



Bereiten Sie die Installation von benutzerdefinierten SnapCenter-Plug-ins vor

SnapCenter Software 4.8

NetApp
January 18, 2024

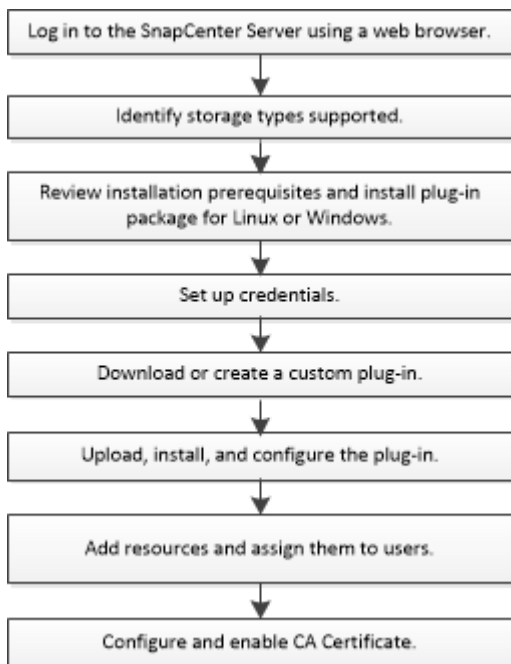
Inhalt

- Bereiten Sie die Installation von benutzerdefinierten SnapCenter-Plug-ins vor. 1
 - Installationsworkflow von benutzerdefinierten SnapCenter Plug-ins 1
 - Voraussetzungen für das Hinzufügen von Hosts und die Installation benutzerdefinierter SnapCenter Plug-ins 1
 - Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows 4
 - Host-Anforderungen für die Installation des SnapCenter Plug-ins Pakets für Linux 5
- Richten Sie Anmeldedaten für benutzerdefinierte SnapCenter-Plug-ins ein 5
- Konfigurieren Sie gMSA unter Windows Server 2012 oder höher 9
- Installieren Sie die benutzerdefinierten SnapCenter-Plug-ins 10
- Konfigurieren Sie das CA-Zertifikat 17

Bereiten Sie die Installation von benutzerdefinierten SnapCenter-Plug-ins vor

Installationsworkflow von benutzerdefinierten SnapCenter Plug-ins

Sie sollten benutzerdefinierte SnapCenter-Plug-ins installieren und einrichten, wenn Sie benutzerdefinierte Plug-in-Ressourcen schützen möchten.



["Entwickeln Sie ein Plug-in für Ihre Applikation"](#)

Voraussetzungen für das Hinzufügen von Hosts und die Installation benutzerdefinierter SnapCenter Plug-ins

Bevor Sie einen Host hinzufügen und die Plug-ins-Pakete installieren, müssen Sie alle Anforderungen erfüllen. Die benutzerdefinierten Plug-ins können sowohl in Windows- als auch in Linux-Umgebungen verwendet werden.

- Sie müssen ein benutzerdefiniertes Plug-in erstellt haben. Weitere Informationen finden Sie in den Entwicklerinformationen.

["Entwickeln Sie ein Plug-in für Ihre Applikation"](#)

- Wenn Sie MySQL oder DB2 Applikationen managen möchten, müssen Sie die benutzerdefinierten Plug-ins für MySQL und DB2 von NetApp heruntergeladen haben.
- Sie müssen Java 1.8 oder Java 11 (64-bit) auf Ihrem Linux- oder Windows-Host installiert haben.
- 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.

- Die benutzerdefinierten Plug-ins müssen auf dem Client-Host verfügbar sein, von dem aus der Add-Host-Vorgang ausgeführt wird.

Allgemein

Wenn Sie iSCSI verwenden, sollte der iSCSI-Dienst ausgeführt werden.

