Installieren Sie das SnapCenter Plug-in für Microsoft Exchange Server

SnapCenter Software 4.7

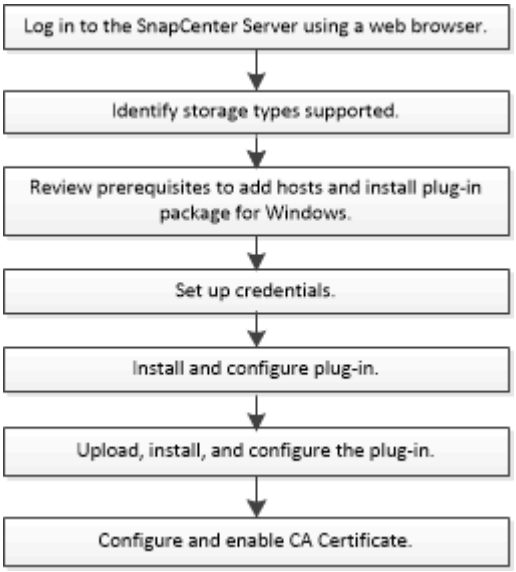
NetApp
September 26, 2025

Inhalt

Installieren Sie das SnapCenter Plug-in für Microsoft Exchange Server

Installations-Workflow 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 für das Hinzufügen von Hosts und die Installation 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 mit lokalen Anmeldeberechtigungen auf dem Remote-Host verfügen.
- Sie müssen Microsoft Exchange Server 2013, 2016 oder 2019 für Standalone- und Database Availability Group-Konfigurationen verwenden.
- 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 Sie Cluster-Nodes in SnapCenter verwalten, müssen Sie einen Benutzer mit Administratorrechten für alle Nodes im Cluster besitzen.
- Sie müssen über einen Benutzer mit Administratorrechten auf dem Exchange Server verfügen.
- Wenn SnapManager für Microsoft Exchange Server und SnapDrive für Windows bereits installiert sind, müssen Sie den von SnapDrive für Windows verwendeten VSS Hardware Provider deinstallieren, bevor

Sie Plug-in für Exchange auf demselben Exchange-Server installieren, um den erfolgreichen Datenschutz mit SnapCenter zu gewährleisten.

- Wenn SnapManager für Microsoft Exchange Server und das Plug-in für Exchange auf demselben Server installiert sind, müssen Sie alle vom SnapManager für Microsoft Exchange Server erstellten Zeitpläne aussetzen oder löschen.
- Der Host muss auf den vollständig qualifizierten Domänennamen (FQDN) vom Server resolable sein. Wenn die Hosts-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>*.
- Stellen Sie sicher, dass die folgenden Ports in der Firewall nicht blockiert sind, da sonst der Vorgang zum Hinzufügen eines Hosts fehlschlägt. Um dieses Problem zu lösen, müssen Sie den dynamischen Portbereich konfigurieren. Weitere Informationen finden Sie unter "Microsoft-Dokumentation".
  - Port-Bereich 50000 - 51000 für Windows 2016 und Exchange 2016
  - Port-Bereich 6000 - 6500 für Windows 2012 R2 und Exchange 2013
  - Portbereich 49152 - 65536 für Windows 2019

Führen Sie die folgenden Befehle aus, um den Port-Bereich zu identifizieren:

- Netsh int ipv4 zeigen Dynamit tcp
- Netsh int ipv4 zeigen Dynamit udp
- Netsh int ipv6 zeigen Dynamit tcp
- Netsh int ipv6 zeigen Dynamit udp

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

Element	Anforderungen
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.
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".

Berechtigungen für Exchange Server erforderlich

Damit SnapCenter das Hinzufügen von Exchange Server oder DAG sowie die Installation des SnapCenter Plug-ins für Microsoft Exchange Server auf einem Host oder einer DAG aktivieren kann, müssen Sie SnapCenter mit Anmeldedaten für einen Benutzer mit einem Minimum an Berechtigungen und Berechtigungen konfigurieren.

Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten verfügen, und über lokale Anmeldeberechtigungen auf dem entfernten Exchange-Host sowie über Administratorberechtigungen auf allen Knoten in der DAG. Der Domänenbenutzer benötigt die folgenden Mindestberechtigungen:

- Add-MailboxDatabaseCopy
- Datenbank Entmounten
- Get-AdServerSettings
- Get-DatabaseVerfügbarkeitGroup
- Get-ExchangeServer
- Get-Mailboxdatenbank

- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistik
- Get-PublicFolderDatabase
- Move-ActiveMailboxDatenbank
- Move-DatabasePath - KonfigurationNur: €true
- Mount-Datenbank
- Neue Postboxdatenbank
- New-PublicFolderDatabase
- Mailboxdatenbank entfernen
- Entfernen Sie-MailboxDatabaseCopy
- Entfernen Sie die-PublicFolderDatabase
- Resume-MailboxDatabaseCopy
- Set-AdServerSettings
- Set-mailboxdatenbank -allowfilerestore: €true
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

