehreren Hosts gleichzeitig installieren, indem Sie das Cmdlet "Install-SmHostPackage PowerShell" verwenden.

Was Sie brauchen

Sie müssen sich bei SnapCenter als Domänenbenutzer mit lokalen Administratorrechten auf jedem Host, auf dem Sie das Plug-in-Paket installieren möchten, angemeldet haben.

Schritte

1. Starten Sie PowerShell.
2. Erstellen Sie auf dem SnapCenter-Server-Host eine Sitzung mit dem Cmdlet "Open-SmConnection" und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das SnapCenter-Plug-in für Microsoft SQL Server auf mehreren Remote-Hosts mit dem Cmdlet "Install-SmHostPackage" und den erforderlichen Parametern.

   Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch".

   Sie können die Option -skipprecheck verwenden, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.

4. Geben Sie Ihre Anmeldeinformationen für die Remote-Installation ein.

Installieren Sie das SnapCenter-Plug-in für Microsoft SQL Server im Hintergrund über die Befehlszeile

Sie sollten das SnapCenter Plug-in für Microsoft SQL Server über die Benutzeroberfläche von SnapCenter installieren. Wenn Sie jedoch aus irgendeinem Grund nicht in der Lage sind, das Installationsprogramm Plug-in für SQL Server unbeaufsichtigt im Silent-Modus von der Windows-Befehlszeile aus auszuführen.

Was Sie brauchen

- Vor der Installation müssen Sie die frühere Version des SnapCenter-Plug-ins für Microsoft SQL Server löschen.

  Weitere Informationen finden Sie unter "So installieren Sie ein SnapCenter-Plug-in manuell und direkt über den Plug-in-Host".

Schritte

1. Überprüfen Sie, ob der Ordner C:\temp auf dem Plug-in-Host vorhanden ist und der angemeldete Benutzer vollen Zugriff darauf hat.
2. Laden Sie das Plug-in für SQL Server unter C:\ProgramData\NetApp\SnapCenter\Package Repository herunter.

   Auf diesen Pfad kann von dem Host zugegriffen werden, auf dem der SnapCenter-Server installiert ist.