SHA512-Hash

- Bei von NetApp bereitgestellten benutzerdefinierten Plug-ins sollten Sie sicherstellen, dass Sie den SHA512-Hash der benutzerdefinierten Plug-in-Datei zur Datei *Custom_Plugin_Prüfsummen_list* hinzugefügt haben.
 - Für den Linux-Host befindet sich der SHA512-Hash unter */var/opt/snapcenter/scc/Custom_Plugin_Prüfsummen_list.txt*
 - Für Windows-Host befindet sich der SHA512-Hash unter *C:\Programme\NetApp\SnapCenter Plug-in Creator\etc\Custom_Plugin_checksum_list.txt*

Der SHA512-Hash für benutzerdefinierte Installationspfade befindet sich bei `<Custom Path>\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\Custom_Plugin_Prüfsummen_list.txt`

Die Custom_Plugin_Prüfsummenliste ist Teil der benutzerdefinierten Plug-in-Installation auf dem Host von SnapCenter.

- Für benutzerdefinierte Plug-ins, die für Ihre Anwendung erstellt wurden, sollten Sie die folgenden Schritte ausführen:
 - a. Hat den SHA512-Hash der Plug-in-ZIP-Datei erzeugt.

Sie können Online-Tools wie verwenden ["SHA512-Hash"](#).
 - b. Der erzeugte SHA512-Hash wurde in einer neuen Zeile der Datei *Custom_Plugin_Checksumme_list* hinzugefügt.

Die Kommentare beginnen mit # Symbol, um das Plug-in zu identifizieren, zu dem der Hash gehört.

Nachfolgend ein Beispiel für einen Eintrag von SHA512-Hash in der Prüfsummendatei:

```
#ORASCPM
03721f567a1e4a1cb5569066b9a58af619ee12b1f8713108f81b696cfbdb81c25232fa63
d6e6777a2b2a1ec068bb0a93a59a8ade71587182f8bccbe81f7e0ba6
```

Windows Hosts

- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten mit lokalen Anmeldeberechtigungen auf dem Remote-Host verfügen.
- Wenn Sie Cluster-Nodes in SnapCenter verwalten, müssen Sie einen Benutzer mit Administratorrechten für alle Nodes im Cluster besitzen.

Linux-Hosts

- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder nicht-Root-Benutzer aktiviert haben.
- Sie müssen Java 1.8 oder Java 11 (64-bit) auf Ihrem Linux-Host installiert haben.

Wenn Sie Windows Server 2019 oder Windows Server 2016 für den SnapCenter-Server-Host verwenden, müssen Sie Java 1.8 oder Java 11 (64-Bit) installieren. Das Interoperabilitäts-Matrix-Tool (IMT) enthält aktuelle Informationen zu Anforderungen.

["Java-Downloads für alle Betriebssysteme"](#)

["NetApp Interoperabilitäts-Matrix-Tool"](#)

- Sie müssen sudo-Berechtigungen für den nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen. Fügen Sie die folgenden Zeilen zur Datei /etc/sudoers mit dem Dienstprogramm visudo Linux hinzu.