Konfigurieren Sie gMSA unter Windows Server 2012 oder höher

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

Element	Anforderungen
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.
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-in für Windows ein

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

Über diese Aufgabe

Sie müssen Anmeldedaten für die Installation von Plug-ins auf Windows-Hosts einrichten. Obwohl Sie nach der Implementierung von Hosts und der Installation von Plug-ins Anmeldedaten für Windows erstellen können, sollten Sie vor der Implementierung von Hosts und Plug-ins zunächst die Anmeldedaten nach dem Hinzufügen von SVMs erstellen.

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

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

vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppe und die Sicherungsberechtigungen zuweisen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Credential**.
3. Klicken Sie Auf **Neu**.

   Das Fenster Credential wird angezeigt.

4. Gehen Sie auf der Seite Credential wie folgt vor:

Für dieses Feld…	Tun Sie das…
Name der Anmeldeinformationen	Geben Sie einen Namen für die Anmeldedaten 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 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 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`
Passwort	Geben Sie das für die Authentifizierung verwendete Passwort ein.

Für dieses Feld…	Tun Sie das…
Authentifizierung	Wählen Sie Windows als Authentifizierungsmodus aus.

5. Klicken Sie auf **OK**.

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.

Fügen Sie Hosts hinzu und installieren Sie das Plug-in für Exchange

Sie können die Seite SnapCenter Add Host 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 ein Cluster installieren.

Was Sie brauchen

- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Plug-in-Installations- und Deinstallationsberechtigungen verfügt, wie z. B. die SnapCenter-Admin
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, wenn Sie keine Anmeldedaten angeben oder

der Benutzer zu einem lokalen Workgroup-Benutzer gehört, müssen Sie UAC auf dem Host deaktivieren.

- Der Nachrichtenwarteschlange-Service muss ausgeführt werden.
- Wenn Sie Group Managed Service Account (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren. Weitere Informationen finden Sie unter"Konfigurieren Sie das Gruppenkonto für Managed Services unter Windows Server 2012 oder höher für Microsoft Exchange Server".

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 Plug-in-Pakete für einen einzelnen Host oder Cluster installieren.
- Ist ein Exchange-Knoten Teil einer DAG, kann der SnapCenter-Server nicht nur einen Knoten hinzufügen.
- Wenn Sie Plug-ins auf einem Cluster (Exchange DAG) installieren, werden sie auf allen Knoten des Clusters installiert, selbst wenn einige Knoten keine Datenbanken auf NetApp LUNs haben.

Ab SnapCenter 4.6 unterstützt SCE die Mandantenfähigkeit und Sie können einen Host über die folgenden Methoden hinzufügen:

Fügen Sie einen Host-Vorgang hinzu	4.5 und früher	4.6 und höher
Fügen Sie IP-lose DAG in einer anderen Domäne oder anderen Domäne hinzu	Nicht unterstützt	Unterstützt
Fügen Sie mehrere IP-DAGs mit eindeutigen Namen hinzu. Diese befinden sich in derselben oder in mehreren Domänen	Unterstützt	Unterstützt
Fügen Sie mehrere IP- oder IP-lose DAGs mit denselben Host-Namen und/oder DB-Namen in Cross-Domain hinzu	Nicht unterstützt	Unterstützt
Hinzufügen mehrerer IP/IP-loser DAGs mit demselben Namen und domänenübergreifender	Nicht unterstützt	Unterstützt
Fügen Sie mehrere Standalone-Hosts mit demselben Namen und domänenübergreifender Infrastruktur hinzu	Nicht unterstützt	Unterstützt

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

Falls SnapManager für Microsoft Exchange Server und SnapDrive für Windows bereits installiert sind, Und Sie möchten Plug-in für Exchange auf demselben Exchange-Server installieren, müssen Sie den von SnapDrive für Windows verwendeten VSS Hardware-Anbieter deaktivieren, da er mit dem VSS Hardware Provider, der mit Plug-in für Exchange und SnapCenter Plug-ins Package für Windows installiert ist, nicht kompatibel ist. 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. Vergewissern Sie sich, dass **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 als Hosttyp * Windows* aus. SnapCenter Server fügt den Host hinzu und installiert dann auf dem Host das Plug-in für Windows und das Plug-in für Exchange, falls sie nicht bereits installiert sind. Plug-in für Windows und Plug-in für Exchange müssen die gleiche Version sein. Wenn zuvor eine andere Version des Plug-ins für Windows installiert wurde, aktualisiert SnapCenter die Version als Teil der Installation.

