



Konfigurieren und aktivieren Sie die bidirektionale SSL-Kommunikation

SnapCenter Software 4.9

NetApp
March 20, 2024

Inhalt

- Konfigurieren und aktivieren Sie die bidirektionale SSL-Kommunikation 1
 - Konfigurieren Sie die bidirektionale SSL-Kommunikation 1
 - Aktivieren Sie die bidirektionale SSL-Kommunikation 3

Konfigurieren und aktivieren Sie die bidirektionale SSL-Kommunikation

Konfigurieren Sie die bidirektionale SSL-Kommunikation

Sie sollten die bidirektionale SSL-Kommunikation so konfigurieren, dass die gegenseitige Kommunikation zwischen dem SnapCenter-Server und den Plug-ins gesichert ist.

Bevor Sie beginnen

- Sie sollten die CSR-Datei des CA-Zertifikats mit der unterstützten Mindestschlüssellänge von 3072 erstellt haben.
- Das CA-Zertifikat sollte die Serverauthentifizierung und die Clientauthentifizierung unterstützen.
- Sie sollten über ein CA-Zertifikat mit privatem Schlüssel und Fingerabdruck-Details verfügen.
- Sie sollten die Einweg-SSL-Konfiguration aktiviert haben.

Weitere Informationen finden Sie unter ["Abschnitt „CA-Zertifikat konfigurieren“.](#)

- Sie müssen die bidirektionale SSL-Kommunikation auf allen Plug-in-Hosts und dem SnapCenter-Server aktiviert haben.

Umgebungen mit einigen Hosts oder Servern, die für die bidirektionale SSL-Kommunikation nicht aktiviert sind, werden nicht unterstützt.

Schritte

1. Um den Port zu binden, führen Sie die folgenden Schritte auf dem SnapCenter-Server-Host für SnapCenter IIS-Webserver-Port 8146 (Standard) und erneut für SMCore-Port 8145 (Standard) mit PowerShell-Befehlen durch.
 - a. Entfernen Sie die vorhandene selbstsignierte SnapCenter-Zertifikatport-Bindung mit dem folgenden PowerShell Befehl.

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
```

Beispiel:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

```
> netsh http delete sslcert ipport=0.0.0.0:8146
```

- b. Binden Sie das neu beschaffte CA-Zertifikat an den SnapCenter-Server und den SMCore-Port.

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>  
certhash=$cert appid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

Beispiel:

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:8146
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

2. Um auf das CA-Zertifikat zuzugreifen, fügen Sie den Standard-IIS-Webserver-Benutzer „**IIS AppPool\SnapCenter**“ von SnapCenter in die Zertifikatsberechtigungsliste ein, indem Sie die folgenden Schritte ausführen, um auf das neu beschaffte CA-Zertifikat zuzugreifen.
 - a. Rufen Sie die Microsoft Management Console (MMC) auf, und klicken Sie dann auf **Datei > Snapln hinzufügen/entfernen**.
 - b. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
 - c. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
 - d. Klicken Sie Auf **Konsolenwurzel > Zertifikate – Lokaler Computer > Persönlich > Zertifikate**.
 - e. Wählen Sie das SnapCenter-Zertifikat aus.
 - f. Um den Assistenten zum Hinzufügen von Benutzerberechtigungen zu starten, klicken Sie mit der rechten Maustaste auf das CA-Zertifikat und wählen **Alle Aufgaben > Private Schlüssel verwalten**.
 - g. Klicken Sie auf **Hinzufügen**, im Assistenten Benutzer und Gruppen auswählen ändern Sie den Speicherort in den lokalen Computernamen (ganz oben in der Hierarchie)
 - h. Fügen Sie den Benutzer IIS AppPool\SnapCenter hinzu, geben Sie die vollen Kontrollberechtigungen ein.
3. Fügen Sie für die IIS-Berechtigung **CA-Zertifikat** den neuen DWORD-Registrierungsschlüssel-Eintrag im SnapCenter-Server über den folgenden Pfad hinzu:

Im Windows-Registrierungs-Editor, Traverse auf den unten genannten Pfad,

```
HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
```

4. Erstellen Sie einen neuen DWORD-Registrierungsschlüsseleintrag im Kontext DER SCHANNEL-Registrierungskonfiguration.