3. Kopieren Sie die Installationsdatei auf den Host, auf dem Sie das Plug-in installieren möchten.
4. Navigieren Sie von einer Windows-Eingabeaufforderung auf dem lokalen Host zum Verzeichnis, in das Sie die Plug-in-Installationsdateien gespeichert haben.
5. Installieren Sie das Plug-in für 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
```

Ersetzen Sie die Platzhalterwerte durch Ihre Daten

- Debug_Log_Path ist der Name und der Speicherort der Protokolldatei für das Installationsprogramm der Suite.
- Log_Path ist der Speicherort der Installationsprotokolle der Plug-in-Komponenten (SCW, SCSCSQL und SMCore).
- Num ist der Port, an dem SnapCenter mit SMCore kommuniziert
- Install_Directory_Path ist das Installationsverzeichnis des Host-Plug-in-Pakets.
- Domain\Administrator ist das SnapCenter-Plug-in für Microsoft Windows-Webservice-Konto.
- Passwort ist das Passwort für das SnapCenter-Plug-in für Microsoft Windows Webservice-Konto.
  ```
  "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
  ```

  Bei der Installation von Plug-in für SQL Server müssen alle Parameter beachtet werden.

6. Überwachen Sie den Windows Task Scheduler, die Hauptinstallationsprotokolldatei C:\Installdebug.log und die zusätzlichen Installationsdateien in C:\Temp.
7. Überwachen Sie das Verzeichnis %temp%, um zu überprüfen, ob die msiexe.exe Installationsprogramme fehlerfrei installiert werden.

Die Installation des Plug-ins für SQL Server registriert das Plug-in auf dem Host und nicht auf dem SnapCenter-Server. Sie können das Plug-in auf dem SnapCenter Server registrieren, indem Sie den Host mithilfe der SnapCenter GUI oder PowerShell Cmdlet hinzufügen. Nach dem Hinzufügen des Hosts wird das Plug-in automatisch erkannt.

Überwachen Sie den Status der Installation des Plug-ins für SQL Server

Sie können den Fortschritt der Installation des SnapCenter-Plug-in-Pakets über die Seite Jobs überwachen. Möglicherweise möchten Sie den Installationsfortschritt prüfen, um festzustellen, wann die Installation abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
-

Abgeschlossen mit Warnungen oder konnte aufgrund von Warnungen nicht gestartet werden

- Warteschlange

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite Überwachen auf **Jobs**.
3. Gehen Sie auf der Seite Jobs folgendermaßen vor, um die Liste so zu filtern, dass nur Plug-in-Installationsvorgänge aufgeführt werden:
   a. Klicken Sie Auf **Filter**.
   b. Optional: Geben Sie das Start- und Enddatum an.
   c. Wählen Sie im Dropdown-Menü Typ die Option **Plug-in Installation**.
   d. Wählen Sie im Dropdown-Menü Status den Installationsstatus aus.
   e. Klicken Sie Auf **Anwenden**.
4. Wählen Sie den Installationsauftrag aus und klicken Sie auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite Jobdetails auf **Protokolle anzeigen**.

Konfigurieren Sie das CA-Zertifikat

ZertifikatCSR-Datei erstellen

Sie können eine Zertifikatsignierungsanforderung (CSR) generieren und das Zertifikat importieren, das von einer Zertifizierungsstelle (CA) mit dem generierten CSR abgerufen werden kann. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block von codiertem Text, der einem autorisierten Zertifikatanbieter zur Beschaffung des signierten CA-Zertifikats übergeben wird.

Informationen zum Generieren einer CSR finden Sie unter "So generieren Sie eine CSR-Datei für das CA-Zertifikat".

> Wenn Sie das CA-Zertifikat für Ihre Domain (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie die Erstellung der CA-Zertifikat-CSR-Datei überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die entsprechenden Hostnamen im CA-Zertifikat aufgeführt werden. Das Zertifikat kann aktualisiert werden, indem Sie das Feld Alternative Name (SAN) des Studienteilnehmers ausfüllen, bevor Sie das Zertifikat beschaffen. Bei einem Platzhalter-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

Importieren von CA-Zertifikaten

Sie müssen die CA-Zertifikate mithilfe der Microsoft-Verwaltungskonsole (MMC) auf den SnapCenter-Server und die Windows-Host-Plug-ins importieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin**

hinzufügen/entfernen.

2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Importassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie dann auf **Weiter**.
Dateiformat Importieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

> Der Import des Zertifikats sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: *.pfx, *.p12 und *.p7b).

7. Wiederholen Sie Schritt 5 für den Ordner „persönlich“.

Abrufen des Daumenabdrucks für das CA-Zertifikat

Ein ZertifikatDaumendruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Ein Daumendruck wird aus dem Inhalt des Zertifikats mithilfe eines Daumendruckalgorithmus berechnet.

Schritte

1. Führen Sie auf der GUI folgende Schritte durch:
   a. Doppelklicken Sie auf das Zertifikat.
   b. Klicken Sie im Dialogfeld Zertifikat auf die Registerkarte **Details**.
   c. Blättern Sie durch die Liste der Felder und klicken Sie auf **Miniaturdruck**.
   d. Kopieren Sie die hexadezimalen Zeichen aus dem Feld.
   e. Entfernen Sie die Leerzeichen zwischen den hexadezimalen Zahlen.

   Wenn der Daumendruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3

2a 7b“, wird nach dem Entfernen der Leerzeichen der Text „a909502dd82ae41433e6f83886b00d4277a32a7b“ lauten.

2. Führen Sie Folgendes aus PowerShell aus:
   a. Führen Sie den folgenden Befehl aus, um den Daumendruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreff-Namens zu identifizieren.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Kopieren Sie den Daumendruck.

Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-in-Diensten

Sie sollten das CA-Zertifikat mit den Windows-Host-Plug-in-Diensten konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Führen Sie die folgenden Schritte auf dem SnapCenter-Server und allen Plug-in-Hosts durch, auf denen CA-Zertifikate bereits bereitgestellt wurden.

Schritte

1. Entfernen Sie die vorhandene Zertifikatbindung mit SMCore-Standardport 8145, indem Sie den folgenden Befehl ausführen:

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

   Beispiel:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Binden Sie das neu installierte Zertifikat an die Windows Host Plug-in-Dienste, indem Sie die folgenden Befehle ausführen:
   ```

