



Configurare e abilitare la comunicazione SSL bidirezionale

SnapCenter Software 5.0

NetApp
July 18, 2024

Sommario

- Configurare e abilitare la comunicazione SSL bidirezionale 1
 - Configurare la comunicazione SSL bidirezionale..... 1
 - Abilitare la comunicazione SSL bidirezionale..... 3

Configurare e abilitare la comunicazione SSL bidirezionale

Configurare la comunicazione SSL bidirezionale

È necessario configurare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra il server SnapCenter e i plug-in.

Prima di iniziare

- Il file CSR del certificato CA dovrebbe essere stato generato con la lunghezza minima supportata della chiave di 3072.
- Il certificato CA deve supportare l'autenticazione del server e l'autenticazione del client.
- È necessario disporre di un certificato CA con chiave privata e dettagli di identificazione personale.
- La configurazione SSL unidirezionale dovrebbe essere stata attivata.

Per ulteriori informazioni, vedere ["Sezione Configure CA certificate \(Configura certificato CA\)."](#)

- È necessario attivare la comunicazione SSL bidirezionale su tutti gli host plug-in e sul server SnapCenter.

L'ambiente con alcuni host o server non abilitati per la comunicazione SSL bidirezionale non è supportato.

Fasi

1. Per eseguire il binding della porta, attenersi alla seguente procedura sull'host del server SnapCenter per la porta 8146 del server Web IIS SnapCenter (impostazione predefinita) e ancora per la porta 8145 SMCORE (impostazione predefinita) utilizzando i comandi PowerShell.

- a. Rimuovere il binding della porta del certificato autofirmato SnapCenter esistente utilizzando il seguente comando PowerShell.

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

Ad esempio,

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

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

- b. Associare il certificato CA appena procurato al server SnapCenter e alla porta SMCORE.

```
> $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>
```

Ad esempio,

```
> $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. Per accedere all'autorizzazione al certificato CA, aggiungere l'utente predefinito del server Web IIS di SnapCenter "**IIS AppPool/SnapCenter**" nell'elenco delle autorizzazioni del certificato eseguendo la procedura seguente per accedere al certificato CA appena procurato.
 - a. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file > Aggiungi/Rimuovi SnapIn**.
 - b. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
 - c. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
 - d. Fare clic su **Directory principale console > certificati – computer locale > personale > certificati**.
 - e. Selezionare il certificato SnapCenter.
 - f. Per avviare l'aggiunta guidata autorizzazioni utente, fare clic con il pulsante destro del mouse sul certificato CA e selezionare **tutte le attività > Gestisci chiavi private**.
 - g. Fare clic su **Aggiungi**, nella procedura guidata Seleziona utenti e gruppi modificare la posizione in Nome computer locale (in alto nella gerarchia)
 - h. Aggiungere l'utente di IIS AppPool/SnapCenter, assegnare autorizzazioni di controllo complete.
3. Per l'autorizzazione IIS * del certificato CA, aggiungere la nuova voce delle chiavi di registro DWORD nel server SnapCenter dal seguente percorso:

Nell'editor del Registro di sistema di Windows, passare al percorso indicato di seguito,

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

4. Creare una nuova voce della chiave del Registro di sistema DWORD nel contesto della configurazione DEL Registro DI sistema SCHANNEL.

```
SendTrustedIssuerList = 0
```

```
ClientAuthTrustMode = 2
```

Configurare il plug-in Windows di SnapCenter per la comunicazione SSL bidirezionale

È necessario configurare il plug-in Windows di SnapCenter per la comunicazione SSL bidirezionale utilizzando i comandi PowerShell.

Prima di iniziare

Assicurarsi che il thumbprint del certificato CA sia disponibile.

Fasi

1. Per collegare la porta, eseguire le seguenti operazioni sull'host plug-in di Windows per la porta SMCore 8145 (impostazione predefinita).
 - a. Rimuovere il binding della porta del certificato autofirmato SnapCenter esistente utilizzando il seguente comando PowerShell.

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

Ad esempio,

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

- b. Associare il certificato CA appena procurato alla porta SMCore.

```
> $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>
```

Ad esempio,

```
> $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
```

Abilitare la comunicazione SSL bidirezionale

È possibile abilitare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra il server SnapCenter e i plug-in utilizzando i comandi PowerShell.

Prima di iniziare

Eseguire i comandi per tutti i plug-in e l'agente SMCORE prima e poi per il server.

Fasi

1. Per attivare la comunicazione SSL bidirezionale, eseguire i seguenti comandi sul server SnapCenter per i plug-in, il server e per ciascuno degli agenti per i quali è richiesta la comunicazione SSL bidirezionale.

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

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

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

2. Eseguire l'operazione di riciclo del pool di applicazioni IIS SnapCenter utilizzando il seguente comando. >
`Restart-WebAppPool -Name "SnapCenter"`

3. Per i plug-in di Windows, riavviare il servizio SMCORE eseguendo il seguente comando PowerShell:

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

Disattiva la comunicazione SSL bidirezionale

È possibile disattivare la comunicazione SSL bidirezionale utilizzando i comandi PowerShell.

A proposito di questa attività

- Eseguire i comandi per tutti i plug-in e l'agente SMCORE prima e poi per il server.
- Quando si disattiva la comunicazione SSL bidirezionale, il certificato CA e la relativa configurazione non vengono rimossi.
- Per aggiungere un nuovo host al server SnapCenter, è necessario disattivare il protocollo SSL bidirezionale per tutti gli host plug-in.
- NLB e F5 non sono supportati.

Fasi

1. Per disattivare la comunicazione SSL bidirezionale, eseguire i seguenti comandi sul server SnapCenter per tutti gli host plug-in e l'host SnapCenter.

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

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

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

2. Eseguire l'operazione di riciclo del pool di applicazioni IIS SnapCenter utilizzando il seguente comando. >
`Restart-WebAppPool -Name "SnapCenter"`

3. Per i plug-in di Windows, riavviare il servizio SMCORE eseguendo il seguente comando PowerShell:

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

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.