Installieren Sie das SnapCenter -Plug-in für Microsoft Exchange Server

SnapCenter software

NetApp
November 06, 2025

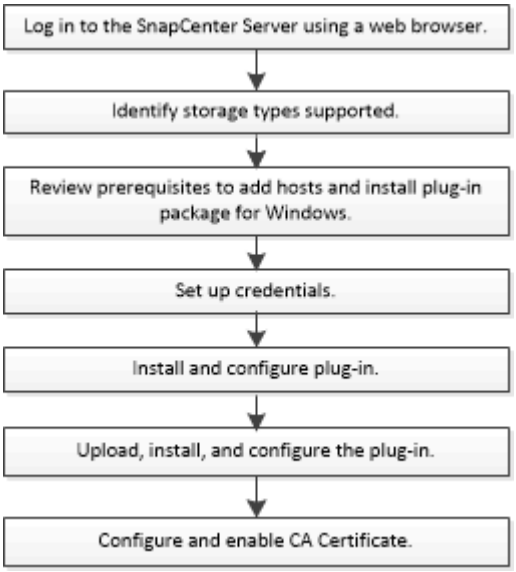
Inhalt

Installieren Sie das SnapCenter -Plug-in für Microsoft Exchange Server . . . 1
Installationsablauf des SnapCenter Plug-ins für Microsoft Exchange Server . . . 1
Voraussetzungen zum Hinzufügen von Hosts und Installieren des SnapCenter -Plug-ins für Microsoft Exchange Server . . . 1
Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows . . . 2
Exchange Server-Berechtigungen erforderlich . . . 3
Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows . . . 4
Einrichten der Anmeldeinformationen für das SnapCenter -Plug-in für Windows . . . 5
Konfigurieren von gMSA unter Windows Server 2016 oder höher . . . 7
Hosts hinzufügen und Plug-in für Exchange installieren . . . 8
Konfigurieren Sie einen benutzerdefinierten Port für die NET TCP-Kommunikation . . . 13
Installieren Sie das Plug-in für Exchange vom SnapCenter Server-Host mithilfe von PowerShell-Cmdlets . . . 14
Installieren Sie das SnapCenter -Plug-in für Exchange im Hintergrund über die Befehlszeile . . . 15
Überwachen des Installationsstatus des SnapCenter -Plug-In-Pakets . . . 16
CA-Zertifikat konfigurieren . . . 17
CA-Zertifikat-CSR-Datei generieren . . . 17
CA-Zertifikate importieren . . . 18
Abrufen des CA-Zertifikatfingerabdrucks . . . 18
Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten . . . 19
CA-Zertifikate für Plug-Ins aktivieren . . . 20
Konfigurieren Sie SnapManager 7.x für die Koexistenz von Exchange und SnapCenter . . . 20

Installieren Sie das SnapCenter -Plug-in für Microsoft Exchange Server

Installationsablauf des SnapCenter Plug-ins für Microsoft Exchange Server

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



Voraussetzungen zum Hinzufügen von Hosts und Installieren des SnapCenter -Plug-ins für Microsoft Exchange Server

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

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten und lokalen Anmeldeberechtigungen auf dem Remotehost verfügen.
- Sie müssen Microsoft Exchange Server 2013, 2016 oder 2019 für eigenständige und Datenbankverfügbarkeitsgruppenkonfigurationen verwenden.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Wenn Sie Clusterknoten in SnapCenter verwalten, benötigen Sie einen Benutzer mit Administratorrechten für alle Knoten im Cluster.
- Sie müssen über einen Benutzer mit Administratorberechtigungen auf dem Exchange-Server verfügen.
- Wenn SnapManager für Microsoft Exchange Server und SnapDrive für Windows bereits installiert sind, müssen Sie die Registrierung des von SnapDrive für Windows verwendeten VSS-Hardwareanbieters

aufheben, bevor Sie das Plug-in für Exchange auf demselben Exchange Server installieren, um einen erfolgreichen Datenschutz mit SnapCenter sicherzustellen.

