Configurare il certificato CA

SnapCenter Software 4.8

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/it-it/snapcenter-48/protect-scc/reference_generate_CA_certificate_CSR_file.html on September 26, 2025. Always check docs.netapp.com for the latest.

Sommario

Configurare il certificato CA . . . 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 per il servizio plug-in personalizzati di SnapCenter sull'host Linux . . . 3
  - Gestire la password per l'archivio chiavi del plug-in personalizzato e l'alias della coppia di chiavi firmate CA in uso . . . 3
  - Configurare i certificati root o intermedi per l'archivio di trust del plug-in personalizzato . . . 4
  - Configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato . . . 4
  - Configurare l'elenco CRL (Certificate Revocation List) per i plug-in personalizzati di SnapCenter . . . 5
- Configurare il certificato CA per il servizio plug-in personalizzati di SnapCenter sull'host Windows . . . 6
  - Gestire la password per l'archivio chiavi del plug-in personalizzato e l'alias della coppia di chiavi firmate CA in uso . . . 6
  - Configurare i certificati root o intermedi per l'archivio di trust del plug-in personalizzato . . . 7
  - Configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato . . . 7
  - Configurare l'elenco CRL (Certificate Revocation List) per i plug-in personalizzati di SnapCenter . . . 8
- Abilitare i certificati CA per i plug-in . . . 8

Configurare il certificato CA

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.

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**.
Sicurezza	Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**.

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
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 per il servizio plug-in personalizzati di SnapCenter sull'host Linux

È necessario gestire la password dell'archivio chiavi dei plug-in personalizzati e il relativo certificato, configurare il certificato CA, configurare i certificati root o intermedi per l'archivio certificati attendibili dei plug-in personalizzati e configurare la coppia di chiavi firmate CA per l'archivio di fiducia dei plug-in personalizzati con il servizio Plug-in personalizzati di SnapCenter per attivare il certificato digitale installato.

I plug-in personalizzati utilizzano il file 'keystore.jks', che si trova in */opt/NetApp/snapcenter/scc/etc* sia come Trust-store che come keystore.

Gestire la password per l'archivio chiavi del plug-in personalizzato e l'alias della coppia di chiavi firmate CA in uso

Fasi

1. È possibile recuperare la password predefinita del keystore del plug-in personalizzato dal file di proprietà dell'agente del plug-in personalizzato.

   È il valore corrispondente alla chiave 'KEYSTORE_PASS'.

2. Modificare la password del keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Modificare la password per tutti gli alias delle chiavi private nel
keystore con la stessa password utilizzata per il keystore:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

3. Riavviare il servizio dopo aver modificato la password.

La password per il keystore del plug-in personalizzato e per tutte le password alias associate della chiave privata deve essere la stessa.

Configurare i certificati root o intermedi per l'archivio di trust del plug-in personalizzato

È necessario configurare i certificati root o intermedi senza la chiave privata per l'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato: /Opt/NetApp/snapcenter/scc/ecc.
2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Aggiungere un certificato root o intermedio:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Riavviare il servizio dopo aver configurato i certificati root o
intermedi in un archivio di trust plug-in personalizzato.
```

Aggiungere il certificato CA principale e i certificati CA intermedi.

Configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato

È necessario configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato /opt/NetApp/snapcenter/scc/ecc.
2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Aggiungere il certificato CA con chiave pubblica e privata.

   ```
   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
   -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
   ```

5. Elencare i certificati aggiunti nel keystore.

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA in password archivio chiavi.

   La password predefinita customizzato del plug-in keystore è il valore della chiave KEYSTORE_PASS nel file agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . Se il nome alias nel certificato CA è lungo e contiene spazi o
   caratteri speciali ("*",","), modificare il nome alias con un nome
   semplice:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Configurare il nome alias del certificato CA nel file
   agent.properties.
   ```

   Aggiornare questo valore con la chiave SCC_CERTIFICATE_ALIAS.

8. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Configurare l'elenco CRL (Certificate Revocation List) per i plug-in personalizzati di SnapCenter

A proposito di questa attività

- I plug-in personalizzati di SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in personalizzati di SnapCenter è ' opt/NetApp/snapcenter/scc/etc/crl'.

Fasi

1. È possibile modificare e aggiornare la directory predefinita nel file agent.properties in base alla chiave CRL_PATH.

   È possibile inserire più file CRL in questa directory. I certificati in entrata verranno verificati per ciascun CRL.