Stellen Sie sicher, dass Sie sudo Version 1.8.7 oder höher verwenden.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/  
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,  
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,  
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc  
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/  
LINUX_USER/.sc_netapp/Linux_Prechecks.sh  
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config  
_Check.sh  
Cmnd_Alias SCCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/bin/sc_command_executor  
Cmnd_Alias SCCMDEXECUTOR =checksum_value==  
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor  
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,  
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD  
Defaults: LINUX_USER !visiblepw  
Defaults: LINUX_USER !requiretty
```

LINUX_USER ist der Name des nicht-root-Benutzers, den Sie erstellt haben.


Sie erhalten den *checksum_value* aus der Datei **oracle_checksum.txt**, die sich unter *C:\ProgramData\NetApp\SnapCenter\Package Repository* befindet.



Das Beispiel sollte nur als Referenz zur Erstellung eigener Daten verwendet werden.


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

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

Element	Anforderungen
Betriebssysteme	Microsoft Windows Aktuelle Informationen zu unterstützten Versionen finden Sie im " NetApp Interoperabilitäts-Matrix-Tool ".
MindestRAM für das SnapCenter Plug-in auf dem Host	1 GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	5 GB  Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	<ul style="list-style-type: none">• Microsoft .NET Framework 4.7.2 oder höher• Windows Management Framework (WMF) 4.0 oder höher• PowerShell 4.0 oder höher <p>Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".</p> <p>Informationen zur .NET-spezifischen Fehlerbehebung finden Sie unter "Das Upgrade oder die Installation von SnapCenter schlägt bei älteren Systemen, die keine Internetverbindung haben, fehl."</p>

Host-Anforderungen für die Installation des SnapCenter Plug-ins Pakets für Linux

Bevor Sie das SnapCenter-Plug-ins-Paket für Linux installieren, sollten Sie sicherstellen, dass der Host die Anforderungen erfüllt.

Element	Anforderungen
Betriebssysteme	<ul style="list-style-type: none">• Red Hat Enterprise Linux• Oracle Linux• SUSE Linux Enterprise Server (SLES)
MindestRAM für das SnapCenter Plug-in auf dem Host	1 GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	2 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	Java 1.8 (64-bit) Oracle Java oder OpenJDK Varianten Wenn SIE JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die JAVA_HOME-Option unter <code>/var/opt/snapcenter/spl/etc/spl.properties</code> auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.

Aktuelle Informationen zu unterstützten Versionen finden Sie im ["NetApp Interoperabilitäts-Matrix-Tool"](#)

Richten Sie Anmeldedaten für benutzerdefinierte SnapCenter-Plug-ins ein

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

Datenbanken oder Windows-Dateisystemen erstellen.

Was Sie brauchen

- Linux-Hosts

Sie müssen Anmeldedaten für die Installation von Plug-ins auf Linux-Hosts einrichten.

Sie müssen die Anmeldedaten für den Root-Benutzer oder für einen Benutzer ohne Root einrichten, der über sudo-Berechtigungen verfügt, um das Plug-in zu installieren und zu starten.

Best Practice: Obwohl Sie nach der Bereitstellung von Hosts und der Installation von Plug-ins Anmeldedaten für Linux erstellen dürfen, empfiehlt es sich, nach dem Hinzufügen von SVMs Anmeldeinformationen zu erstellen, bevor Sie Hosts bereitstellen und Plug-ins installieren.

- Windows Hosts

Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-ins installieren.

Sie müssen die Anmeldedaten mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.

- Benutzerdefinierte Plug-ins-Applikationen

Das Plug-in verwendet die Anmeldeinformationen, die beim Hinzufügen einer Ressource ausgewählt oder erstellt wurden. Wenn eine Ressource während des Datenschutzzvorgangs keine Anmeldeinformationen benötigt, können Sie die Anmeldeinformationen auf **Keine** setzen.

Über diese Aufgabe

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**.

Credential
✕

Provide information for the Credential you want to add

Credential Name

Username

i

Password


Authentication

Linux
▼

Use sudo privileges i

4. Geben Sie auf der Seite Credential die Informationen an, die zum Konfigurieren von Anmeldeinformationen erforderlich sind:

Für dieses Feld...	Tun Sie das...
Name der Anmeldeinformationen	Geben Sie einen Namen für die Anmeldedaten ein.

Für dieses Feld...	Tun Sie das...