- Wenn SnapManager für Microsoft Exchange Server und Plug-in für Exchange auf demselben Server installiert sind, müssen Sie alle von SnapManager für Microsoft Exchange Server erstellten Zeitpläne aus dem Windows-Scheduler aussetzen oder löschen.
- Der Host muss vom Server aus in den vollqualifizierten Domänennamen (FQDN) auflösbar sein. Wenn die Hosts-Datei geändert wird, um sie auflösbar zu machen, und wenn sowohl der Kurzname als auch der FQDN in der Hosts-Datei angegeben sind, erstellen Sie einen Eintrag in der SnapCenter -Hosts-Datei im folgenden Format: *<IP-Adresse> <Host-FQDN> <Hostname>*.
- Stellen Sie sicher, dass die folgenden Ports in der Firewall nicht blockiert sind, da sonst der Vorgang zum Hinzufügen des Hosts fehlschlägt. Um dieses Problem zu beheben, müssen Sie den dynamischen Portbereich konfigurieren. Weitere Informationen finden Sie unter "Microsoft-Dokumentation" .
  - Portbereich 50000 – 51000 für Windows 2016 und Exchange 2016
  - Portbereich 6000 – 6500 für Windows 2012 R2 und Exchange 2013
  - Portbereich 49152 – 65536 für Windows 2019

Um den Portbereich zu identifizieren, führen Sie die folgenden Befehle aus:

- netsh int ipv4 show dynamicport tcp
- netsh int ipv4 show dynamicport udp
- netsh int ipv6 show dynamicport tcp
- netsh int ipv6 show dynamicport udp

Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows

Bevor Sie das SnapCenter Plug-Ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatz- und Größenanforderungen des Hostsystems vertraut sein.

Artikel	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .
Mindest-RAM für das SnapCenter -Plug-In auf dem Host	1 GB

Artikel	Anforderungen
Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host	5 GB Sie sollten ausreichend Speicherplatz zuweisen und den Speicherverbrauch des Protokollordners überwachen. Der erforderliche Protokollspeicherplatz variiert je nach Anzahl der zu schützenden Entitäten und der Häufigkeit der Datenschutzvorgänge. Wenn nicht genügend Speicherplatz vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket • PowerShell Core 7.4.2 • Java 11 Oracle Java und OpenJDK Java 11 Oracle Java und OpenJDK werden nur für SAP HANA, IBM Db2, PostgreSQL, MySQL, von NetApp unterstützte Plug-Ins und andere benutzerdefinierte Anwendungen benötigt, die auf einem Windows-Host installiert werden können. Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Exchange Server-Berechtigungen erforderlich

Damit SnapCenter Exchange Server oder DAG hinzufügen und das SnapCenter Plug-in für Microsoft Exchange Server auf einem Host oder DAG installieren kann, müssen Sie SnapCenter mit Anmeldeinformationen für einen Benutzer mit einem Mindestsatz an Berechtigungen und Berechtigungen konfigurieren.

Sie benötigen einen Domänenbenutzer mit lokalen Administratorrechten und lokalen Anmeldeberechtigungen auf dem Remote-Exchange-Host sowie Administratorberechtigungen auf allen Knoten in der DAG. Der Domänenbenutzer benötigt die folgenden Mindestberechtigungen:

- Hinzufügen-MailboxDatabaseCopy
- Dismount-Datenbank
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer
- Get-MailboxDatabase

- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics
- Get-PublicFolderDatabase
- Verschieben-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly:$true
- Mount-Datenbank
- Neue Mailbox-Datenbank
- Neue PublicFolderDatabase
- Entfernen-MailboxDatabase
- Entfernen-MailboxDatabaseCopy
- Entfernen-PublicFolderDatabase
- Lebenslauf-MailboxDatenbankkopie
- Set-AdServerSettings
- Set-MailboxDatabase -allowfilerestore:$true
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows

Bevor Sie das SnapCenter Plug-Ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatz- und Größenanforderungen des Hostsystems vertraut sein.

Artikel	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .
Mindest-RAM für das SnapCenter -Plug-In auf dem Host	1 GB

Artikel	Anforderungen
Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host	5 GB Sie sollten ausreichend Speicherplatz zuweisen und den Speicherverbrauch des Protokollordners überwachen. Der erforderliche Protokollspeicherplatz variiert je nach Anzahl der zu schützenden Entitäten und der Häufigkeit der Datenschutzvorgänge. Wenn nicht genügend Speicherplatz vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket • PowerShell Core 7.4.2 • Java 11 Oracle Java und OpenJDK Java 11 Oracle Java und OpenJDK werden nur für SAP HANA, IBM Db2, PostgreSQL, MySQL, von NetApp unterstützte Plug-Ins und andere benutzerdefinierte Anwendungen benötigt, die auf einem Windows-Host installiert werden können. Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Einrichten der Anmeldeinformationen für das SnapCenter -Plug-in für Windows

SnapCenter verwendet Anmeldeinformationen, um Benutzer für SnapCenter -Vorgänge zu authentifizieren. Sie sollten Anmeldeinformationen für die Installation des Plug-In-Pakets und zusätzliche Anmeldeinformationen für die Durchführung von Datenschutzvorgängen an Datenbanken erstellen.