```
SendTrustedIssuerList = 0
```

ClientAuthTrustMode = 2

Konfigurieren Sie das SnapCenter-Windows-Plug-in für die bidirektionale SSL-Kommunikation

Sie sollten das SnapCenter-Windows-Plug-in für die bidirektionale SSL-Kommunikation mithilfe von PowerShell Befehlen konfigurieren.

Bevor Sie beginnen

Stellen Sie sicher, dass der Fingerabdruck des CA-Zertifikats verfügbar ist.

Schritte

1. Um den Port zu binden, führen Sie die folgenden Aktionen auf dem Windows-Plug-in-Host für SMCore-Port 8145 aus (Standard).

- a. Entfernen Sie die vorhandene selbstsignierte SnapCenter-Zertifikatport-Bindung mit dem folgenden PowerShell Befehl.

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

Beispiel:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

- b. Binden Sie das neu beschaffte CA-Zertifikat an den SMCore-Port.

```
> $cert = "<CA_certificate thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert  
appid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

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

Beispiel:

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

Aktivieren Sie die bidirektionale SSL-Kommunikation

Sie können bidirektionale SSL-Kommunikation aktivieren, um die gegenseitige

Kommunikation zwischen SnapCenter Server und den Plug-ins mithilfe von PowerShell Befehlen zu sichern.

Bevor Sie beginnen

Führen Sie die Befehle für alle Plug-ins und den SMCore-Agent zuerst und dann für den Server aus.

Schritte

1. Um die bidirektionale SSL-Kommunikation zu aktivieren, führen Sie die folgenden Befehle auf dem SnapCenter-Server für die Plug-ins, den Server und für jeden Agenten aus, für den die bidirektionale SSL-Kommunikation erforderlich ist.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName <Plugin_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

2. Führen Sie den IIS-SnapCenter-Anwendungspool-Recyclingvorgang mit dem folgenden Befehl durch. >
`Restart-WebAppPool -Name "SnapCenter"`

3. Starten Sie für Windows-Plug-ins den SMCore-Dienst neu, indem Sie den folgenden PowerShell-Befehl ausführen:

```
> Restart-Service -Name SnapManagerCoreService
```

Deaktivieren Sie die bidirektionale SSL-Kommunikation

Sie können die bidirektionale SSL-Kommunikation mithilfe von PowerShell Befehlen deaktivieren.

Über diese Aufgabe

- Führen Sie die Befehle für alle Plug-ins und den SMCore-Agent zuerst und dann für den Server aus.
- Wenn Sie die bidirektionale SSL-Kommunikation deaktivieren, werden das CA-Zertifikat und seine Konfiguration nicht entfernt.
- Um dem SnapCenter-Server einen neuen Host hinzuzufügen, müssen Sie die bidirektionale SSL-Verbindung für alle Plug-in-Hosts deaktivieren.
- NLB und F5 werden nicht unterstützt.

Schritte

1. Um die bidirektionale SSL-Kommunikation zu deaktivieren, führen Sie die folgenden Befehle auf dem SnapCenter-Server für alle Plug-in-Hosts und den SnapCenter-Host aus.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName <Agent_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

2. Führen Sie den IIS-SnapCenter-Anwendungspool-Recyclingvorgang mit dem folgenden Befehl durch. >
`Restart-WebAppPool -Name "SnapCenter"`
3. Starten Sie für Windows-Plug-ins den SMCORE-Dienst neu, indem Sie den folgenden PowerShell-Befehl ausführen:

```
> Restart-Service -Name SnapManagerCoreService
```

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtlich geschützten Urhebers 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.