Benutzername	<p>Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen.</p> <ul style="list-style-type: none"> • Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe <p>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:</p> <ul style="list-style-type: none"> ◦ <i>NetBIOS\Benutzername</i> ◦ <i>Domain FQDN\Benutzername</i> • Lokaler Administrator (nur für Arbeitsgruppen) <p>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: <i>Username</i></p>
Passwort	Geben Sie das für die Authentifizierung verwendete Passwort ein.
Authentifizierungsmodus	Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten.
Sudo-Berechtigungen verwenden	<p>Aktivieren Sie das Kontrollkästchen Sudo-Berechtigungen verwenden, wenn Sie Anmeldedaten für einen nicht-Root-Benutzer erstellen möchten.</p> <p> Nur für Linux-Benutzer verfügbar.</p>

5. Klicken Sie auf **OK**.

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

Konfigurieren 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 -Effectivelmmediately
3. Erstellen und Konfigurieren des gMSA:
 - a. Erstellen Sie ein Benutzerkonto in folgendem Format:

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

Beispiel:

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

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

Um dies zu tun, führen Sie den folgenden Befehl aus PowerShell:

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

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

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

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. Starten Sie den Host neu.
 - b. Installieren Sie das gMSA auf Ihrem Host, indem Sie den folgenden Befehl über die PowerShell-Eingabeaufforderung ausführen: `Install-AdServiceAccount <gMSA>`
 - c. Überprüfen Sie Ihr gMSA-Konto, indem Sie folgenden Befehl ausführen: `Test-AdServiceAccount <gMSA>`
5. Weisen Sie dem konfigurierten gMSA auf dem Host die Administratorrechte zu.
6. Fügen Sie den Windows-Host hinzu, indem Sie das konfigurierte gMSA-Konto im SnapCenter-Server angeben.

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

Installieren Sie die benutzerdefinierten SnapCenter-Plug-ins

Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts

Sie müssen Hosts über die Seite SnapCenterAdd Host hinzufügen und dann die Plug-in-Pakete installieren. Die Plug-ins werden automatisch auf den Remote-Hosts installiert. Sie können einen Host hinzufügen und die Plug-in-Pakete entweder für einen einzelnen Host oder für einen Cluster installieren.

Was Sie brauchen

- Sie sollten ein Benutzer sein, der einer Rolle zugewiesen wird, die über die Berechtigungen für die Plug-in-Installation und -Deinstallation verfügt, wie z. B. die Rolle „SnapCenter Admin“.
- Stellen Sie sicher, dass der Nachrichtenwarteschlange ausgeführt wird.
- Wenn Sie Group Managed Service Account (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

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


Über diese Aufgabe


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

Wenn Sie Plug-ins auf einem Cluster (WSFC) installieren, werden die Plug-ins auf allen Nodes des Clusters installiert.


Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Überprüfen Sie, ob die Registerkarte **verwaltete Hosts** oben ausgewählt ist.
3. Klicken Sie Auf **Hinzufügen**.
4. Führen Sie auf der Seite Hosts die folgenden Aktionen durch:



Für dieses Feld...	Tun Sie das...
Host-Typ	<p>Wählen Sie den Host-Typ aus:</p> <ul style="list-style-type: none">• Windows• Linux <p> Die benutzerdefinierten Plug-ins können sowohl in Windows als auch in Linux Umgebungen verwendet werden.</p>
Host-Name	<p>Geben Sie den vollständig qualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein.</p> <p>SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den FQDN einzugeben.</p> <p>In Windows-Umgebungen wird die IP-Adresse nur für nicht vertrauenswürdige Domänen-Hosts unterstützt, wenn sie in den FQDN auflöst.</p> <p>Sie können die IP-Adressen oder FQDN eines eigenständigen Hosts eingeben.</p> <p>Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Unterdomäne ist, müssen Sie den FQDN angeben.</p>

Für dieses Feld...	Tun Sie das...
Anmeldedaten	<p>Wählen Sie entweder den von Ihnen erstellten Anmeldeinformationsnamen aus, oder erstellen Sie neue Anmeldedaten.</p> <p>Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Weitere Informationen finden Sie unter Informationen zum Erstellen von Anmeldeinformationen.</p> <p>Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen positionieren.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Der Authentifizierungsmodus für die Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten zum Hinzufügen von Hosts angeben.</p> </div>

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

Für dieses Feld...	Tun Sie das...