Informationen zu diesem Vorgang

Sie müssen Anmeldeinformationen für die Installation von Plug-Ins auf Windows-Hosts einrichten. Obwohl Sie Anmeldeinformationen für Windows erstellen können, nachdem Sie Hosts bereitgestellt und Plug-Ins installiert haben, empfiehlt es sich, die Anmeldeinformationen nach dem Hinzufügen von SVMs zu erstellen, bevor Sie Hosts bereitstellen und Plug-Ins installieren.

Richten Sie die Anmeldeinformationen mit Administratorrechten ein, einschließlich Administratorrechten auf dem Remote-Host.

Wenn Sie Anmeldeinformationen für einzelne Ressourcengruppen einrichten und der Benutzername nicht über

vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppen- und Sicherungsrechte zuweisen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.

   Das Fenster „Anmeldeinformationen“ wird angezeigt.

4. Gehen Sie auf der Seite „Anmeldeinformationen“ wie folgt vor:

Für dieses Feld…	Machen Sie Folgendes…
Anmeldeinformationsname	Geben Sie einen Namen für die Anmeldeinformationen ein.
Benutzername	Geben Sie den Benutzernamen ein, der für die Authentifizierung verwendet wird. • Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe Geben Sie den Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe 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 für Systeme, 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 Administratorgruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld „Benutzername“ ist: `UserName`
Passwort	Geben Sie das zur Authentifizierung verwendete Passwort ein.
Authentifizierung	Wählen Sie Windows als Authentifizierungsmodus.

5. Klicken Sie auf **OK**.

Konfigurieren von gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein gruppenverwaltetes Dienstkonto (gMSA) erstellen, das eine automatisierte Kennwortverwaltung für Dienstkonten von einem verwalteten Domänenkonto aus ermöglicht.

Bevor Sie beginnen

- Sie sollten über einen Domänencontroller mit Windows Server 2016 oder höher verfügen.
- Sie sollten über einen Host mit Windows Server 2016 oder höher verfügen, der Mitglied der Domäne 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-Domänencontroller aus: Add-KDSRootKey -EffectiveImmediately
3. Erstellen und konfigurieren Sie Ihr gMSA:
   a. Erstellen Sie ein Benutzergruppenkonto im folgenden Format:

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

   Zum 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.