Für dieses Feld…	Tun Sie das…
Host-Name	Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den vollständig qualifizierten Domänennamen (FQDN) einzugeben. Eine IP-Adresse wird nur für nicht vertrauenswürdige Domänenhosts unterstützt, wenn sie auf den FQDN auflöst. Wenn Sie einen Host mit SnapCenter hinzufügen und dieser Teil einer Unterdomäne ist, müssen Sie den FQDN angeben. Sie können IP-Adressen oder den FQDN einer der folgenden Adressen eingeben: • Eigenständiger Host • Exchange DAG Vorteile einer Exchange DAG: ◦ Fügen Sie eine DAG hinzu, indem Sie den DAG-Namen, die DAG-IP-Adresse, den Node-Namen oder die Node-IP-Adresse angeben. ◦ Fügen Sie den DAG-Cluster ohne IP hinzu, indem Sie die IP-Adresse oder den FQDN eines der DAG-Cluster-Nodes angeben. ◦ Fügen Sie IP-lose DAG hinzu, die sich in derselben Domäne oder einer anderen Domäne befindet. Sie können auch mehrere IP/IP-basierte DAGs mit demselben Namen und aber verschiedenen Domänen hinzufügen. Für einen eigenständigen Host oder eine Exchange-DAG (domänenübergreifend oder gleiche Domäne) wird empfohlen, FQDN oder die IP-Adresse des Hosts oder der DAG bereitzustellen.

Für dieses Feld…	Tun Sie das…
Anmeldedaten	Wählen Sie den von Ihnen erstellten Anmeldeinformationsnamen aus, oder erstellen Sie die neuen Anmeldeinformationen. 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 zum Installieren auswählen die zu installierenden Plug-ins aus.

   Wenn Sie Plug-in für Exchange auswählen, wird das SnapCenter-Plug-in für Microsoft SQL Server automatisch deaktiviert. Microsoft empfiehlt, dass SQL Server und Exchange-Server aufgrund der verwendeten Speichermenge und anderer von Exchange benötigten Ressourcen nicht auf demselben System installiert werden.

6. (Optional) 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.

Für dieses Feld…	Tun Sie das…
Installationspfad	Der Standardpfad lautet `C:\Program Files\NetApp\SnapCenter`. Optional können Sie den Pfad anpassen.
Fügen Sie alle Hosts in der DAG hinzu	Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine DAG hinzufügen.
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€*. GSSA wird nur für den SnapCenter-Plug-in für Windows-Dienst als Anmelde-Dienstkonto verwendet.

7. Klicken Sie Auf **Absenden**.

   Wenn Sie das Kontrollkästchen Vorabprüfungen nicht aktiviert haben, wird der Host validiert, um festzustellen, ob es die Anforderungen für die Installation des Plug-ins erfüllt. Wenn die Mindestanforderungen nicht erfüllt werden, werden die entsprechenden Fehler- oder Warnmeldungen angezeigt.

   Wenn der Fehler mit dem Festplattenspeicher oder RAM zusammenhängt, können Sie die Datei Web.config unter aktualisieren `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.

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

Sie sollten das Plug-in für Exchange über die SnapCenter-Benutzeroberfläche installieren. Wenn Sie die GUI nicht verwenden möchten, können Sie PowerShell

Cmdlets auf dem SnapCenter Server Host oder auf einem Remote Host verwenden.

Was Sie brauchen

- SnapCenter-Server muss installiert und konfiguriert worden sein.
- Sie müssen ein lokaler Administrator auf dem Host oder ein Benutzer mit Administratorrechten sein.
- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen Plug-in, Installation und Deinstallation verfügt, wie z. B. SnapCenter Admin
- Vor der Installation des Plug-ins für Exchange müssen Sie die Installationsanforderungen und die Typen der unterstützten Konfigurationen geprüft haben.
- Der Host, auf dem das Plug-in für Exchange installiert werden soll, muss ein Windows-Host sein.

Schritte

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

   Es kann sich dabei um einen Standalone-Host oder eine DAG handeln. Wenn Sie eine DAG angeben, ist der Parameter *-IsDAG* erforderlich.

