CA-Zertifikat konfigurieren

SnapCenter software

NetApp
November 06, 2025

Inhalt

CA-Zertifikat konfigurieren

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**.

In diesem Assistentenfenster …	Gehen Sie wie folgt vor…
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"
   ```

Konfigurieren Sie das CA-Zertifikat für den von NetApp unterstützten Plug-In-Dienst auf dem Linux-Host

Sie sollten das Kennwort des Plug-In-Schlüsselspeichers und seines Zertifikats verwalten, das CA-Zertifikat konfigurieren, Stamm- oder Zwischenzertifikate für den Plug-In-Truststore konfigurieren und ein von der CA signiertes Schlüsselpaar für den Plug-In-Truststore mit dem SnapCenter -Plug-In-Dienst konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Die Plug-Ins verwenden die Datei „keystore.jks“, die sich unter */opt/ NetApp/snapcenter/scc/etc* befindet,

sowohl als Truststore als auch als Keystore.

Verwalten Sie das Kennwort für den Plug-In-Schlüsselspeicher und den Alias des verwendeten, von der Zertifizierungsstelle signierten Schlüsselpaars.

Schritte

1. Sie können das Standardkennwort für den Plug-in-Keystore aus der Eigenschaftendatei des Plug-in-Agenten abrufen.

   Dies ist der Wert, der dem Schlüssel „KEYSTORE_PASS“ entspricht.

2. Ändern Sie das Keystore-Passwort:

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

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

   Aktualisieren Sie dasselbe für den Schlüssel KEYSTORE_PASS in der Datei *agent.properties*.

3. Starten Sie den Dienst nach der Änderung des Kennworts neu.

> Das Kennwort für den Plug-In-Schlüsselspeicher und für alle zugehörigen Aliaskennwörter des privaten Schlüssels müssen identisch sein.

Konfigurieren Sie Stamm- oder Zwischenzertifikate für den Plug-In-Truststore

Sie sollten die Stamm- oder Zwischenzertifikate ohne den privaten Schlüssel für den Plug-In-Truststore konfigurieren.

Schritte

1. Navigieren Sie zu dem Ordner, der den Plug-In-Schlüsselspeicher enthält: /opt/NetApp/snapcenter/scc/etc.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

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

4. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:

   ```
    keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
   . Starten Sie den Dienst neu, nachdem Sie die Stamm- oder Zwischenzertifikate für den Plug-In-Truststore konfiguriert haben.
   ```

Sie sollten das Stamm-CA-Zertifikat und dann die Zwischen-CA-Zertifikate hinzufügen.

Konfigurieren Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore

Sie sollten das von der Zertifizierungsstelle signierte Schlüsselpaar für den Truststore des Plug-Ins konfigurieren.

Schritte

1. Navigieren Sie zu dem Ordner, der den Plug-In-Schlüsselspeicher /opt/ NetApp/snapcenter/scc/etc enthält.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

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

4. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem 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. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-Zertifikat in das Schlüsselspeicherkennwort.

   Das Standardkennwort für den Plug-in-Schlüsselspeicher ist der Wert des Schlüssels KEYSTORE_PASS in der Datei agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . Wenn der Aliasname im CA-Zertifikat lang ist und Leerzeichen oder
   Sonderzeichen („*“, „,“) enthält, ändern Sie den Aliasnamen in einen
   einfachen Namen:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Konfigurieren Sie den Aliasnamen aus dem CA-Zertifikat in der Datei
   agent.properties.
   ```

   Aktualisieren Sie diesen Wert anhand des Schlüssels SCC_CERTIFICATE_ALIAS.

8. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore konfiguriert haben.

Konfigurieren der Zertifikatsperrliste (CRL) für Plug-Ins

Informationen zu diesem Vorgang

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

Schritte

1. Sie können das Standardverzeichnis in der Datei agent.properties anhand des Schlüssels CRL_PATH ändern und aktualisieren.

   Sie können mehr als eine CRL-Datei in diesem Verzeichnis ablegen. Die eingehenden Zertifikate werden anhand der einzelnen CRLs überprüft.