Port	<p>Behalten Sie die Standard-Port-Nummer oder geben Sie die Port-Nummer an.</p> <p>Die Standardanschlussnummer ist 8145. Wenn der SnapCenter-Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Wenn Sie die Plug-ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.</p> </div>

Für dieses Feld...	Tun Sie das...
Installationspfad	<p>Die benutzerdefinierten Plug-ins können entweder auf einem Windows-System oder auf einem Linux-System installiert werden.</p> <ul style="list-style-type: none"> • Der Standardpfad für das SnapCenter Plug-ins-Paket für Windows ist C:\Programme\NetApp\SnapCenter. <p>Optional können Sie den Pfad anpassen.</p> <ul style="list-style-type: none"> • Für das SnapCenter Plug-ins-Paket für Linux lautet der Standardpfad: /Opt/NetApp/snapcenter. <p>Optional können Sie den Pfad anpassen.</p> <ul style="list-style-type: none"> • Für die benutzerdefinierten SnapCenter Plug-ins: <ul style="list-style-type: none"> i. Klicken Sie im Abschnitt Benutzerdefinierte Plug-ins auf Durchsuchen und wählen Sie den Ordner mit dem gezippten benutzerdefinierten Plug-in aus. <p>Der Ordner mit gezippten Daten enthält den benutzerdefinierten Plug-in-Code und die XML-Datei Deskriptor.</p> <p>Navigieren Sie zum Storage Plug-in zu <i>C:\ProgramData\NetApp\SnapCenter\Package Repository</i>, und wählen Sie aus <i>Storage.zip</i> Ordner.</p> ii. Klicken Sie Auf Upload. <p>Die XML-Datei Deskriptor im Ordner gezipptes benutzerdefiniertes Plug-in wird vor dem Hochladen des Pakets validiert.</p> <p>Die benutzerdefinierten Plug-ins, die auf den SnapCenter-Server hochgeladen werden, werden aufgelistet.</p> <p>Wenn Sie MySQL oder DB2 Applikationen managen möchten, können Sie die benutzerdefinierten MySQL und DB2 Plug-ins verwenden, die von NetApp zur Verfügung gestellt werden. Die benutzerdefinierten MySQL und DB2 Plug-ins sind im verfügbar "NetApp Automation Store"</p>

Für dieses Feld...	Tun Sie das...
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	<p>Aktivieren Sie für Windows-Host dieses Kontrollkästchen, wenn Sie die Plug-in-Dienste über das Group Managed Service Account (gMSA) ausführen möchten.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> Geben Sie den gMSA-Namen in folgendem Format an: Domainname\AccountName€.</p> <p> GSSA wird nur für den SnapCenter-Plug-in für Windows-Dienst als Anmelde-Dienstkonto verwendet.</p> </div>

7. Klicken Sie Auf **Absenden**.

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

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



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

8. Wenn der Hosttyp Linux ist, überprüfen Sie den Fingerabdruck und klicken Sie dann auf **Bestätigen und Senden**.



Eine Fingerabdruck-Verifizierung ist erforderlich, auch wenn zuvor derselbe Host zu SnapCenter hinzugefügt wurde und der Fingerabdruck bestätigt wurde.

9. Überwachen Sie den Installationsfortschritt.

Die installationsspezifischen Log-Dateien befinden sich unter /Custom_Location/snapcenter/logs.

Installieren Sie SnapCenter Plug-in-Pakete für Linux oder Windows auf mehreren Remote Hosts mithilfe von Cmdlets

Sie können die SnapCenter-Plug-in-Pakete für Linux oder Windows gleichzeitig auf mehreren Hosts installieren, indem Sie das Cmdlet "Install-SmHostPackage PowerShell" verwenden.

Was Sie brauchen

Der Benutzer, der einen Host hinzugefügt hat, sollte über die Administratorrechte auf dem Host verfügen.

Schritte

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

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

Sie können die Option `-skipprecheck` verwenden, wenn Sie die Plug-ins manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen erfüllt, um das Plug-in zu installieren.

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

Installieren Sie die benutzerdefinierten SnapCenter-Plug-ins auf Linux-Hosts über die Befehlszeilenschnittstelle

Sie sollten die benutzerdefinierten SnapCenter-Plug-ins über die SnapCenter-Benutzeroberfläche (UI) installieren. Wenn Ihre Umgebung die Remote-Installation des Plug-ins über die SnapCenter-Benutzeroberfläche nicht zulässt, können Sie die benutzerdefinierten Plug-ins entweder im Konsolenmodus oder im Ruhemodus mithilfe der Befehlszeilenschnittstelle (CLI) installieren.

Schritte

1. Kopieren Sie das SnapCenter Plug-ins Paket für die Linux Installationsdatei (`snapcenter_linux_host_Plugin.bin`) von `C:\ProgramData\NetApp\SnapCenter\Paket-Repository` auf den Host, auf dem Sie die benutzerdefinierten Plug-ins installieren möchten.

Sie können von dem Host, auf dem der SnapCenter-Server installiert ist, auf diesen Pfad zugreifen.

2. Navigieren Sie in der Eingabeaufforderung zum Verzeichnis, in dem Sie die Installationsdatei kopiert haben.
3. Installieren Sie das Plug-in:

```
path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address  
-DSERVER_HTTPS_PORT=port_number_for_server
```

- -DPORT gibt den HTTPS-Kommunikationsport SMCore an.
- -DSERVER_IP gibt die IP-Adresse des SnapCenter-Servers an.
- -DSERVER_HTTPS_PORT gibt den HTTPS-Port des SnapCenter-Servers an.
- -DUSER_INSTALL_dir gibt das Verzeichnis an, in dem das SnapCenter-Plug-ins-Paket für Linux installiert werden soll.
- DINSTALL_LOG_NAME gibt den Namen der Protokolldatei an.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Fügen Sie den Host mit dem Cmdlet "Add-Smhost" und den erforderlichen Parametern zum SnapCenter-Server hinzu.

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

5. Melden Sie sich bei SnapCenter an und laden Sie das benutzerdefinierte Plug-in über die UI oder mithilfe von PowerShell Cmdlets hoch.

Sie können das benutzerdefinierte Plug-in über die Benutzeroberfläche hochladen. Verwenden Sie dazu die Verweis "[Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts](#)" Abschnitt.

Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten weitere Informationen zu PowerShell Cmdlets.






["SnapCenter Software Cmdlet Referenzhandbuch"](#).

Überwachen Sie den Status der Installation benutzerdefinierter Plug-ins

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 vor dem Erwerb des Zertifikats das Feld alternativer Antragstellername (SAN) ausfüllen. 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"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

Konfigurieren Sie das CA-Zertifikat für den benutzerdefinierten SnapCenter-Plug-ins-Dienst auf dem Linux-Host

Sie sollten das Passwort des benutzerdefinierten Plug-ins-Schlüsselspeichers und dessen Zertifikat verwalten, das CA-Zertifikat konfigurieren, Root- oder Zwischenzertifikate für den benutzerdefinierten Plug-ins-Vertrauensspeicher konfigurieren und das CA-signierte Schlüsselpaar für den benutzerdefinierten Plug-ins-Vertrauensspeicher mit dem SnapCenter-Dienst Benutzerdefinierte Plug-ins konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Benutzerdefinierte Plug-ins verwenden die Datei 'keystore.jks', die sich unter */opt/NetApp/snapcenter/scc/etc* sowohl als Vertrauensspeicher als auch als Schlüsselspeicher befindet.

Passwort für benutzerdefinierten Plug-in-Schlüsselspeicher und Alias des verwendeten CA-signierten Schlüsselpaares verwalten

Schritte

1. Sie können benutzerdefinierte Plug-in Schlüsselspeicher Standardpasswort aus benutzerdefinierten Plug-in Agent Eigenschaftsdatei abrufen.

Es ist der Wert, der dem Schlüssel 'KEYSTORE_PASS' entspricht.

2. Ändern Sie das Schlüsselspeicher-Passwort:

```
keytool -storepasswd -keystore keystore.jks
. Ändern Sie das Kennwort für alle Aliase privater Schlüsseleinträge im Schlüsselspeicher auf dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Aktualisieren Sie das gleiche für den Schlüssel KEYSTORE_PASS in *agent.properties* Datei.

3. Starten Sie den Dienst neu, nachdem Sie das Passwort geändert haben.



Das Kennwort für den benutzerdefinierten Plug-in-Schlüsselspeicher und für alle zugeordneten Alias-Passwörter des privaten Schlüssels sollte gleich sein.

Konfigurieren Sie Root- oder Zwischenzertifikate in einem benutzerdefinierten Plug-in Trust-Store

Sie sollten die Stammzertifikate oder Zwischenzertifikate ohne privaten Schlüssel als benutzerdefinierten Plug-in-Vertrauensspeicher konfigurieren.

Schritte

1. Navigieren Sie zu dem Ordner mit dem benutzerdefinierten Plug-in-Keystore:
/Opt/NetApp/snapcenter/scc/etc

2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie ein Stammzertifikat oder ein Zwischenzertifikat hinzu:

```
keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Starten Sie den Dienst neu, nachdem Sie die Stammzertifikate oder
Zwischenzertifikate in einen benutzerdefinierten Plug-in Trust-Store
konfiguriert haben.
```



Sie sollten das Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate hinzufügen.

Konfigurieren Sie das CA-signierte Schlüsselpaar in einem benutzerdefinierten Plug-in-Vertrauensspeicher

Sie sollten das CA-signierte Schlüsselpaar für den benutzerdefinierten Plug-in Trust-Store konfigurieren.

Schritte

1. Navigieren Sie zum Ordner mit dem benutzerdefinierten Plug-in keystore /opt/NetApp/snapcenter/scc/etc.
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen Schlüssel hinzu.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

```
keytool -list -v -keystore keystore.jks
```

6. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für das CA-Zertifikat in das Schlüsselspeicher-Passwort.

Das benutzerdefinierte Standard-Plug-in-Schlüsselspeicher-Passwort ist der Wert der SCHLÜSSELDATEI KEYSTORE_PASS in agent.properties.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

. Wenn der Alias-Name im CA-Zertifikat lang ist und Leerzeichen oder Sonderzeichen enthält („*“, „/“), ändern Sie den Alias-Namen in einen einfachen Namen:

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. Konfigurieren Sie den Alias-Namen aus dem CA-Zertifikat in der Datei `agent.properties`.

Diesen Wert mit dem Schlüssel `SCC_CERTIFICATE_ALIAS` aktualisieren.

8. Starten Sie den Dienst neu, nachdem Sie das CA-signierte Schlüsselpaar in einen benutzerdefinierten Plug-in Trust-Store konfiguriert haben.

Konfigurieren der Zertifikatsperrliste (CRL) für benutzerdefinierte SnapCenter-Plug-ins

Über diese Aufgabe

- Benutzerdefinierte SnapCenter-Plug-ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für SnapCenter Custom Plug-ins ist ' `opt/NetApp/snapcenter/scc/etc/crl`'.

Schritte

1. Sie können das Standardverzeichnis in der Datei `agent.properties` mit dem Schlüssel `CRL_PATH` ändern und aktualisieren.

Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren. Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Konfigurieren Sie das CA-Zertifikat für den benutzerdefinierten SnapCenter-Plug-ins-Dienst auf Windows-Host

Sie sollten das Passwort des benutzerdefinierten Plug-ins-Schlüsselspeichers und dessen Zertifikat verwalten, das CA-Zertifikat konfigurieren, Root- oder Zwischenzertifikate für den benutzerdefinierten Plug-ins-Vertrauensspeicher konfigurieren und das CA-signierte Schlüsselpaar für den benutzerdefinierten Plug-ins-Vertrauensspeicher mit dem SnapCenter-Dienst Benutzerdefinierte Plug-ins konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Benutzerdefinierte Plug-ins verwenden die Datei `keystore.jks`, die sich unter `C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc` befindet, sowohl als Vertrauensspeicher als auch als Schlüsselspeicher.

Passwort für benutzerdefinierten Plug-in-Schlüsselspeicher und Alias des verwendeten CA-signierten Schlüsselpaars verwalten

Schritte

1. Sie können benutzerdefinierte Plug-in Schlüsselspeicher Standardpasswort aus benutzerdefinierten Plug-in Agent Eigenschaftsdatei abrufen.

Es ist der Wert, der dem Schlüssel *KEYSTORE_PASS* entspricht.