   ```
   > $cert = “<certificate thumbprint>”

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

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

   Beispiel:

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

Aktivieren Sie CA-Zertifikate für Plug-ins

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikate im SnapCenter-Server und den entsprechenden Plug-in-Hosts bereitstellen. Sie sollten die CA-Zertifikatsvalidierung für die Plug-ins aktivieren.

Was Sie brauchen

- Sie können die CA-Zertifikate mit dem Cmdlet "Run_set-SmCertificateSettings_" aktivieren oder deaktivieren.
- Sie können den Zertifikatsstatus für die Plug-ins mithilfe der *get-SmCertificateSettings* anzeigen.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **verwaltete Hosts**.
3. Wählen Sie ein- oder mehrere Plug-in-Hosts aus.
4. Klicken Sie auf **Weitere Optionen**.
5. Wählen Sie **Zertifikatvalidierung Aktivieren**.

Nach Ihrer Beendigung

Auf dem Reiter Managed Hosts wird ein Schloss angezeigt, und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- Zeigt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-in-Host zugewiesen ist.
- Zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- Zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- Zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

> Wenn der Status gelb oder grün lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Konfiguration der Disaster Recovery

Disaster Recovery eines SnapCenter Plug-ins für SQL Server

Wenn das SnapCenter-Plug-in für SQL Server ausfällt, wechseln Sie zu einem anderen SQL-Host und stellen Sie die Daten mit wenigen Schritten wieder her.

Was Sie brauchen

- Der sekundäre Host sollte das gleiche Betriebssystem, die gleiche Anwendung und den gleichen Hostnamen wie der primäre Host haben.
- Schieben Sie das SnapCenter-Plug-in für SQL Server auf einen anderen Host, indem Sie die Seite **Add Host** oder **Modify Host** verwenden.

"Management von Hosts"

Schritte

1. Wählen Sie den Host auf der Seite **Hosts** aus, um das SnapCenter-Plug-in für SQL Server zu ändern und zu installieren.
2. (Optional) Ersetzen Sie das SnapCenter-Plug-in für SQL Server-Konfigurationsdateien vom Disaster Recovery-Backup (DR) auf die neue Maschine.
3. Importieren Sie Windows- und SQL-Zeitpläne aus dem SnapCenter-Plug-in für SQL Server-Ordner aus dem DR-Backup.

Weitere Informationen finden Sie im "Disaster Recovery-APIs" Video:

Storage Disaster Recovery (DR) für SnapCenter Plug-in für SQL Server

Sie können das SnapCenter Plug-in für SQL Server Storage wiederherstellen, indem Sie den DR-Modus für Storage auf der Seite Globale Einstellungen aktivieren.

Was Sie brauchen

- Stellen Sie sicher, dass sich die Plug-ins im Wartungsmodus befinden.
- SnapMirror/SnapVault Beziehung aufheben"SnapMirror Beziehungen unterbrechen"
- Verbinden Sie die LUN aus dem sekundären Server mit dem gleichen Laufwerksbuchstaben.
- Stellen Sie sicher, dass alle Laufwerke mit denselben Laufwerksbuchstaben verbunden sind, die vor der DR verwendet wurden.
- MSSQL-Serverdienst neu starten.
- Stellen Sie sicher, dass die SQL-Ressourcen wieder online sind.

Über diese Aufgabe

Disaster Recovery (DR) wird auf VMDK- und RDM-Konfigurationen nicht unterstützt.

