Konfigurieren des CA-Zertifikats für den Windows-Host

SnapCenter software

NetApp
November 06, 2025

Inhalt

Konfigurieren des CA-Zertifikats für den Windows-Host . . . 1
CA-Zertifikat-CSR-Datei generieren . . . 1
CA-Zertifikate importieren . . . 1
Abrufen des CA-Zertifikatfingerabdrucks . . . 2
Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten . . . 3
Konfigurieren des CA-Zertifikats mit der SnapCenter -Site . . . 3
Aktivieren von CA-Zertifikaten für SnapCenter . . . 4

Konfigurieren des CA-Zertifikats für den Windows-Host

CA-Zertifikat-CSR-Datei generieren

Sie können eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren und das Zertifikat importieren, das Sie mithilfe der generierten CSR von einer Zertifizierungsstelle (Certificate Authority, CA) erhalten können. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block verschlüsselten Textes, der einem autorisierten Zertifikatsanbieter übergeben wird, um das signierte CA-Zertifikat zu beschaffen.

Die RSA-Schlüssellänge des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter "So generieren Sie eine CA-Zertifikat-CSR-Datei" .

Wenn Sie das CA-Zertifikat für Ihre Domäne (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie das Generieren der CSR-Datei des CA-Zertifikats überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die jeweiligen Hostnamen im CA-Zertifikat erwähnt werden. Das Zertifikat kann aktualisiert werden, indem vor dem Erwerb des Zertifikats das Feld „Subject Alternative Name (SAN)“ ausgefüllt wird. Bei einem Wildcard-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

CA-Zertifikate importieren

Sie müssen die CA-Zertifikate mithilfe der Microsoft Management Console (MMC) in den SnapCenter -Server und die Windows-Host-Plug-Ins importieren.

Schritte

1. Gehen Sie zur Microsoft-Verwaltungskonsole (MMC) und klicken Sie dann auf **Datei** > **Snap-In hinzufügen/entfernen**.
2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
4. Klicken Sie auf **Konsolenstamm** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsstellen** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Importieren**, um den Importassistenten zu starten.
6. Schließen Sie den Assistenten wie folgt ab:

In diesem Assistentenfenster …	Gehen Sie wie folgt vor…
Privaten Schlüssel importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie anschließend auf **Weiter**.
Importdateiformat	Nehmen Sie keine Änderungen vor; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Kennwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Abschließen des Zertifikatimport-Assistenten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**, um den Import zu starten.

Das zu importierende Zertifikat sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: *.pfx, *.p12 und *.p7b).

7. Wiederholen Sie Schritt 5 für den Ordner „Persönlich“.

Abrufen des CA-Zertifikatfingerabdrucks

Ein Zertifikatfingerabdruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Aus dem Inhalt des Zertifikats wird mithilfe eines Fingerabdruckalgorithmus ein Fingerabdruck berechnet.

Schritte

1. Führen Sie auf der GUI Folgendes aus:
   a. Doppelklicken Sie auf das Zertifikat.
   b. Klicken Sie im Dialogfeld „Zertifikat“ auf die Registerkarte „Details“.
   c. Blättern Sie durch die Liste der Felder und klicken Sie auf **Fingerabdruck**.
   d. Kopieren Sie die Hexadezimalzeichen aus dem Feld.
   e. Entfernen Sie die Leerzeichen zwischen den Hexadezimalzahlen.

      Wenn der Fingerabdruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, lautet er nach dem Entfernen der Leerzeichen: „a909502dd82ae41433e6f83886b00d4277a32a7b“.

2. Führen Sie in PowerShell Folgendes aus:
   a. Führen Sie den folgenden Befehl aus, um den Fingerabdruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreffnamens zu identifizieren.

      Get-ChildItem -Pfad Zertifikat:\LocalMachine\My

   b. Kopieren Sie den Fingerabdruck.

Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten

Sie sollten das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Führen Sie die folgenden Schritte auf dem SnapCenter -Server und allen Plug-In-Hosts aus, auf denen bereits CA-Zertifikate bereitgestellt sind.

Schritte

1. Entfernen Sie die vorhandene Zertifikatsbindung mit dem SMCore-Standardport 8145, indem Sie den folgenden Befehl ausführen:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Beispiel:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Binden Sie das neu installierte Zertifikat an die Windows-Host-Plug-in-Dienste, indem Sie die folgenden Befehle ausführen:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
   ```

   Beispiel:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
   ```

Konfigurieren des CA-Zertifikats mit der SnapCenter -Site

Sie sollten das CA-Zertifikat mit der SnapCenter -Site auf dem Windows-Host konfigurieren.

Schritte

1. Öffnen Sie den IIS-Manager auf dem Windows-Server, auf dem SnapCenter installiert ist.
2. Klicken Sie im linken Navigationsbereich auf **Verbindungen**.
3. Erweitern Sie den Namen des Servers und **Sites**.

4. Wählen Sie die SnapCenter -Website aus, auf der Sie das SSL-Zertifikat installieren möchten.
5. Navigieren Sie zu **Aktionen** > **Site bearbeiten** und klicken Sie auf **Bindungen**.
6. Wählen Sie auf der Seite „Bindungen“ die Option **Bindung für https** aus.
7. Klicken Sie auf **Bearbeiten**.
8. Wählen Sie aus der Dropdown-Liste „SSL-Zertifikat“ das kürzlich importierte SSL-Zertifikat aus.
9. Klicken Sie auf **OK**.

> Die SnapCenter Scheduler-Site (Standardport: 8154, HTTPS) ist mit einem selbstsignierten Zertifikat konfiguriert. Dieser Port kommuniziert innerhalb des SnapCenter Server-Hosts und muss nicht mit einem CA-Zertifikat konfiguriert werden. Wenn Ihre Umgebung jedoch die Verwendung eines CA-Zertifikats erfordert, wiederholen Sie die Schritte 5 bis 9 mithilfe der SnapCenter Scheduler-Site.

> Wenn das kürzlich bereitgestellte CA-Zertifikat nicht im Dropdown-Menü aufgeführt ist, überprüfen Sie, ob das CA-Zertifikat mit dem privaten Schlüssel verknüpft ist.

> Stellen Sie sicher, dass das Zertifikat über den folgenden Pfad hinzugefügt wird: **Konsolenstamm > Zertifikate – Lokaler Computer > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.

Aktivieren von CA-Zertifikaten für SnapCenter

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikatvalidierung für den SnapCenter -Server aktivieren.

Bevor Sie beginnen

- Sie können die CA-Zertifikate mit dem Cmdlet „Set-SmCertificateSettings“ aktivieren oder deaktivieren.
- Sie können den Zertifikatsstatus für den SnapCenter -Server mit dem Cmdlet Get-SmCertificateSettings anzeigen.

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie sich an die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Schritte

1. Navigieren Sie auf der Seite „Einstellungen“ zu **Einstellungen** > **Globale Einstellungen** > **CA-Zertifikateinstellungen**.
2. Wählen Sie **Zertifikatvalidierung aktivieren**.
3. Klicken Sie auf **Übernehmen**.

Nachdem Sie fertig sind

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 für den Plug-In-Host kein CA-Zertifikat aktiviert oder 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.