



Installieren Sie das SnapCenter-Plug-in für Unix-Dateisysteme

SnapCenter Software 5.0

NetApp
July 18, 2024

Inhalt

- Installieren Sie das SnapCenter-Plug-in für Unix-Dateisysteme 1
 - Voraussetzungen für das Hinzufügen von Hosts und das Installieren von Plug-ins Package für Linux 1
 - Fügen Sie Hosts hinzu und installieren Sie Plug-ins Package for Linux mithilfe der GUI 2
 - Konfigurieren Sie den SnapCenter-Plug-in-Loader-Dienst 5
 - Konfigurieren Sie das CA-Zertifikat mit dem SnapCenter Plug-in Loader (SPL)-Service auf dem Linux-Host 9
 - Aktivieren Sie CA-Zertifikate für Plug-ins 12

Installieren Sie das SnapCenter-Plug-in für Unix-Dateisysteme

Voraussetzungen für das Hinzufügen von Hosts und das Installieren von Plug-ins Package für Linux

Bevor Sie einen Host hinzufügen und das Plug-in-Paket für Linux installieren, müssen Sie alle Anforderungen erfüllen.

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie können entweder die passwortbasierte Authentifizierung für den Root- oder nicht-Root-Benutzer oder die SSH-Schlüsselauthentifizierung verwenden.

Das SnapCenter-Plug-in für Unix-Dateisysteme kann von einem Benutzer installiert werden, der kein Root-Benutzer ist. Sie sollten jedoch die sudo-Berechtigungen für den nicht-Root-Benutzer konfigurieren, um den Plug-in-Prozess zu installieren und zu starten. Nach der Installation des Plug-ins werden die Prozesse als effektiver nicht-Root-Benutzer ausgeführt.

- Anmeldedaten mit Authentifizierungsmodus als Linux für den Installationsbenutzer erstellen.
- Sie müssen Java 1.8.x oder Java 11, 64-Bit, auf Ihrem Linux-Host installiert haben.



Stellen Sie sicher, dass Sie nur die zertifizierte Version VON JAVA 11 auf dem Linux-Host installiert haben.



Informationen zum Herunterladen von JAVA finden Sie unter: "[Java-Downloads für alle Betriebssysteme](#)"

- Sie sollten **bash** als Standard-Shell für die Plug-in-Installation haben.

Linux Host-Anforderungen

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	2 GB

Element	Anforderungen
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	<p>2 GB</p> <p> 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.</p>
Erforderliche Softwarepakete	<ul style="list-style-type: none"> • Java 1.8.x (64 Bit) Oracle Java und OpenJDK • Java 11 (64 Bit) Oracle Java und OpenJDK <p> Stellen Sie sicher, dass Sie nur die zertifizierte Version VON JAVA 11 auf dem Linux-Host installiert haben.</p> <p>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.</p>

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

Fügen Sie Hosts hinzu und installieren Sie Plug-ins Package for Linux mithilfe der GUI


Sie können die Seite Host hinzufügen verwenden, um Hosts hinzuzufügen und anschließend das SnapCenter-Plug-ins-Paket für Linux zu installieren. Die Plug-ins werden automatisch auf den Remote-Hosts 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	Wählen Sie Linux als Hosttyp aus.
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>Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Unterdomäne ist, müssen Sie den FQDN angeben.</p>
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 data-bbox="873 1234 928 1289" style="border: 1px solid gray; border-radius: 50%; width: 34px; height: 34px; display: flex; align-items: center; justify-content: center; margin: 10px 0;"> i </div> <p style="margin-left: 20px;">Der Authentifizierungsmodus für die Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten zum Hinzufügen von Hosts angeben.</p>

5. Wählen Sie im Abschnitt zu installierende Plug-ins auswählen **Unix-Dateisysteme** aus.
6. (Optional) Klicken Sie Auf **Weitere Optionen**.

Für dieses Feld...	Tun Sie das...
Port	<p>Behalten Sie die Standard-Port-Nummer bei 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>
Installationspfad	<p>Der Standardpfad ist <i>/opt/NetApp/snapcenter</i>.</p> <p>Optional können Sie den Pfad anpassen. Wenn Sie den benutzerdefinierten Pfad verwenden, stellen Sie sicher, dass der Standardinhalt der Sudoers mit dem benutzerdefinierten Pfad aktualisiert wird.</p>
Überspringen Sie optionale Prüfungen vor der Installation	<p>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.</p>

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.



