Konfigurieren Sie die zertifikatbasierte Authentifizierung

SnapCenter Software 4.9

NetApp
March 20, 2024

Inhalt

Konfigurieren Sie die zertifikatbasierte Authentifizierung

Exportieren Sie Zertifikate der Zertifizierungsstelle (CA) vom SnapCenter-Server

Sie sollten die CA-Zertifikate über die Microsoft Management Console (MMC) vom SnapCenter-Server auf die Plug-in-Hosts exportieren.

Bevor Sie beginnen

Sie sollten die bidirektionale SSL-Konfiguration vorgenommen haben.

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 Fenster Zertifikate Snap-in die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenstamm** > **Zertifikate - Lokaler Computer** > **Persönlich** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf das beschaffte CA-Zertifikat, das für den SnapCenter-Server verwendet wird, und wählen Sie dann **Alle Aufgaben** > **Export** aus, um den Export-Assistenten zu starten.
6. Führen Sie die folgenden Aktionen im Assistenten aus.

Für diese Option…	Gehen Sie wie folgt vor…
Privaten Schlüssel Exportieren	Wählen Sie **Nein, exportieren Sie den privaten Schlüssel nicht**, und klicken Sie dann auf **Weiter**.
Dateiformat Exportieren	Klicken Sie Auf **Weiter**.
Dateiname	Klicken Sie auf **Browse** und geben Sie den Dateipfad an, um das Zertifikat zu speichern, und klicken Sie auf **Weiter**.
Assistent zum Exportieren von Zertifikaten abschließen	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Export zu starten.

Die zertifikatbasierte Authentifizierung wird für SnapCenter HA-Konfigurationen und das SnapCenter Plug-in für VMware vSphere nicht unterstützt.

Zertifikat der Zertifizierungsstelle (CA) auf die Windows-Plug-in-Hosts importieren

Um das exportierte SnapCenter-Server-CA-Zertifikat zu verwenden, sollten Sie das zugehörige Zertifikat über die Microsoft-Managementkonsole (MMC) auf die SnapCenter-Windows-Plug-in-Hosts 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 Fenster Zertifikate Snap-in die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenstamm** > **Zertifikate - Lokaler Computer** > **Persönlich** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Personal“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Import-Assistenten zu starten.
6. Führen Sie die folgenden Aktionen im Assistenten aus.

Für diese Option…	Gehen Sie wie folgt vor…
Speicherort Des Geschäfts	Klicken Sie Auf **Weiter**.
Zu importierende Datei	Wählen Sie das SnapCenter-Serverzertifikat aus, das mit der Erweiterung .cer endet.
Zertifikatspeicher	Klicken Sie Auf **Weiter**.
Assistent zum Exportieren von Zertifikaten abschließen	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

Importieren Sie das CA-Zertifikat in die UNIX-Host-Plug-ins, und konfigurieren Sie Root- oder Zwischenzertifikate in den SPL-Trust-Store

Importieren Sie das CA-Zertifikat auf die UNIX-Plug-in-Hosts

Sie sollten das CA-Zertifikat auf die UNIX-Plug-in-Hosts importieren.

Über diese Aufgabe

- Sie können das Kennwort für den SPL-Keystore und den Alias des CA-Schlüsselpaars verwalten, das gerade verwendet wird.
- Das Passwort für den SPL-Keystore und für das zugehörige Alias-Passwort des privaten Schlüssels muss

identisch sein.

Schritte

1. Sie können SPL Schlüsselspeicher Standardpasswort aus SPL Eigenschaftsdatei abrufen. Es ist der Wert, der dem Schlüssel entspricht `SPL_KEYSTORE_PASS`.
2. Ändern Sie das Schlüsselspeicher-Passwort: `$ keytool -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>" -keystore keystore.jks`
4. Aktualisieren Sie das gleiche für den Schlüssel SPL_KEYSTORE_PASS in `spl.properties` Datei:
5. Starten Sie den Dienst neu, nachdem Sie das Passwort geändert haben.

Konfigurieren Sie Root- oder Zwischenzertifikate in SPL Trust-Store

Sie sollten die Stammzertifikate oder Zwischenzertifikate für den SPL-Vertrauensspeicher konfigurieren. Sie sollten das Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate hinzufügen.

Schritte

1. Navigieren Sie zu dem Ordner, der den SPL-Keystore enthält: `/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`
4. Fügen Sie ein Stammzertifikat oder ein Zwischenzertifikat hinzu: `$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. Starten Sie den Dienst neu, nachdem Sie die Stammzertifikate oder Zwischenzertifikate in den SPL Trust-Store konfiguriert haben.

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

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

Schritte

1. Navigieren Sie zu dem Ordner, der den SPL-Keystore enthält `/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`
4. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen Schlüssel hinzu. `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -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.

   Standard-SPL-Keystore-Kennwort ist der Wert des Schlüssels SPL_KEYSTORE_PASS in `spl.properties` Datei:

   ```
   $ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
   ```

8. 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 "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
9. Konfigurieren Sie den Aliasnamen aus dem Schlüsselspeicher in `spl.properties` Datei: Diesen Wert mit dem Schlüssel SPL_CERTIFICATE_ALIAS aktualisieren.
10. Starten Sie den Dienst neu, nachdem Sie das CA-signierte Schlüsselpaar auf SPL Trust-Store konfiguriert haben.

Aktivieren Sie die zertifikatbasierte Authentifizierung

Führen Sie das folgende PowerShell-Cmdlet aus, um die zertifikatbasierte Authentifizierung für SnapCenter Server und die Windows Plug-in-Hosts zu aktivieren. Bei Linux-Plug-in-Hosts wird die zertifikatbasierte Authentifizierung aktiviert, wenn Sie die bidirektionale SSL-Funktion aktivieren.

- So aktivieren Sie die clientzertifikatbasierte Authentifizierung:

  ```
  Set-SmConfigSettings -Agent –configSettings
  @{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
  ```

- So deaktivieren Sie die clientzertifikatbasierte Authentifizierung:

  ```
  Set-SmConfigSettings -Agent –configSettings
  @{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
  ```