Configurare il certificato CA

SnapCenter software

NetApp
November 06, 2025

Sommario

Configurare il certificato CA . . . 1
- Genera file CSR del certificato CA . . . 1
- Importa certificati CA . . . 1
- Ottieni l'impronta digitale del certificato CA . . . 2
- Configurare il certificato CA con i servizi plug-in host di Windows . . . 2
- Configurare il certificato CA per il servizio plug-in supportato da NetApp sull'host Linux . . . 3
  - Gestisci la password per il keystore del plug-in e l'alias della coppia di chiavi firmata dalla CA in uso . . . 3
  - Configurare i certificati radice o intermedi per collegare trust-store . . . 4
  - Configurare la coppia di chiavi firmata dalla CA per collegare l'archivio attendibile . . . 4
  - Configurare l'elenco di revoche dei certificati (CRL) per i plug-in . . . 5
- Configurare il certificato CA per il servizio plug-in supportato da NetApp sull'host Windows . . . 6
  - Gestisci la password per il keystore del plug-in e l'alias della coppia di chiavi firmata dalla CA in uso . . . 6
  - Configurare i certificati radice o intermedi per collegare trust-store . . . 6
  - Configurare la coppia di chiavi firmata dalla CA per collegare l'archivio attendibile . . . 7
  - Configurare l'elenco di revoche dei certificati (CRL) per i plug-in SnapCenter . . . 7
- Abilita i certificati CA per i plug-in . . . 8

Configurare il certificato CA

Genera 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 sarà associata una chiave privata.

CSR è un blocco di testo codificato che viene 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 un CSR, vedere "Come generare il file CSR del certificato CA" .

Se possiedi il certificato CA per il tuo dominio (*.domain.company.com) o per il tuo sistema (machine1.domain.company.com), puoi saltare la generazione del file CSR del certificato CA. È possibile distribuire il certificato CA esistente con SnapCenter.

Per le configurazioni cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere menzionati nel certificato CA. È possibile aggiornare il certificato compilando il campo Subject Alternative Name (SAN) prima di ottenere il certificato. Per un certificato con caratteri jolly (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

Importa certificati CA

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

Passi

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati – Computer locale** > **Autorità di certificazione radice attendibili** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Autorità di certificazione radice attendibili", quindi selezionare **Tutte le attività** > **Importa** per avviare la procedura guidata di importazione.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Procedi come segue…
Importa chiave privata	Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**.
Formato file di importazione	Non apportare modifiche; fare clic su **Avanti**.

In questa finestra della procedura guidata…	Procedi come segue…
Sicurezza	Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**.
Completamento della procedura guidata di importazione del certificato	Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'importazione.

Il certificato di importazione deve essere incluso nella chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

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

Ottieni l'impronta digitale del certificato CA

L'impronta digitale di un certificato è una stringa esadecimale che identifica un certificato. L'impronta digitale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione digitale.

Passi

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. Scorri l'elenco dei campi e clicca su **Impronta digitale**.
   d. Copia i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se l'impronta digitale 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: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il seguente comando per elencare l'identificazione personale del certificato installato e identificare il certificato installato di recente tramite il nome dell'oggetto.

      Get-ChildItem -Percorso Cert:\LocalMachine\My

   b. Copia l'impronta digitale.

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

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

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

Passi

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>
   ```

   Per esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in host di
   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"
   ```

   Per 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 supportato da NetApp sull'host Linux

È necessario gestire la password del keystore dei plug-in e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per il trust-store dei plug-in e configurare la coppia di chiavi firmata dalla CA per il trust-store dei plug-in con il servizio plug-in SnapCenter per attivare il certificato digitale installato.

Il plug-in utilizza il file 'keystore.jks', che si trova in */opt/ NetApp/snapcenter/scc/etc* sia come archivio attendibile che come archivio chiavi.

Gestisci la password per il keystore del plug-in e l'alias della coppia di chiavi firmata dalla CA in uso

Passi

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

   È il valore corrispondente alla chiave 'KEYSTORE_PASS'.

2. Cambia la password del keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Modificare la password per tutti gli alias delle voci di chiave
privata 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 e per tutte le password alias associate alla chiave privata devono essere le stesse.

Configurare i certificati radice o intermedi per collegare trust-store

È necessario configurare i certificati radice o intermedi senza la chiave privata per collegare trust-store.

