Installieren Sie das SnapCenter -Plug-in für Microsoft Windows

SnapCenter software

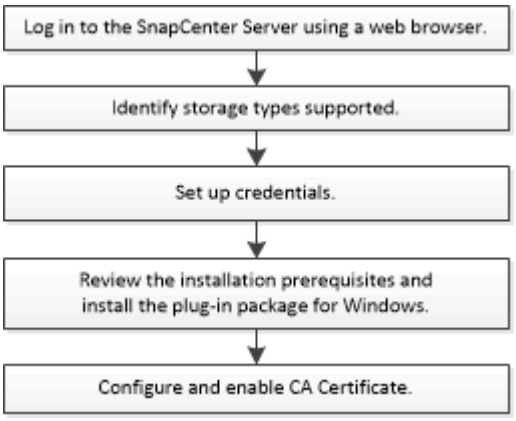
NetApp
November 06, 2025

Inhalt

Installieren Sie das SnapCenter -Plug-in für Microsoft Windows

Installationsablauf des SnapCenter Plug-ins für Microsoft Windows

Sie müssen das SnapCenter Plug-in für Microsoft Windows installieren und einrichten, wenn Sie Windows-Dateien schützen möchten, bei denen es sich nicht um Datenbankdateien handelt.



Installationsanforderungen für das SnapCenter -Plug-in für Microsoft Windows

Sie sollten sich bestimmter Installationsanforderungen bewusst sein, bevor Sie das Plug-in für Windows installieren.

Bevor Sie mit der Verwendung des Plug-ins für Windows beginnen, muss der SnapCenter Administrator den SnapCenter -Server installieren und konfigurieren und die erforderlichen Aufgaben ausführen.

- Sie müssen über SnapCenter Administratorrechte verfügen, um das Plug-in für Windows zu installieren.

  Die SnapCenter Administratorrolle muss über Administratorrechte verfügen.

- Sie müssen den SnapCenter -Server installiert und konfiguriert haben.
- 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.
- Sie müssen SnapMirror und SnapVault einrichten, wenn Sie eine Backup-Replikation wünschen.

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" . Wenn Sie ein Windows-Cluster-Setup verwenden, sollten Sie auch die Windows-Remoteverwaltung (WinRM) installieren und konfigurieren.
Mindest-RAM für das SnapCenter -Plug-In auf dem Host	1 GB
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 Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Richten Sie Ihre Anmeldeinformationen für das Plug-in für Windows ein

SnapCenter verwendet Anmeldeinformationen, um Benutzer für SnapCenter -Vorgänge zu authentifizieren. Sie sollten Anmeldeinformationen für die Installation von SnapCenter -Plug-Ins und zusätzliche Anmeldeinformationen für die Durchführung von Datenschutzvorgängen auf Windows-Dateisystemen erstellen.

Was Sie brauchen

- Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-Ins installieren.
- Sie müssen die Anmeldeinformationen mit Administratorrechten, einschließlich Administratorrechten, auf dem Remote-Host einrichten.
- Wenn Sie Anmeldeinformationen für einzelne Ressourcengruppen einrichten und der Benutzer nicht über

vollständige Administratorrechte verfügt, müssen Sie dem Benutzer 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**.
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/Passwort	Geben Sie den Benutzernamen und das Kennwort ein, die für die Authentifizierung verwendet werden. • 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` ◦ `UserName@upn` • 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“ lautet wie folgt: `UserName` Verwenden Sie in den Passwörtern keine doppelten Anführungszeichen (") oder Backticks (`). Sie sollten die Zeichen „Kleiner als“ (<) und „Ausrufezeichen“ (!) nicht zusammen in Passwörtern verwenden. Zum Beispiel kleiner als <!10, kleiner als 10 <!, Backtick `12.

Für dieses Feld…	Machen Sie Folgendes…
Passwort	Geben Sie das zur Authentifizierung verwendete Passwort ein.

5. Klicken Sie auf **OK**.

   Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie möglicherweise einem Benutzer oder einer Benutzergruppe auf der Seite „Benutzer und Zugriff“ die Anmeldeinformationsverwaltung zuweisen.

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 SnapCenter Plug-in für Microsoft Windows installieren

Sie können die SnapCenter -Seite „Host hinzufügen“ verwenden, um Windows-Hosts hinzuzufügen. Das SnapCenter -Plug-in für Microsoft Windows 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 den Berechtigungen zum Installieren und Deinstallieren von Plug-Ins zugewiesen ist, beispielsweise die SnapCenter Administratorrolle.
- 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 SnapCenter -Benutzer sollte der Rolle „Als Dienst anmelden“ des Windows-Servers hinzugefügt werden.
- Sie sollten sicherstellen, dass der Nachrichtenwarteschlangendienst ausgeführt wird.
- Wenn Sie ein gruppenverwaltetes Dienstkonto (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

  "Konfigurieren Sie das gruppenverwaltete Dienstkonto auf Windows Server 2016 oder höher für das Windows-Dateisystem"

Informationen zu diesem Vorgang

- Sie können einen SnapCenter -Server nicht als Plug-In-Host zu einem anderen SnapCenter -Server hinzufügen.
- Windows-Plug-Ins
  - Microsoft Windows
  - Microsoft Exchange Server
  - Microsoft SQL Server
  - SAP HANA
- Installieren von Plug-ins auf einem Cluster

  Wenn Sie Plug-Ins auf einem Cluster (WSFC, Oracle RAC oder Exchange DAG) installieren, werden sie auf allen Knoten des Clusters installiert.