Das Precheck-Skript überprüft den Firewall-Status des Plug-in-Ports nicht, wenn er in den Regeln für die Ablehnung der Firewall angegeben ist.

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:\Program Files\NetApp\SnapCenter WebApp* aktualisieren, um die Standardwerte zu ändern. Wenn der Fehler mit anderen Parametern zusammenhängt, sollten Sie das Problem beheben.



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

8. Überprüfen Sie den Fingerabdruck, und klicken Sie dann auf **Bestätigen und Senden**.



SnapCenter unterstützt keinen ECDSA-Algorithmus.



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`.

Ergebnis

Alle auf dem Host gemounteten Dateisysteme werden automatisch erkannt und auf der Seite „Ressourcen“ angezeigt. Wenn nichts angezeigt wird, klicken Sie auf **Ressourcen aktualisieren**.

Überwachung des Installationsstatus

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
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Um die Liste auf der Seite **Jobs** so zu filtern, dass nur Plug-in-Installationsvorgänge aufgelistet 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**.
 - 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 **Job Details** auf **Protokolle anzeigen**.

Konfigurieren Sie den SnapCenter-Plug-in-Loader-Dienst

Der SnapCenter-Plug-in-Loader-Dienst lädt das Plug-in-Paket, damit Linux mit dem SnapCenter-Server interagieren kann. Der SnapCenter-Plug-in-Loader-Dienst wird

installiert, wenn Sie das SnapCenter-Plug-ins-Paket für Linux installieren.



Über diese Aufgabe

Nach der Installation des SnapCenter-Plug-ins-Pakets für Linux wird der SnapCenter-Plug-in-Loader-Dienst automatisch gestartet. Wenn der SnapCenter-Plug-in-Loader-Dienst nicht automatisch gestartet wird, sollten Sie Folgendes tun:

- Stellen Sie sicher, dass das Verzeichnis, in dem das Plug-in ausgeführt wird, nicht gelöscht wird
- Erhöhen Sie den Speicherplatz, der der Java Virtual Machine zugewiesen ist

Die Datei `spl.properties` befindet sich unter `/Custom_Location/NetApp/snapcenter/spl/etc/` und enthält die folgenden Parameter: Diesen Parametern werden Standardwerte zugewiesen.

Parametername	Beschreibung
PROTOKOLL_LEVEL	Zeigt die unterstützten Protokollebenen an. Mögliche Werte sind TRACE, DEBUG, INFO, WARN, FEHLER, Und TÖDLICH.
SPL_PROTOKOLL	Zeigt das von SnapCenter Plug-in Loader unterstützte Protokoll an. Nur das HTTPS-Protokoll wird unterstützt. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.
SNAPCENTER_SERVER_PROTOCOL	Zeigt das von SnapCenter-Server unterstützte Protokoll an. Nur das HTTPS-Protokoll wird unterstützt. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.
SKIP_JAVAHOME_UPDATE	Standardmäßig erkennt der SPL-Dienst den java-Pfad und aktualisiert DEN JAVA_HOME-Parameter. Daher ist der Standardwert AUF FALSE gesetzt. Sie können auf „TRUE“ setzen, wenn Sie das Standardverhalten deaktivieren und den java-Pfad manuell korrigieren möchten.
SPL_KEYSTORE_PASS	Zeigt das Kennwort der Schlüsselspeicherdatei an. Sie können diesen Wert nur ändern, wenn Sie das Passwort ändern oder eine neue Schlüsselspeicherdatei erstellen.

