



Configurare il certificato CA per l'host Windows

SnapCenter Software 6.0

NetApp
July 23, 2024

Sommario

- Configurare il certificato CA per l'host Windows 1
 - Generare il file CSR del certificato CA 1
 - Importare i certificati CA 1
 - Ottenere il thumbprint del certificato CA 2
 - Configurare il certificato CA con i servizi plug-in dell'host Windows 2
 - Configurare il certificato CA con il sito SnapCenter 3
 - Abilitare i certificati CA per SnapCenter 4

Configurare il certificato CA per l'host Windows

Generare il file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato verrà associata una chiave privata.

CSR è un blocco di testo codificato fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.



La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare una CSR, vedere ["Come generare il file CSR del certificato CA"](#).



Se si possiede il certificato CA per il dominio (*.domain.company.com) o il sistema (machine1.domain.company.com), è possibile ignorare la generazione del file CSR del certificato CA. È possibile implementare il certificato CA esistente con SnapCenter.

Per le configurazioni del cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere indicati nel certificato CA. Il certificato può essere aggiornato compilando il campo Subject alternative Name (SAN) (Nome alternativo soggetto) prima di procurarsi il certificato. Per un certificato wild card (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

Importare i certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host di Windows utilizzando la console di gestione Microsoft (MMC).

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file > Aggiungi/Rimuovi Snapin**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
4. Fare clic su **root console > certificati – computer locale > autorità di certificazione root attendibili > certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Trusted Root Certification Authorities", quindi selezionare **All Tasks > Import** per avviare l'importazione guidata.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata...	Effettuare le seguenti operazioni...
Importa chiave privata	Selezionare l'opzione Sì , importare la chiave privata, quindi fare clic su Avanti .
Formato del file di importazione	Non apportare modifiche; fare clic su Avanti .

In questa finestra della procedura guidata...	Effettuare le seguenti operazioni...
Sicurezza	Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su Avanti .
Completamento dell'importazione guidata certificati	Esaminare il riepilogo, quindi fare clic su fine per avviare l'importazione.



Il certificato di importazione deve essere fornito in bundle con la chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personal".

Ottenere il thumbprint del certificato CA

Un'identificazione personale del certificato è una stringa esadecimale che identifica un certificato. Un'identificazione personale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione personale.

Fasi

1. Eseguire le seguenti operazioni sulla GUI:
 - a. Fare doppio clic sul certificato.
 - b. Nella finestra di dialogo certificato, fare clic sulla scheda **Dettagli**.
 - c. Scorrere l'elenco dei campi e fare clic su **Thumbprint**.
 - d. Copiare i caratteri esadecimali dalla casella.
 - e. Rimuovere gli spazi tra i numeri esadecimali.

Ad esempio, se la stampa personale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "A909502ddd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
 - a. Eseguire il comando seguente per elencare l'identificazione del certificato installato e identificare il certificato installato di recente in base al nome del soggetto.

```
Get-ChildItem -Path Certate: LocalMachine/My
```

- b. Copiare la stampa personale.

Configurare il certificato CA con i servizi plug-in dell'host Windows

È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire le seguenti operazioni sul server SnapCenter e su tutti gli host plug-in in cui sono già implementati i certificati CA.

Fasi

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

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

Ad esempio:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Associare il certificato appena installato ai servizi plug-in
dell'host Windows eseguendo i seguenti comandi:
```

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

Ad esempio:

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

Configurare il certificato CA con il sito SnapCenter

È necessario configurare il certificato CA con il sito SnapCenter sull'host Windows.

Fasi

1. Aprire Gestione IIS sul server Windows in cui è installato SnapCenter.
2. Nel riquadro di navigazione a sinistra, fare clic su **connessioni**.
3. Espandere il nome del server e **Sites**.
4. Selezionare il sito Web di SnapCenter su cui si desidera installare il certificato SSL.
5. Accedere a **azioni > Modifica sito**, fare clic su **associazioni**.
6. Nella pagina binding, selezionare **binding for https**.
7. Fare clic su **Edit** (Modifica).
8. Dall'elenco a discesa SSL certificate (certificato SSL), selezionare il certificato SSL importato di recente.
9. Fare clic su **OK**.



Il sito dell'utilità di pianificazione SnapCenter (porta predefinita: 8154, HTTPS) è configurato con un certificato autofirmato. Questa porta comunica all'interno dell'host del server SnapCenter e non è obbligatoria la configurazione con un certificato CA. Tuttavia, se l'ambiente in uso richiede l'utilizzo di un certificato CA, ripetere i passaggi da 5 a 9 utilizzando il sito Utilità di pianificazione di SnapCenter.



Se il certificato CA distribuito di recente non è elencato nel menu a discesa, controllare se il certificato CA è associato alla chiave privata.



Assicurarsi che il certificato venga aggiunto utilizzando il seguente percorso: **Root console > certificati – computer locale > autorità di certificazione root attendibili > certificati**.

Abilitare i certificati CA per SnapCenter

È necessario configurare i certificati CA e attivare la convalida del certificato CA per il server SnapCenter.

Prima di iniziare

- È possibile attivare o disattivare i certificati CA utilizzando il cmdlet `Set-SmCertificateSettings`.
- È possibile visualizzare lo stato del certificato per il server SnapCenter utilizzando il cmdlet `Get-SmCertificateSettings`.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo `Get-Help command_name`. In alternativa, fare riferimento a ["Guida di riferimento al cmdlet del software SnapCenter"](#).

Fasi

1. Nella pagina Settings (Impostazioni), selezionare **Settings** (Impostazioni) > **Global Settings** (Impostazioni globali) > **CA Certificate Settings** (Impostazioni certificato CA).
2. Selezionare **attiva convalida certificato**.
3. Fare clic su **Apply** (Applica).

Al termine

L'host della scheda host gestiti visualizza un lucchetto e il colore del lucchetto indica lo stato della connessione tra il server SnapCenter e l'host del plug-in.

- Indica che all'host del plug-in non è abilitato o assegnato alcun certificato CA.
- Indica che il certificato CA è stato validato correttamente.
- Indica che non è stato possibile validare il certificato CA.
- Indica che non è stato possibile recuperare le informazioni di connessione.



Quando lo stato è giallo o verde, le operazioni di protezione dei dati vengono completate correttamente.

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.