Configurare il certificato CA per il servizio plug-in personalizzati di SnapCenter sull'host Windows

È necessario gestire la password dell'archivio chiavi dei plug-in personalizzati e il relativo certificato, configurare il certificato CA, configurare i certificati root o intermedi per l'archivio certificati attendibili dei plug-in personalizzati e configurare la coppia di chiavi firmate CA per l'archivio di fiducia dei plug-in personalizzati con il servizio Plug-in personalizzati di SnapCenter per attivare il certificato digitale installato.

I plug-in personalizzati utilizzano il file *keystore.jks*, che si trova in _C: File di programma NetApp, SnapCenter, Snapcenter Plug-in Creator, ecc., sia come archivio di fiducia che come archivio chiavi.

Gestire la password per l'archivio chiavi del plug-in personalizzato e l'alias della coppia di chiavi firmate CA in uso

Fasi

1. È possibile recuperare la password predefinita del keystore del plug-in personalizzato dal file di proprietà dell'agente del plug-in personalizzato.

   È il valore corrispondente alla chiave *KEYSTORE_PASS*.

2. Modificare la password del keystore:

   keytool -storepasswd -keystore keystore.jks

   > Se il comando "keytool" non viene riconosciuto dal prompt dei comandi di Windows, sostituire il comando keytool con il relativo percorso completo.

   C: File di programma Java <jdk_version> keytool.exe" -storepasswd -keystore keystore.jks

3. Modificare la password per tutti gli alias delle chiavi private nel keystore con la stessa password utilizzata per il keystore:

   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks

   Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

4. Riavviare il servizio dopo aver modificato la password.

   > La password per il keystore del plug-in personalizzato e per tutte le password alias associate della chiave privata deve essere la stessa.

Configurare i certificati root o intermedi per l'archivio di trust del plug-in personalizzato

È necessario configurare i certificati root o intermedi senza la chiave privata per l'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato _C: File di programma/NetApp/SnapCenter/Snapcenter Plug-in Creator
2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

   keytool -list -v -keystore keystore.jks

4. Aggiungere un certificato root o intermedio:

   Keytool -import -trustcaacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. Riavviare il servizio dopo aver configurato i certificati root o intermedi in un archivio di trust plug-in personalizzato.

Aggiungere il certificato CA principale e i certificati CA intermedi.

Configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato

È necessario configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato _C: File di programma/NetApp/SnapCenter/Snapcenter Plug-in Creator
2. Individuare il file *keystore.jks*.
3. Elencare i certificati aggiunti nel keystore:

   keytool -list -v -keystore keystore.jks

4. Aggiungere il certificato CA con chiave pubblica e privata.

   Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS

5. Elencare i certificati aggiunti nel keystore.

   keytool -list -v -keystore keystore.jks

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA in password archivio chiavi.

   La password predefinita customizzato del plug-in keystore è il valore della chiave KEYSTORE_PASS nel file agent.properties.

Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore keystore.jks

8. Configurare il nome alias del certificato CA nel file *agent.properties*.

   Aggiornare questo valore con la chiave SCC_CERTIFICATE_ALIAS.

9. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Configurare l'elenco CRL (Certificate Revocation List) per i plug-in personalizzati di SnapCenter

A proposito di questa attività

- Per scaricare il file CRL più recente per il certificato CA correlato, vedere "Come aggiornare il file dell'elenco di revoca dei certificati nel certificato CA di SnapCenter".
- I plug-in personalizzati di SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in personalizzati di SnapCenter è _'C: File di programma, NetApp, SnapCenter, SnapCenter Plug-in Creator, ecc.

Fasi

1. È possibile modificare e aggiornare la directory predefinita nel file *agent.properties* in base alla chiave CRL_PATH.
2. È possibile inserire più file CRL in questa directory.

   I certificati in entrata verranno verificati per ciascun CRL.

Abilitare i certificati CA per i plug-in

È necessario configurare i certificati CA e implementarne i certificati nel server SnapCenter e negli host plug-in corrispondenti. Attivare la convalida del certificato CA per i plug-in.

Cosa ti serve

- È possibile attivare o disattivare i certificati CA utilizzando il cmdlet Esegui *set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando le *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 anche a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina hosts, fare clic su **Managed hosts**.
3. Selezionare uno o più host plug-in.
4. Fare clic su **altre opzioni**.

5. Selezionare **attiva convalida certificato**.

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 il certificato CA non è né abilitato né assegnato all'host del plug-in.
- 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 © 2025 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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.