Parametername	Beschreibung
SPL_PORT	<p>Zeigt die Portnummer an, auf der der SnapCenter-Plug-in-Loader ausgeführt wird.</p> <p>Sie können den Wert hinzufügen, wenn der Standardwert fehlt.</p> <div style="display: flex; align-items: center;">  <p>Nach der Installation der Plug-ins sollten Sie den Wert nicht ändern.</p> </div>
SNAPCENTER_SERVER_HOST	<p>Zeigt die IP-Adresse oder den Hostnamen des SnapCenter-Servers an.</p>
SPL_KEYSTORE_PATH	<p>Zeigt den absoluten Pfad der Schlüsselspeicherdatei an.</p>
SNAPCENTER_SERVER_PORT	<p>Zeigt die Portnummer an, auf der der SnapCenter-Server ausgeführt wird.</p>
„LOGS_MAX_COUNT“	<p>Zeigt die Anzahl der SnapCenter-Plug-in-Loader-Protokolldateien an, die im Ordner <i>/Custom_location/snapcenter/spl/logs</i> aufbewahrt werden.</p> <p>Der Standardwert ist 5000. Wenn der Zähler größer als der angegebene Wert ist, werden die letzten 5000 geänderten Dateien beibehalten. Die Prüfung auf die Anzahl der Dateien erfolgt automatisch alle 24 Stunden ab dem Start des SnapCenter Plug-in Loader-Dienstes.</p> <div style="display: flex; align-items: center;">  <p>Wenn Sie die Datei <i>spl.properties</i> manuell löschen, wird die Anzahl der zu behaltenden Dateien auf 9999 festgelegt.</p> </div>
JAVA_HOME	<p>Zeigt den absoluten Verzeichnispfad des JAVA_HOME an, der zum Starten des SPL-Dienstes verwendet wird.</p> <p>Dieser Pfad wird während der Installation und im Rahmen des Startens von SPL festgelegt.</p>
LOG_MAX_SIZE	<p>Zeigt die maximale Größe der Job-Log-Datei an.</p> <p>Sobald die maximale Größe erreicht ist, wird die Protokolldatei gezippt und die Protokolle werden in die neue Datei dieses Jobs geschrieben.</p>

Parametername	Beschreibung
BEIBEHALTEN_LOGS_OF_LAST_DAYS	Zeigt die Anzahl der Tage an, bis zu denen die Protokolle aufbewahrt werden.
ENABLE_CERTIFICATE_VALIDATION	<p>Zeigt true an, wenn die Zertifikatvalidierung für den Host aktiviert ist.</p> <p>Sie können diesen Parameter entweder aktivieren oder deaktivieren, indem Sie den spl.properties bearbeiten oder den SnapCenter GUI oder Cmdlet verwenden.</p>

Wenn einer dieser Parameter dem Standardwert nicht zugewiesen ist oder Sie den Wert zuweisen oder ändern möchten, können Sie die Datei spl.properties ändern. Sie können auch die Datei spl.properties überprüfen und die Datei bearbeiten, um Probleme zu beheben, die mit den Werten, die den Parametern zugeordnet sind, zusammenhängen. Nachdem Sie die Datei spl.properties geändert haben, sollten Sie den SnapCenter-Plug-in-Loader-Dienst neu starten.

Schritte

1. Führen Sie bei Bedarf eine der folgenden Aktionen aus:

- Starten Sie den SnapCenter-Plug-in-Loader-Dienst:
 - Führen Sie als Root-Benutzer Folgendes aus:

```
/custom_location/NetApp/snapcenter/spl/bin/spl start
```
 - Führen Sie als Benutzer ohne Root Folgendes aus: sudo

```
/custom_location/NetApp/snapcenter/spl/bin/spl start
```
- Stoppen Sie den SnapCenter-Plug-in-Loader-Dienst:
 - Führen Sie als Root-Benutzer Folgendes aus:

```
/custom_location/NetApp/snapcenter/spl/bin/spl stop
```
 - Führen Sie als Benutzer ohne Root Folgendes aus: sudo

```
/custom_location/NetApp/snapcenter/spl/bin/spl stop
```



Sie können die Option -Force mit dem Befehl STOP verwenden, um den SnapCenter Plug-in Loader Dienst nachdrücklich zu stoppen. Vor diesem Verfahren sollten Sie jedoch Vorsicht walten lassen, da auch die bestehenden Vorgänge beendet werden.