Konfigurieren Sie das CA-Zertifikat für den von NetApp unterstützten Plug-In-Dienst auf dem Windows-Host

Sie sollten das Kennwort des Plug-In-Schlüsselspeichers und seines Zertifikats verwalten, das CA-Zertifikat konfigurieren, Stamm- oder Zwischenzertifikate für den Plug-In-Truststore konfigurieren und ein von der CA signiertes Schlüsselpaar für den Plug-In-Truststore mit dem SnapCenter -Plug-In-Dienst konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Die Plug-ins verwenden die Datei *keystore.jks*, die sich unter *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* befindet, sowohl als Truststore als auch als Keystore.

Verwalten Sie das Kennwort für den Plug-In-Schlüsselspeicher und den Alias des verwendeten, von der Zertifizierungsstelle signierten Schlüsselpaars.

Schritte

1. Sie können das Standardkennwort für den Plug-in-Keystore aus der Eigenschaftendatei des Plug-in-Agenten abrufen.

   Es handelt sich um den Wert, der dem Schlüssel *KEYSTORE_PASS* entspricht.

2. Ändern Sie das Keystore-Passwort:

   keytool -storepasswd -keystore keystore.jks

   > Wenn der Befehl „keytool“ in der Windows-Eingabeaufforderung nicht erkannt wird, ersetzen Sie den Befehl „keytool“ durch seinen vollständigen Pfad.

   C:\Programme\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore keystore.jks

3. Ändern Sie das Kennwort für alle Aliase der privaten Schlüsseleinträge im Schlüsselspeicher in dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:

   keytool -keypasswd -alias "Aliasname_im_Zertifikat" -keystore keystore.jks

   Aktualisieren Sie dasselbe für den Schlüssel KEYSTORE_PASS in der Datei *agent.properties*.

4. Starten Sie den Dienst nach der Änderung des Kennworts neu.

> Das Kennwort für den Plug-In-Schlüsselspeicher und für alle zugehörigen Aliaskennwörter des privaten Schlüssels müssen identisch sein.

Konfigurieren Sie Stamm- oder Zwischenzertifikate für den Plug-In-Truststore

Sie sollten die Stamm- oder Zwischenzertifikate ohne den privaten Schlüssel für den Plug-In-Truststore konfigurieren.

Schritte

1. Navigieren Sie zu dem Ordner mit dem Plug-in-Schlüsselspeicher *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

   keytool -list -v -keystore keystore.jks

4. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:

   keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder Zwischenzertifikate für den Plug-In-Truststore konfiguriert haben.

> Sie sollten das Stamm-CA-Zertifikat und dann die Zwischen-CA-Zertifikate hinzufügen.

Konfigurieren Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore

Sie sollten das von der Zertifizierungsstelle signierte Schlüsselpaar für den Truststore des Plug-Ins konfigurieren.

Schritte

1. Navigieren Sie zu dem Ordner mit dem Plug-in-Schlüsselspeicher *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei *keystore.jks*.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

   keytool -list -v -keystore keystore.jks

4. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem 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. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-Zertifikat in das Schlüsselspeicherkennwort.

   Das Standardkennwort für den Plug-in-Schlüsselspeicher ist der Wert des Schlüssels KEYSTORE_PASS in der Datei agent.properties.

   keytool -keypasswd -alias "Aliasname_im_CA_Zertifikat" -keystore keystore.jks

8. Konfigurieren Sie den Aliasnamen aus dem CA-Zertifikat in der Datei *agent.properties*.

   Aktualisieren Sie diesen Wert anhand des Schlüssels SCC_CERTIFICATE_ALIAS.

9. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore konfiguriert haben.

Konfigurieren der Zertifikatsperrliste (CRL) für SnapCenter -Plug-Ins

Informationen zu diesem Vorgang

- Um die neueste CRL-Datei für das entsprechende CA-Zertifikat herunterzuladen, siehe "So aktualisieren Sie die Zertifikatsperrlistendatei im SnapCenter CA-Zertifikat" .
- SnapCenter Plug-Ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für 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* anhand des Schlüssels CRL_PATH ändern und aktualisieren.
2. Sie können mehr als eine CRL-Datei in diesem Verzeichnis ablegen.

   Die eingehenden Zertifikate werden anhand der einzelnen CRLs überprüft.

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.