- Speicher der E-Serie

  Sie können das Plug-in für Windows nicht auf einem Windows-Host installieren, der mit einem Speicher der E-Serie verbunden ist.

> SnapCenter unterstützt nicht das Hinzufügen desselben Hosts (Plug-In-Hosts) zu SnapCenter , wenn der Host bereits Teil einer Arbeitsgruppe ist und in eine andere Domäne geändert wurde oder umgekehrt. Wenn Sie denselben Host hinzufügen möchten, sollten Sie den Host aus SnapCenter entfernen und erneut hinzufügen.

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 den Hosttyp **Windows** aus. SnapCenter Server fügt den Host hinzu und installiert dann das Plug-in für Windows, falls es nicht bereits auf dem Host installiert ist.
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. Sie können die IP-Adressen oder den FQDN eines der folgenden Elemente eingeben: • Eigenständiger Host • Windows Server-Failoverclustering (WSFC) Wenn Sie mit SnapCenter einen Host hinzufügen und dieser Teil einer Subdomäne ist, müssen Sie den FQDN angeben.
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. Details zu den Anmeldeinformationen, einschließlich Benutzername, Domäne und Hosttyp, werden angezeigt, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen bewegen. Der Authentifizierungsmodus 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.

   Für neue Bereitstellungen werden keine Plug-In-Pakete aufgelistet.

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.
Installationspfad	Der Standardpfad ist C:\Programme\ NetApp\ SnapCenter. Optional können Sie den Pfad anpassen. Für das SnapCenter Plug-ins-Paket für Windows lautet der Standardpfad C:\Programme\ NetApp\ SnapCenter. Wenn Sie möchten, können Sie den Standardpfad jedoch anpassen.
Alle Hosts im Cluster hinzufügen	Aktivieren Sie dieses Kontrollkästchen, um alle Clusterknoten in einem WSFC hinzuzufügen.
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 Anforderungen für die Installation des Plug-Ins erfüllt. Speicherplatz, RAM, PowerShell-Version, .NET-Version und Speicherort werden anhand der Mindestanforderungen überprüft. Werden die Mindestanforderungen nicht erfüllt, werden entsprechende Fehler- bzw. 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.

Installieren Sie das SnapCenter -Plug-in für Microsoft Windows mithilfe von PowerShell-Cmdlets auf mehreren Remotehosts

Wenn Sie das SnapCenter Plug-in für Microsoft Windows auf mehreren Hosts gleichzeitig installieren möchten, können Sie dies mithilfe des `Install-SmHostPackage` PowerShell-Cmdlet.

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

Schritte

1. Starten Sie PowerShell.
2. Richten Sie auf dem SnapCenter Server-Host eine Sitzung ein, indem Sie `Open-SmConnection` Cmdlet und geben Sie dann Ihre Anmeldeinformationen ein.
3. Fügen Sie den eigenständigen Host oder den Cluster mithilfe des `Add-SmHost` Cmdlet und die erforderlichen Parameter.

   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" .

4. Installieren Sie das Plug-in auf mehreren Hosts mithilfe der `Install-SmHostPackage` Cmdlet und die erforderlichen Parameter.

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

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

Sie können das SnapCenter -Plug-in für Microsoft Windows lokal auf einem Windows-Host installieren, wenn Sie das Plug-in nicht remote über die SnapCenter -GUI installieren können. Sie können das Installationsprogramm des SnapCenter -Plug-ins für

Microsoft Windows unbeaufsichtigt im stillen Modus über die Windows-Befehlszeile ausführen.

Bevor Sie beginnen

- Sie müssen das Hosting-Paket ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) installiert haben.
- Sie müssen PowerShell 7.4.2 oder höher installiert haben.
- Sie müssen ein lokaler Administrator auf dem Host sein.

Schritte

1. Laden Sie das SnapCenter -Plug-in für Microsoft Windows von Ihrem Installationsort herunter.

   Der Standardinstallationspfad ist beispielsweise C:\ProgramData\ NetApp\ SnapCenter\Package Repository.

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

2. Kopieren Sie die Installationsdatei auf den Host, auf dem Sie das Plug-In installieren möchten.
3. Navigieren Sie in der Eingabeaufforderung zu dem Verzeichnis, in das Sie die Installationsdatei heruntergeladen haben.
4. Geben Sie den folgenden Befehl ein und ersetzen Sie die Variablen durch Ihre Daten:

   ```
   "snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""
   BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=
   ISFeatureInstall=SCW
   ```

   Beispiel:

   ```
   `"C:\ProgramData\NetApp\SnapCenter\Package Repository
   \snapcenter_windows_host_plugin.exe"/silent /debuglog"C:
   \HPPW_SCW_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
   SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
   BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
   ISFeatureInstall=SCW`
   ```

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

   Geben Sie die Werte für die folgenden Variablen 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:\PathToLog\setupexe.log".

Variable	Wert
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.

Der Parameter *debuglog* enthält den Pfad der Protokolldatei für SnapCenter. Das Schreiben in diese Protokolldatei ist die bevorzugte Methode zum Abrufen von Informationen zur Fehlerbehebung, da die Datei die Ergebnisse der Prüfungen enthält, die die Installation hinsichtlich der Plug-In-Voraussetzungen durchführt.

Bei Bedarf finden Sie zusätzliche Informationen zur Fehlerbehebung in der Protokolldatei für das SnapCenter für Windows-Paket. Die Protokolldateien für das Paket werden (die ältesten zuerst) im Ordner *%Temp%* aufgelistet, beispielsweise *C:\temp*\.

Bei der Installation des Plug-ins für Windows 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**.

Konfigurieren des CA-Zertifikats

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.