- Starten Sie den SnapCenter-Plug-in-Loader-Dienst neu:
 - Führen Sie als Root-Benutzer Folgendes aus:

```
/custom_location/NetApp/snapcenter/spl/bin/spl restart
```
 - Führen Sie als Benutzer ohne Root Folgendes aus: sudo

```
/custom_location/NetApp/snapcenter/spl/bin/spl restart
```
- Suchen Sie den Status des SnapCenter-Plug-in-Loader-Dienstes:
 - Führen Sie als Root-Benutzer Folgendes aus:

```
/custom_location/NetApp/snapcenter/spl/bin/spl status
```

- Führen Sie als Benutzer ohne Root Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
- Finden Sie die Änderung im SnapCenter-Plug-in-Loader-Dienst:
 - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
 - Führen Sie als Benutzer ohne Root Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Konfigurieren Sie das CA-Zertifikat mit dem SnapCenter Plug-in Loader (SPL)-Service auf dem Linux-Host

Sie sollten das Passwort von SPL Keystore und dessen Zertifikat verwalten, das CA-Zertifikat konfigurieren, Root- oder Zwischenzertifikate für SPL Trust-Store konfigurieren und das CA-signierte Schlüsselpaar für SPL Trust-Store mit dem SnapCenter Plug-in Loader Service konfigurieren, um das installierte digitale Zertifikat zu aktivieren.



SPL verwendet die Datei 'keystore.jks', die sich bei '/var/opt/snapcenter/spl/etc' sowohl als Vertrauensspeicher als auch als Schlüsselspeicher befindet.

Passwort für SPL-Schlüsselspeicher und Alias des verwendeten CA-signierten Schlüsselpaares verwalten

Schritte

1. Sie können SPL Schlüsselspeicher Standardpasswort aus SPL Eigenschaftsdatei abrufen.

Dieser Wert entspricht dem Schlüssel 'SPL_KEYSTORE_PASS'.

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>" -keystore keystore.jks
```

Aktualisieren Sie das gleiche für den Schlüssel SPL_KEYSTORE_PASS in der Datei spl.properties.

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



Passwort für SPL-Schlüsselspeicher und für alle zugeordneten Alias-Passwort des privaten Schlüssels sollte gleich sein.

Konfigurieren Sie Root- oder Zwischenzertifikate in SPL Trust-Store

Sie sollten die Stammzertifikate oder Zwischenzertifikate ohne privaten Schlüssel in den SPL Trust-Store konfigurieren.

Schritte

1. Navigieren Sie zum Ordner mit dem SPL-Schlüsselspeicher: `/var/opt/snapcenter/spl/etc`.
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

```
keytool -list -v -keystore keystore.jks  
. Fügen Sie ein Stammzertifikat oder ein Zwischenzertifikat hinzu:
```

```
keytool -import -trustcacerts -alias  
<AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore  
keystore.jks  
. Starten Sie den Dienst neu, nachdem Sie die Stammzertifikate oder  
Zwischenzertifikate in den SPL Trust-Store konfiguriert haben.
```



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

Konfigurieren Sie das CA-signierte Schlüsselpaar für SPL Trust-Store

Sie sollten das CA-signierte Schlüsselpaar für den SPL Trust-Store konfigurieren.

Schritte

1. Navigieren Sie zu dem Ordner, der den SPL-Schlüsselspeicher `/var/opt/snapcenter/spl/etc`. Enthält
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

```
keytool -list -v -keystore keystore.jks  
. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen  
Schlüssel hinzu.
```

```
keytool -importkeystore -srckeystore <CertificatePathToImport>  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS  
. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.
```

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

. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.

. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für das CA-Zertifikat in das Schlüsselspeicher-Passwort.

Das Standard-SPL-Schlüsselspeicherkenwort ist der Wert des Schlüssels `SPL_KEYSTORE_PASS` in der Datei `spl.properties`.

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -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 "<OriginalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks
```

. Konfigurieren Sie den Alias-Namen aus dem Schlüsselspeicher, der sich in der Datei `spl.properties` befindet.

Diesen Wert mit dem Schlüssel `SPL_CERTIFICATE_ALIAS` aktualisieren.

4. Starten Sie den Dienst neu, nachdem Sie das CA-signierte Schlüsselpaar auf SPL Trust-Store konfiguriert haben.

Konfigurieren der Zertifikatsperrliste (CRL) für SPL

Sie sollten die CRL für SPL konfigurieren

Über diese Aufgabe

- SPL wird nach den CRL-Dateien in einem vorkonfigurierten Verzeichnis suchen.
- Das Standardverzeichnis für die CRL-Dateien für SPL lautet `/var/opt/snapcenter/spl/etc/crl`.

Schritte

1. Sie können das Standardverzeichnis in der Datei `spl.properties` mit dem Schlüssel `SPL_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.

Bevor Sie beginnen

- 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**.

Nachdem Sie fertig sind

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.

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.