   Führen Sie dazu den folgenden Befehl von PowerShell aus:

```
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 Ihren Host neu.

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

c. Überprüfen Sie Ihr gMSA-Konto, indem Sie den 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 Dienstanmeldekonto verwendet.

Hosts hinzufügen und Plug-in für Exchange installieren

Sie können die SnapCenter -Seite „Host hinzufügen“ verwenden, um Windows-Hosts hinzuzufügen. Das Plug-in für Exchange wird automatisch auf dem angegebenen Host installiert. Dies ist die empfohlene Methode zum Installieren von Plug-Ins. Sie können einen Host hinzufügen und ein Plug-In entweder für einen einzelnen Host oder einen Cluster installieren.

Bevor Sie beginnen

- Wenn das Betriebssystem des SnapCenter Server-Hosts Windows 2019 und das Betriebssystem des Plug-in-Hosts Windows 2022 ist, sollten Sie Folgendes durchführen:
  - Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher
  - Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher
- Sie müssen ein Benutzer sein, dem eine Rolle mit Berechtigungen zum Installieren und Deinstallieren von Plug-Ins zugewiesen ist, beispielsweise der SnapCenter Administrator.

- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Der Nachrichtenwarteschlangendienst muss ausgeführt werden.
- Wenn Sie ein gruppenverwaltetes Dienstkonto (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren. Weitere Informationen finden Sie unter"Konfigurieren Sie ein gruppenverwaltetes Dienstkonto auf Windows Server 2016 oder höher für Microsoft Exchange Server" .

Informationen zu diesem Vorgang

- Sie können einen SnapCenter -Server nicht als Plug-In-Host zu einem anderen SnapCenter -Server hinzufügen.
- Sie können einen Host hinzufügen und Plug-In-Pakete entweder für einen einzelnen Host oder einen Cluster installieren.
- Wenn ein Exchange-Knoten Teil einer DAG ist, können Sie nicht nur einen Knoten zum SnapCenter -Server hinzufügen.
- Wenn Sie Plug-Ins auf einem Cluster (Exchange DAG) installieren, werden sie auf allen Knoten des Clusters installiert, auch wenn einige Knoten keine Datenbanken auf NetApp LUNs haben.

Ab SnapCenter 4.6 unterstützt SCE Mandantenfähigkeit und Sie können einen Host mit den folgenden Methoden hinzufügen:

Hostvorgang hinzufügen	4.5 und früher	4.6 und höher
Fügen Sie einen IP-losen DAG in einer anderen oder einer anderen Domäne hinzu	Nicht unterstützt	Unterstützt
Fügen Sie mehrere IP-DAGs mit eindeutigen Namen hinzu, die sich in derselben oder einer anderen Domäne befinden.	Unterstützt	Unterstützt
Fügen Sie mehrere IP- oder IP-lose DAGs hinzu, die denselben Hostnamen und/oder DB-Namen domänenübergreifend haben	Nicht unterstützt	Unterstützt
Fügen Sie mehrere IP/IP-lose DAGs mit demselben Namen und domänenübergreifend hinzu	Nicht unterstützt	Unterstützt
Fügen Sie mehrere eigenständige Hosts mit demselben Namen und domänenübergreifend hinzu	Nicht unterstützt	Unterstützt

Das Plug-in für Exchange hängt vom SnapCenter Plug-in-Paket für Windows ab und die Versionen müssen identisch sein. Während der Installation des Plug-ins für Exchange wird standardmäßig das SnapCenter Plug-ins-Paket für Windows ausgewählt und zusammen mit dem VSS-Hardwareanbieter installiert.

Wenn SnapManager für Microsoft Exchange Server und SnapDrive für Windows bereits installiert sind und Sie das Plug-in für Exchange auf demselben Exchange Server installieren möchten, müssen Sie die Registrierung des von SnapDrive für Windows verwendeten VSS-Hardwareanbieters aufheben, da dieser nicht mit dem VSS-Hardwareanbieter kompatibel ist, der mit dem Plug-in für Exchange und dem SnapCenter Plug-ins Package für Windows installiert wurde. Weitere Informationen finden Sie unter "So registrieren Sie den Data

ONTAP VSS Hardware Provider manuell" .

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Stellen Sie sicher, dass oben **Managed Hosts** ausgewählt ist.
3. Klicken Sie auf **Hinzufügen**.
4. Gehen Sie auf der Seite „Hosts“ wie folgt vor:

Für dieses Feld…	Machen Sie Folgendes…
Hosttyp	Wählen Sie **Windows** als Hosttyp. SnapCenter Server fügt den Host hinzu und installiert dann auf dem Host das Plug-in für Windows und das Plug-in für Exchange, falls diese noch nicht installiert sind. Plug-in für Windows und Plug-in für Exchange müssen dieselbe Version haben. Wenn zuvor eine andere Version des Plug-ins für Windows installiert war, aktualisiert SnapCenter die Version im Rahmen der Installation.

Für dieses Feld…	Machen Sie Folgendes…
Hostname	Geben Sie den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den vollqualifizierten Domänennamen (FQDN) einzugeben. Eine IP-Adresse wird für nicht vertrauenswürdige Domänenhosts nur unterstützt, wenn sie in den FQDN aufgelöst wird. Wenn Sie mit SnapCenter einen Host hinzufügen und dieser Teil einer Subdomäne ist, müssen Sie den FQDN angeben. Sie können IP-Adressen oder den FQDN eines der folgenden Elemente eingeben: • Eigenständiger Host • DAG austauschen Für einen Exchange-DAG können Sie: ◦ Fügen Sie einen DAG hinzu, indem Sie den DAG-Namen, die DAG-IP-Adresse, den Knotennamen oder die Knoten-IP-Adresse angeben. ◦ Fügen Sie den IP-losen DAG-Cluster hinzu, indem Sie die IP-Adresse oder den FQDN eines der DAG-Clusterknoten angeben. ◦ Fügen Sie einen DAG ohne IP hinzu, der sich in derselben oder einer anderen Domäne befindet. Sie können auch mehrere IP/IP-lose DAGs mit demselben Namen, aber unterschiedlichen Domänen hinzufügen. Für einen eigenständigen Host oder einen Exchange-DAG (domänenübergreifend oder dieselbe Domäne) wird empfohlen, den FQDN oder die IP-Adresse des Hosts oder DAG anzugeben.