3. Installieren Sie das Plug-in für Exchange mit dem Cmdlet *Install-SmHostPackage* mit den erforderlichen Parametern.

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

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

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

Was Sie brauchen

- Sie müssen Ihre Microsoft Exchange Server-Ressourcen gesichert haben.
- Sie müssen die SnapCenter-Plug-in-Pakete installiert haben.
- 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 vollständigen Zugriff darauf hat.
2. Laden Sie das SnapCenter Plug-in für Microsoft Windows von *C:\ProgramData\NetApp\SnapCenter\Paket* 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. Geben Sie den folgenden Befehl ein, um die Variablen durch Ihre Daten zu ersetzen:

   _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_SERVICECEPWD= SCHEICE= SCHEINSW

   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\\BI_SERVICECOUNT,SPERW_Administrator,SPEICEICE_DER_DER_SPREN,SnapCenter,SCEICEICEICHTE_DER_DER_DER_DER_Administrator_SPREN,SPREN

   Alle während der Installation von Plug-in für Exchange übergebenen Parameter gelten bei der Groß-/Kleinschreibung.

   a. */silent /debuglog„C:\Installdebug.log“ /log„C:\temp“ BI_SNAPCENTER_PORT=8145 SUITE_INSTALLDIR=„C:\Programme“ BI_SERVICEACCOUNT=Demo\Administrator BI_SERVICEPWD=Netapp1! ISFeatureInstall=HPW, SCW*

      Geben Sie die folgenden Werte für die Variablen ein:

Variabel	Wert
/Debuglog“<Debug_Log_Path>	Geben Sie den Namen und den Speicherort der Protokolldatei für das Installationsprogramm der Suite an, wie im folgenden Beispiel: *Setup.exe /debuglog„C:\PathToLog\setupexe.log*
BI_SNAPCENTER_PORT	Geben Sie den Port an, auf dem SnapCenter mit SMCore kommuniziert.
SUITE_INSTALLDIR	Geben Sie das Installationsverzeichnis für das Host-Plug-in-Paket an.
BI_SERVICEACCOUNT	Geben Sie das SnapCenter-Plug-in für das Web-Service-Konto von Microsoft Windows an.

Variabel	Wert
BI_SERVICEPWD	Geben Sie das Passwort für das SnapCenter-Plug-in für das Microsoft Windows-Webservice-Konto an.
ISFeatureInstall	Geben Sie die Lösung an, die von SnapCenter auf dem Remote-Host implementiert werden soll.

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 Installer *msiexe.exe* die Software fehlerfrei installieren.

Die Installation des Plug-ins für Exchange 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 Installationsstatus des SnapCenter Plug-in-Pakets

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 "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.

- Gibt 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.

Konfigurieren Sie SnapManager 7.x für Exchange und SnapCenter, um koexistieren zu können

Damit das SnapCenter Plug-in für Microsoft Exchange Server gemeinsam mit SnapManager für Microsoft Exchange Server eingesetzt werden kann, müssen Sie das SnapCenter Plug-in für Microsoft Exchange Server auf demselben Exchange Server installieren, auf dem SnapManager für Microsoft Exchange Server installiert ist, indem Sie die Zeitpläne für SnapManager für Exchange deaktivieren. Und neue Zeitpläne und Backups mit dem SnapCenter Plug-in für Microsoft Exchange Server konfigurieren.

Was Sie brauchen

- SnapManager für Microsoft Exchange Server und SnapDrive für Windows sind bereits installiert und Backups von SnapManager für Microsoft Exchange Server sind im System und im SnapInfo Verzeichnis vorhanden.
- Sie sollten die von SnapManager für Microsoft Exchange Server erstellten Backups gelöscht oder zurückgewonnen haben, die Sie nicht mehr benötigen.
- Sie sollten alle Zeitpläne ausgesetzt oder gelöscht haben, die von SnapManager für Microsoft Exchange Server aus dem Windows-Scheduler erstellt wurden.
- Das SnapCenter Plug-in für Microsoft Exchange Server und SnapManager für Microsoft Exchange Server können parallel auf demselben Exchange Server eingesetzt werden. Sie können jedoch kein Upgrade von bestehenden SnapManager für Microsoft Exchange Server Installationen auf SnapCenter durchführen.

SnapCenter bietet keine Upgrade-Option.

- 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 Backup von SnapManager für Microsoft Exchange Server wiederherstellen möchten, müssen Sie weitere Schritte durchführen.

Schritte

1. Bestimmen Sie mithilfe von PowerShell auf allen DAG-Knoten, ob der SnapDrive für Windows VSS Hardware Provider 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. Aus dem SnapDrive-Verzeichnis den VSS Hardware Provider von SnapDrive für Windows: *navssprv.exe -r Service -U*
3. Überprüfen Sie, ob der VSS Hardware Provider 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 SnapCenter-Plug-in für Microsoft Windows-Verzeichnis 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. Beenden Sie die Backup-Zeitpläne für SnapManager für Microsoft Exchange Server.
7. Erstellen Sie über die GUI von SnapCenter 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 nicht jetzt deinstallieren und später ein Backup von SnapManager für Microsoft Exchange Server wiederherstellen möchten:

   a. Heben Sie das SnapCenter Plug-in 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. Aus dem Verzeichnis *C:\Programme\NetApp\SnapDrive* registrieren Sie SnapDrive für Windows auf allen DAG Knoten: *navssprv.exe -r Service -a hostname\\username -p password*