Schritte

1. Navigieren Sie auf der Seite Einstellungen zu **Einstellungen** > **Globale Einstellungen** > **Disaster Recovery**.
2. Wählen Sie **Disaster Recovery Aktivieren**.
3. Klicken Sie Auf **Anwenden**.
4. Überprüfen Sie, ob der DR-Job aktiviert ist oder nicht, indem Sie auf **Monitor** > **Jobs** klicken.

Nach Ihrer Beendigung

- Falls neue Datenbanken nach dem Failover erstellt werden, befinden sich die Datenbanken außerhalb des DR-Modus.

  Die neuen Datenbanken laufen weiterhin so wie vor dem Failover.

- Die neuen Backups, die im DR-Modus erstellt wurden, werden auf der Topologieseite unter SnapMirror oder SnapVault (sekundär) aufgeführt.

Neben den neuen Backups wird ein „i“-Symbol angezeigt, das angibt, dass diese Backups während des DR-Modus erstellt wurden.

- Sie können das SnapCenter-Plug-in für SQL Server Backups löschen, die während des Failovers erstellt wurden, entweder mit der UI oder mit dem folgenden Cmdlet: `Remove-SmBackup`
- Wenn sich nach dem Failover einige der Ressourcen nicht im DR-Modus befinden sollen, verwenden Sie das folgende Cmdlet: `Remove-SmResourceDRMode`

  Weitere Informationen finden Sie im "SnapCenter Software Cmdlet Referenzhandbuch".

- SnapCenter Server verwaltet die einzelnen Storage-Ressourcen (SQL-Datenbanken) im DR- oder nicht-DR-Modus, jedoch nicht die Ressourcengruppe mit Storage-Ressourcen, die sich im DR-Modus oder nicht im DR-Modus befinden.

Failback von sekundärem SnapCenter Plug-in für SQL Server Storage auf den Primärspeicher

Nachdem das SnapCenter Plug-in für den primären SQL Server Storage wieder online ist, sollten Sie ein Failback auf den primären Storage durchführen.

Was Sie brauchen

- Setzen Sie das SnapCenter-Plug-in für SQL Server auf der Seite Managed Hosts in den **Maintenance** -Modus.
- Trennen Sie den sekundären Speicher vom Host, und stellen Sie eine Verbindung zum primären Speicher her.
- Für ein Failback auf den primären Storage stellen Sie sicher, dass die Beziehungsrichtung vor dem Failover unverändert bleibt, indem Sie den umgekehrten Resync-Vorgang durchführen.

  Um die Rollen des primären und sekundären Storage nach der umgekehrten Resync-Operation beizubehalten, führen Sie die erneute Umkehr-Resynchronisierung erneut durch.

  Weitere Informationen finden Sie unter "Spiegelbeziehungen neu synchronisieren"

- MSSQL-Serverdienst neu starten.
- Stellen Sie sicher, dass die SQL-Ressourcen wieder online sind.

> Beim Failover oder Failback des Plug-ins wird der Gesamtstatus des Plug-ins nicht sofort aktualisiert. Der Gesamtstatus von Host und Plug-in wird während der nachfolgenden Aktualisierung des Hosts aktualisiert.

Schritte

1. Navigieren Sie auf der Seite Einstellungen zu **Einstellungen** > **Globale Einstellungen** > **Disaster Recovery**.
2. Deaktivieren Sie Die Option * Disaster Recovery Aktivieren*.
3. Klicken Sie Auf **Anwenden**.
4. Überprüfen Sie, ob der DR-Job aktiviert ist oder nicht, indem Sie auf **Monitor** > **Jobs** klicken.

Nach Ihrer Beendigung

- Sie können das SnapCenter-Plug-in für SQL Server Backups löschen, die während des Failovers erstellt wurden, entweder mit der UI oder mit dem folgenden Cmdlet: `Remove-SmDRFailoverBackups`