2. Ändern Sie das Schlüsselspeicher-Passwort:

```
Keytool -storepasswd -keystore keystore.jks
```



Wenn der Befehl "keytool" in der Windows-Eingabeaufforderung nicht erkannt wird, ersetzen Sie den Befehl keytool mit seinem vollständigen Pfad.

```
C:\Programme\Java\<jdk_Version>\bin\keytool.exe -storepasswd -keystore keystore.jks
```

3. Ändern Sie das Kennwort für alle Aliase privater Schlüsseleinträge im Schlüsselspeicher auf dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:

```
Keytool -keypasswd -alias „alias_Name_in_cert“ -keystore keystore.jks
```

Aktualisieren Sie das gleiche für den Schlüssel *KEYSTORE_PASS* in *agent.properties* Datei.

4. Starten Sie den Dienst neu, nachdem Sie das Passwort geändert haben.



Das Kennwort für den benutzerdefinierten Plug-in-Schlüsselspeicher und für alle zugeordneten Alias-Passwörter des privaten Schlüssels sollte gleich sein.

Konfigurieren Sie Root- oder Zwischenzertifikate in einem benutzerdefinierten Plug-in Trust-Store

Sie sollten die Stammzertifikate oder Zwischenzertifikate ohne privaten Schlüssel als benutzerdefinierten Plug-in-Vertrauensspeicher konfigurieren.

Schritte

1. Navigieren Sie zu dem Ordner mit dem benutzerdefinierten Plug-in-Keystore *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*

2. Suchen Sie die Datei 'keystore.jks'.

3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

```
Keytool -list -V -keystore keystore.jks
```

4. Fügen Sie ein Stammzertifikat oder ein Zwischenzertifikat hinzu:

```
Keytool -Import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. Starten Sie den Dienst neu, nachdem Sie die Stammzertifikate oder Zwischenzertifikate in einen benutzerdefinierten Plug-in Trust-Store konfiguriert haben.



Sie sollten das Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate hinzufügen.

Konfigurieren Sie das CA-signierte Schlüsselpaar in einem benutzerdefinierten Plug-in-Vertrauensspeicher

Sie sollten das CA-signierte Schlüsselpaar für den benutzerdefinierten Plug-in Trust-Store konfigurieren.

Schritte

1. Navigieren Sie zum Ordner mit dem benutzerdefinierten Plug-in Schlüsselspeicher
`C:\Programme\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc`
2. Suchen Sie die Datei `keystore.jks`.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

```
Keytool -list -V -keystore keystore.jks
```

4. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen Schlüssel hinzu.

```
Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

```
Keytool -list -V -keystore keystore.jks
```

6. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für das CA-Zertifikat in das Schlüsselspeicher-Passwort.

Das benutzerdefinierte Standard-Plug-in-Schlüsselspeicher-Passwort ist der Wert der SCHLÜSSELDATEI KEYSTORE_PASS in `agent.properties`.

```
Keytool -keypasswd -alias „alias_Name_in_CA_cert“ -keystore keystore.jks
```

8. Konfigurieren Sie den Alias-Namen aus dem CA-Zertifikat in der Datei `agent.properties`.

Diesen Wert mit dem Schlüssel `SCC_CERTIFICATE_ALIAS` aktualisieren.

9. Starten Sie den Dienst neu, nachdem Sie das CA-signierte Schlüsselpaar in einen benutzerdefinierten Plug-in Trust-Store konfiguriert haben.

Konfigurieren der Zertifikatsperlliste (CRL) für benutzerdefinierte SnapCenter-Plug-ins

Über diese Aufgabe

- Informationen zum Herunterladen der neuesten CRL-Datei für das zugehörige CA-Zertifikat finden Sie unter "[Aktualisieren der Listendatei für Zertifikatsperllisten im SnapCenter CA-Zertifikat](#)".
- Benutzerdefinierte SnapCenter-Plug-ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für benutzerdefinierte SnapCenter Plug-ins ist `'C:\Programme\NetApp\SnapCenter\SnapCenter Plug-in Creator\ etc\crl'`.

Schritte

1. Sie können das Standardverzeichnis in der Datei *agent.properties* mit dem Schlüssel `CRL_PATH` ändern und aktualisieren.
2. Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren.

Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Aktivieren Sie CA-Zertifikate für Plug-ins

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

Was Sie brauchen

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





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

Schritte

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

Nach Ihrer Beendigung

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

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



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

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.