Für dieses Feld…	Machen Sie Folgendes…
Anmeldeinformationen	Wählen Sie den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie die neuen Anmeldeinformationen. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Einzelheiten finden Sie in den Informationen zum Erstellen einer Anmeldeinformation. Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen bewegen. Der Authentifizierungsmodus für Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten „Host hinzufügen“ angeben.

5. Wählen Sie im Abschnitt „Zu installierende Plug-ins auswählen“ die zu installierenden Plug-ins aus.

   Wenn Sie „Plug-in für Exchange“ auswählen, wird die Auswahl von „SnapCenter Plug-in für Microsoft SQL Server“ automatisch aufgehoben. Microsoft empfiehlt, SQL Server und Exchange Server aufgrund der Speicherbelegung und anderer von Exchange benötigter Ressourcennutzung nicht auf demselben System zu installieren.

6. (Optional) Klicken Sie auf **Weitere Optionen**.

Für dieses Feld…	Machen Sie Folgendes…
Hafen	Behalten Sie entweder die Standard-Portnummer bei oder geben Sie die Portnummer an. Die Standard-Portnummer 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.

Für dieses Feld…	Machen Sie Folgendes…
Installationspfad	Der Standardpfad ist `C:\Program Files\NetApp\SnapCenter`. Optional können Sie den Pfad anpassen.
Alle Hosts in der DAG hinzufügen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie einen DAG hinzufügen.
Vorinstallationsprüfungen überspringen	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 ein gruppenverwaltetes Dienstkonto (gMSA), um die Plug-In-Dienste auszuführen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie zum Ausführen der Plug-In-Dienste ein gruppenverwaltetes Dienstkonto (gMSA) verwenden möchten. Geben Sie den gMSA-Namen im folgenden Format an: *Domänenname\Kontoname$*. gMSA wird nur als Anmeldedienstkonto für das SnapCenter -Plug-in für den Windows-Dienst verwendet.

7. Klicken Sie auf **Senden**.

   Wenn Sie das Kontrollkästchen Vorabprüfungen überspringen nicht aktiviert haben, wird überprüft, ob der Host die Voraussetzungen für die Installation des Plug-Ins erfüllt. Wenn die Mindestanforderungen nicht erfüllt sind, werden entsprechende Fehler- oder Warnmeldungen angezeigt.

   Wenn der Fehler mit dem Speicherplatz oder RAM zusammenhängt, können Sie die Datei web.config aktualisieren, die sich unter `C:\Program Files\NetApp\SnapCenter` WebApp zum Ändern der Standardwerte. 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.

8. Überwachen Sie den Installationsfortschritt.

Konfigurieren Sie einen benutzerdefinierten Port für die NET TCP-Kommunikation

Ab der SnapCenter Version 6.0 verwendet das SnapCenter -Plug-in für Windows standardmäßig den Port 909 für die NET TCP-Kommunikation. Wenn der Port 909 verwendet wird, können Sie einen anderen Port für die NET TCP-Kommunikation konfigurieren.

Schritte

1. Ändern Sie den Wert des Schlüssels *NetTCPPort* unter *C:\Programme\ NetApp\ SnapCenter\ SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe.config* in die erforderliche Portnummer. `<add key="NetTCPPort" value="new_port_number" />`
2. Ändern Sie den Wert des Schlüssels *NetTCPPort* unter *C:\Programme\ NetApp\ SnapCenter\ SnapCenter Plug-in für Microsoft Windows\SnapDriveService.dll.config* in die erforderliche Portnummer. `<add key="NetTCPPort" value="new_port_number" />`
3. Heben Sie die Registrierung des Dienstes *Data ONTAP VSS Hardware Provider* auf, indem Sie den folgenden Befehl ausführen: `"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\navssprv.exe" -r service -u`

   Stellen Sie sicher, dass der Dienst nicht in der Liste der Dienste in *services.msc* angezeigt wird.
4. Registrieren Sie den Dienst *Data ONTAP VSS Hardware Provider*, indem Sie den folgenden Befehl ausführen: `"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe" -r service -a ".\LocalSystem"`\`

   Überprüfen Sie, ob der Dienst jetzt in der Liste der Dienste in *services.msc* angezeigt wird.
5. Starten Sie den Dienst „Plug-in für Windows“ neu.

Installieren Sie das Plug-in für Exchange vom SnapCenter Server-Host mithilfe von PowerShell-Cmdlets

Sie sollten das Plug-in für Exchange über die SnapCenter -GUI installieren. Wenn Sie die GUI nicht verwenden möchten, können Sie PowerShell-Cmdlets auf dem SnapCenter Server-Host oder auf einem Remote-Host verwenden.

Bevor Sie beginnen

- SnapCenter Server muss installiert und konfiguriert sein.
- Sie müssen ein lokaler Administrator auf dem Host oder ein Benutzer mit Administratorrechten sein.
- Sie müssen ein Benutzer sein, dem eine Rolle mit Plug-In-, Installations- und Deinstallationsberechtigungen zugewiesen ist, beispielsweise der SnapCenter Administrator.
- Sie müssen die Installationsanforderungen und die unterstützten Konfigurationstypen überprüft haben, bevor Sie das Plug-in für Exchange installieren.
- Der Host, auf dem Sie das Plug-in für Exchange installieren möchten, muss ein Windows-Host sein.

Schritte

1. Richten Sie auf dem SnapCenter Server-Host eine Sitzung mit dem Cmdlet *Open-SmConnection* ein und geben Sie dann Ihre Anmeldeinformationen ein.
2. Fügen Sie den Host hinzu, auf dem Sie das Plug-in für Exchange installieren möchten, indem Sie das Cmdlet *Add-SmHost* mit den erforderlichen Parametern verwenden.

   Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

