



Konfigurieren Sie das CA-Zertifikat für den Windows-Host

SnapCenter Software 6.0

NetApp
July 23, 2024

Inhalt

- Konfigurieren Sie das CA-Zertifikat für den Windows-Host 1
 - ZertifikatCSR-Datei erstellen 1
 - Importieren von CA-Zertifikaten 1
 - Abrufen des Daumenabdrucks für das CA-Zertifikat 2
- Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-in-Diensten 3
- Konfigurieren Sie ein CA-Zertifikat mit SnapCenter Site 3
- Aktivieren Sie CA-Zertifikate für SnapCenter 4

Konfigurieren Sie das CA-Zertifikat für den Windows-Host

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.



CA Certificate RSA-Schlüssel sollten mindestens 3072 Bit lang sein.

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 das Feld Alternative Name (SAN) des Studienteilnehmers ausfüllen, bevor Sie das Zertifikat beschaffen. 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 ein CA-Zertifikat mit SnapCenter Site

Sie sollten das CA-Zertifikat mit der SnapCenter-Site auf einem 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 > Website 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-Serverhosts, und es ist nicht zwingend erforderlich, mit einem CA-Zertifikat zu konfigurieren. Wenn Sie in Ihrer Umgebung jedoch die Verwendung eines CA-Zertifikats vorschreibt, wiederholen Sie die Schritte 5 bis 9 mithilfe des SnapCenter-Planerstandorts.



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 Sie CA-Zertifikate 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.

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. Navigieren Sie auf der Seite Einstellungen zu **Einstellungen > Globale Einstellungen > CA Zertifikateinstellungen**.
2. Wählen Sie **Zertifikatvalidierung Aktivieren**.
3. Klicken Sie Auf **Anwenden**.

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 kein CA-Zertifikat aktiviert oder 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, BEISPIELHAFTE 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.