   Der Host kann ein eigenständiger Host oder ein DAG sein. Wenn Sie einen DAG angeben, ist der Parameter *-IsDAG* erforderlich.

3. Installieren Sie das Plug-in für Exchange mithilfe des Cmdlets *Install-SmHostPackage* mit den erforderlichen Parametern.

   Dieser Befehl installiert das Plug-in für Exchange auf dem angegebenen Host und registriert das Plug-in dann bei SnapCenter.

Installieren Sie das SnapCenter -Plug-in für Exchange im Hintergrund über die Befehlszeile

Sie sollten das Plug-in für Exchange über die SnapCenter -Benutzeroberfläche installieren. Wenn dies aus irgendeinem Grund nicht möglich ist, können Sie das Plug-in für Exchange-Installationsprogramm unbeaufsichtigt im Hintergrundmodus über die Windows-Befehlszeile ausführen.

Bevor Sie beginnen

- Sie müssen Ihre Microsoft Exchange Server-Ressourcen gesichert haben.
- Sie müssen die SnapCenter Plug-In-Pakete installiert haben.
- Sie müssen die frühere Version des SnapCenter -Plug-ins für Microsoft SQL Server vor der Installation löschen.

  Weitere Informationen finden Sie unter "So installieren Sie ein SnapCenter -Plug-In manuell und direkt vom 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 SnapCenter -Plug-in für Microsoft Windows von *C:\ProgramData\ NetApp\ SnapCenter\Package* Repository herunter.

   Auf diesen Pfad kann vom Host aus 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 zu dem Verzeichnis, in dem Sie die Plug-In-Installationsdateien gespeichert haben.
5. Geben Sie den folgenden Befehl ein, um das Plug-In zu installieren.

   snapcenter_windows_host_plugin.exe"/silent /debuglog"<Debug_Log_Path>" /log"<Log_Path>" BI_SNAPCENTER_PORT=<Num> SUITE_INSTALLDIR="<Install_Directory_Pfad>" BI_SERVICEACCOUNT=<Domäne\Administrator> BI_SERVICEPWD=<Passwort> ISFeatureInstall=HPPW,SCW,SCE

   Beispiel:

   C:\ProgramData\ NetApp\ SnapCenter\Package Repository\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\temp" BI_SNAPCENTER_PORT=8145 SUITE_INSTALLDIR="C:\Programme\ NetApp\ SnapCenter" BI_SERVICEACCOUNT=Domäne\Administrator BI_SERVICEPWD=Passwort ISFeatureInstall=HPPW,SCW,SCE

Bei allen während der Installation des Plug-ins für Exchange übergebenen Parametern wird zwischen Groß- und Kleinschreibung unterschieden.

Geben Sie für die Variablen folgende Werte ein:

Variable	Wert
/debuglog"<Debug_Log_Pfad>	Geben Sie den Namen und den Speicherort der Protokolldatei des Suite-Installationsprogramms an, wie im folgenden Beispiel: *Setup.exe /debuglog"C:\PfadZurProtokolldatei\setupexe.log*
BI_SNAPCENTER_PORT	Geben Sie den Port an, über den SnapCenter mit SMCore kommuniziert.
SUITE_INSTALLDIR	Geben Sie das Installationsverzeichnis des Host-Plug-In-Pakets an.
BI_SERVICEACCOUNT	Geben Sie das SnapCenter Plug-in für das Microsoft Windows-Webdienstkonto an.
BI_SERVICEPWD	Geben Sie das Kennwort für das SnapCenter Plug-in für das Microsoft Windows-Webdienstkonto an.
ISFeatureInstall	Geben Sie die Lösung an, die von SnapCenter auf dem Remote-Host bereitgestellt werden soll.

6. Überwachen Sie den Windows-Taskplaner, 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 die Software ohne Fehler installieren.

Bei der Installation des Plug-ins für Exchange wird das Plug-in auf dem Host und nicht auf dem SnapCenter -Server registriert. Sie können das Plug-In auf dem SnapCenter -Server registrieren, indem Sie den Host mithilfe der SnapCenter GUI oder des PowerShell-Cmdlets hinzufügen. Nachdem der Host hinzugefügt wurde, wird das Plug-In automatisch erkannt.

Überwachen des Installationsstatus des SnapCenter -Plug -In-Pakets

Sie können den Fortschritt der Installation des SnapCenter -Plug-In-Pakets auf der Seite „Jobs“ überwachen. Möglicherweise möchten Sie den Installationsfortschritt überprüfen, um festzustellen, wann die Installation abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

Die folgenden Symbole werden auf der Seite „Jobs“ angezeigt und geben den Status des Vorgangs an:

- Im Gange
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In der Warteschlange

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Überwachen** auf **Jobs**.
3. Um auf der Seite **Jobs** die Liste so zu filtern, dass nur Plug-In-Installationsvorgänge aufgeführt werden, gehen Sie wie folgt vor:
   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“ aus.
   d. Wählen Sie im Dropdown-Menü „Status“ den Installationsstatus aus.
   e. Klicken Sie auf **Übernehmen**.
4. Wählen Sie den Installationsauftrag aus und klicken Sie auf **Details**, um die Auftragsdetails anzuzeigen.
5. Klicken Sie auf der Seite **Auftragsdetails** auf **Protokolle anzeigen**.

CA-Zertifikat konfigurieren

CA-Zertifikat-CSR-Datei generieren

Sie können eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren und das Zertifikat importieren, das Sie mithilfe der generierten CSR von einer Zertifizierungsstelle (Certificate Authority, CA) erhalten können. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block verschlüsselten Textes, der einem autorisierten Zertifikatsanbieter übergeben wird, um das signierte CA-Zertifikat zu beschaffen.

Die RSA-Schlüssellänge des CA-Zertifikats muss mindestens 3072 Bit betragen.

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

Wenn Sie das CA-Zertifikat für Ihre Domäne (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie das Generieren der CSR-Datei des CA-Zertifikats überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die jeweiligen Hostnamen im CA-Zertifikat erwähnt werden. Das Zertifikat kann aktualisiert werden, indem vor dem Erwerb des Zertifikats das Feld „Subject Alternative Name (SAN)“ ausgefüllt wird. Bei einem Wildcard-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

CA-Zertifikate importieren

Sie müssen die CA-Zertifikate mithilfe der Microsoft Management Console (MMC) in den SnapCenter -Server und die Windows-Host-Plug-Ins importieren.

Schritte

1. Gehen Sie zur Microsoft-Verwaltungskonsole (MMC) und klicken Sie dann auf **Datei** > **Snap-In hinzufügen/entfernen**.
2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
4. Klicken Sie auf **Konsolenstamm** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsstellen** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Importieren**, um den Importassistenten zu starten.
6. Schließen Sie den Assistenten wie folgt ab:

In diesem Assistentenfenster …	Gehen Sie wie folgt vor…
Privaten Schlüssel importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie anschließend auf **Weiter**.
Importdateiformat	Nehmen Sie keine Änderungen vor; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Kennwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Abschließen des Zertifikatimport-Assistenten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**, um den Import zu starten.

Das zu importierende Zertifikat 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 CA-Zertifikatfingerabdrucks

Ein Zertifikatfingerabdruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Aus dem Inhalt des Zertifikats wird mithilfe eines Fingerabdruckalgorithmus ein Fingerabdruck berechnet.

Schritte

1. Führen Sie auf der GUI Folgendes aus:
   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 **Fingerabdruck**.

d. Kopieren Sie die Hexadezimalzeichen aus dem Feld.

e. Entfernen Sie die Leerzeichen zwischen den Hexadezimalzahlen.

   Wenn der Fingerabdruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, lautet er nach dem Entfernen der Leerzeichen: „a909502dd82ae41433e6f83886b00d4277a32a7b“.

2. Führen Sie in PowerShell Folgendes aus:

   a. Führen Sie den folgenden Befehl aus, um den Fingerabdruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreffnamens zu identifizieren.

      Get-ChildItem -Pfad Zertifikat:\LocalMachine\My

   b. Kopieren Sie den Fingerabdruck.

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 aus, auf denen bereits CA-Zertifikate bereitgestellt sind.

Schritte

1. Entfernen Sie die vorhandene Zertifikatsbindung mit dem 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”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

CA-Zertifikate für Plug-Ins aktivieren

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikate im SnapCenter -Server und den entsprechenden Plug-In-Hosts bereitstellen. Sie sollten die CA-Zertifikatvalidierung für die Plug-Ins aktivieren.

Bevor Sie beginnen

- Sie können die CA-Zertifikate mit dem Cmdlet „*Set-SmCertificateSettings*“ aktivieren oder deaktivieren.
- Den Zertifikatsstatus der Plug-ins können Sie sich mit *Get-SmCertificateSettings* anzeigen lassen.

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Verwaltete Hosts**.
3. Wählen Sie einzelne oder mehrere Plug-In-Hosts aus.
4. Klicken Sie auf **Weitere Optionen**.
5. Wählen Sie **Zertifikatvalidierung aktivieren**.

Nach Abschluss

Auf der Registerkarte „Managed Hosts“ wird ein Vorhängeschloss 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 ist, wurden die Datenschutzvorgänge erfolgreich abgeschlossen.

Konfigurieren Sie SnapManager 7.x für die Koexistenz von Exchange und SnapCenter

Damit das SnapCenter -Plug-in für Microsoft Exchange Server und SnapManager für Microsoft Exchange Server gleichzeitig verwendet werden können, müssen Sie das

SnapCenter -Plug-in für Microsoft Exchange Server auf demselben Exchange Server installieren, auf dem SnapManager für Microsoft Exchange Server installiert ist, die Zeitpläne von SnapManager für Exchange deaktivieren und neue Zeitpläne und Sicherungen mithilfe des SnapCenter -Plug-ins für Microsoft Exchange Server konfigurieren.

Bevor Sie beginnen

- SnapManager für Microsoft Exchange Server und SnapDrive für Windows sind bereits installiert und SnapManager für Microsoft Exchange Server-Backups sind auf dem System und im SnapInfo-Verzeichnis vorhanden.
- Sie sollten die von SnapManager für Microsoft Exchange Server erstellten Backups, die Sie nicht mehr benötigen, gelöscht oder wiederhergestellt haben.
- Sie sollten alle von SnapManager für Microsoft Exchange Server erstellten Zeitpläne aus dem Windows-Planer angehalten oder gelöscht haben.
- SnapCenter Plug-in für Microsoft Exchange Server und SnapManager für Microsoft Exchange Server können auf demselben Exchange Server koexistieren, Sie können jedoch vorhandene SnapManager für Microsoft Exchange Server-Installationen nicht auf SnapCenter aktualisieren.

  SnapCenter bietet keine Option für das Upgrade.

- SnapCenter unterstützt nicht die Wiederherstellung von Exchange-Datenbanken aus SnapManager für Microsoft Exchange Server-Backups.

  Wenn Sie SnapManager für Microsoft Exchange Server nach der Installation des SnapCenter -Plug-ins für Microsoft Exchange Server nicht deinstallieren und später ein SnapManager für Microsoft Exchange Server-Backup wiederherstellen möchten, müssen Sie zusätzliche Schritte ausführen.

Schritte

1. Ermitteln Sie mithilfe von PowerShell auf allen DAG-Knoten, ob der SnapDrive für Windows VSS-Hardwareanbieter registriert ist: *vssadmin list providers*

   ```
   C:\Program Files\NetApp\SnapDrive>vssadmin list providers
   vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
   tool
   (C) Copyright 2001-2013 Microsoft Corp.

   Provider name: 'Data ONTAP VSS Hardware Provider'
      Provider type: Hardware
      Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
      Version: 7. 1. 4. 6845
   ```

2. Heben Sie im SnapDrive -Verzeichnis die Registrierung des VSS-Hardwareanbieters von SnapDrive für Windows auf: *navssprv.exe -r service –u*
3. Überprüfen Sie, ob der VSS-Hardwareanbieter entfernt wurde: *vssadmin list providers*
4. Fügen Sie den Exchange-Host zu SnapCenter hinzu und installieren Sie dann das SnapCenter -Plug-in für Microsoft Windows und das SnapCenter -Plug-in für Microsoft Exchange Server.
5. Überprüfen Sie im Verzeichnis „SnapCenter Plug-in für Microsoft Windows“ auf allen DAG-Knoten, ob der

VSS-Hardwareanbieter registriert ist: *vssadmin list providers*

```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
   Provider type: Hardware
   Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
   Version: 7. 0. 0. 5561
```

6. Stoppen Sie die Sicherungspläne von SnapManager für Microsoft Exchange Server.
7. Erstellen Sie mithilfe der SnapCenter -GUI On-Demand-Backups, konfigurieren Sie geplante Backups und konfigurieren Sie Aufbewahrungseinstellungen.
8. Deinstallieren Sie SnapManager für Microsoft Exchange Server.

   Wenn Sie SnapManager für Microsoft Exchange Server jetzt nicht deinstallieren und später ein SnapManager für Microsoft Exchange Server-Backup wiederherstellen möchten:

   a. Heben Sie die Registrierung des SnapCenter -Plug-ins für Microsoft Exchange Server von allen DAG-Knoten auf: *navssprv.exe -r service -u*

      ```
      C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft
      Windows>navssprv.exe -r service -u
      ```

   b. Registrieren Sie SnapDrive für Windows im Verzeichnis *C:\Programme\ NetApp\ SnapDrive * auf allen DAG-Knoten: *navssprv.exe -r service -a hostname\\username -p password*