Passi

1. Passare alla cartella contenente il keystore del plug-in: /opt/ NetApp/snapcenter/scc/etc.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

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

4. Aggiungi un certificato radice o intermedio:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Riavviare il servizio dopo aver configurato i certificati radice o
intermedi per collegare trust-store.
```

Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

Configurare la coppia di chiavi firmata dalla CA per collegare l'archivio attendibile

È necessario configurare la coppia di chiavi firmata dalla CA nel trust-store del plug-in.

Passi

1. Passare alla cartella contenente il keystore del plug-in /opt/ NetApp/snapcenter/scc/etc.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

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

4. Aggiungere il certificato CA con chiave sia privata che pubblica.

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

5. Elenca 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 con la password del keystore.

   La password predefinita del keystore del plug-in 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 in un nome
semplice:
```

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

   Aggiornare questo valore in base alla chiave SCC_CERTIFICATE_ALIAS.

8. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA per collegare trust-store.

Configurare l'elenco di revoche dei certificati (CRL) per i plug-in

Informazioni su questo compito

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

Passi

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

   È possibile inserire più di un file CRL in questa directory. I certificati in arrivo saranno verificati rispetto a ciascun CRL.

Configurare il certificato CA per il servizio plug-in supportato da NetApp sull'host Windows

È necessario gestire la password del keystore dei plug-in e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per il trust-store dei plug-in e configurare la coppia di chiavi firmata dalla CA per il trust-store dei plug-in con il servizio plug-in SnapCenter per attivare il certificato digitale installato.

Il plug-in utilizza il file *keystore.jks*, che si trova in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* sia come archivio attendibile che come archivio chiavi.

Gestisci la password per il keystore del plug-in e l'alias della coppia di chiavi firmata dalla CA in uso

Passi

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

   È il valore corrispondente alla chiave *KEYSTORE_PASS*.

2. Cambia la password del keystore:

   keytool -storepasswd -keystore keystore.jks

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

   C:\Programmi\Java\<versione_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks

3. Modificare la password per tutti gli alias delle voci di chiave privata 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 e per tutte le password alias associate alla chiave privata devono essere le stesse.

Configurare i certificati radice o intermedi per collegare trust-store

È necessario configurare i certificati radice o intermedi senza la chiave privata per collegare trust-store.

Passi

1. Passare alla cartella contenente il keystore del plug-in *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Individuare il file 'keystore.jks'.

3. Elenca i certificati aggiunti nel keystore:

   keytool -list -v -keystore keystore.jks

4. Aggiungi un certificato radice o intermedio:

   keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. Riavviare il servizio dopo aver configurato i certificati radice o intermedi per collegare trust-store.

   Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

Configurare la coppia di chiavi firmata dalla CA per collegare l'archivio attendibile

È necessario configurare la coppia di chiavi firmata dalla CA nel trust-store del plug-in.

Passi

1. Passare alla cartella contenente il keystore del plug-in *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Individuare il file *keystore.jks*.
3. Elenca i certificati aggiunti nel keystore:

   keytool -list -v -keystore keystore.jks

4. Aggiungere il certificato CA con chiave sia privata che pubblica.

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

5. Elenca 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 con la password del keystore.

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

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

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

   Aggiornare questo valore in base alla chiave SCC_CERTIFICATE_ALIAS.

9. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA per collegare trust-store.

Configurare l'elenco di revoche dei certificati (CRL) per i plug-in SnapCenter

Informazioni su questo compito

- Per scaricare l'ultimo file CRL per il certificato CA correlato, vedere "Come aggiornare il file dell'elenco di revoche dei certificati in SnapCenter CA Certificate" .

- I plug-in SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in SnapCenter è *'C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.

Passi

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

   I certificati in arrivo saranno verificati rispetto a ciascun CRL.

Abilita i certificati CA per i plug-in

È necessario configurare i certificati CA e distribuirli nel server SnapCenter e negli host dei plug-in corrispondenti. Dovresti abilitare la convalida del certificato CA per i plug-in.

Prima di iniziare

- È possibile abilitare o disabilitare i certificati CA utilizzando il cmdlet run *Set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando *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, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Selezionare uno o più host di plug-in.
4. Fare clic su **Altre opzioni**.
5. Selezionare **Abilita convalida certificato**.

Dopo aver finito

Nella scheda Host gestiti viene visualizzato un lucchetto e il colore del lucchetto indica lo stato della connessione tra SnapCenter Server e l'host del plug-in.

- * * indica che il certificato CA non è abilitato né assegnato all'host del plug-in.
- * * indica che il certificato CA è stato convalidato correttamente.
- * * indica che il certificato CA non è stato convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

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

Informazioni sul copyright

Informazioni sul marchio commerciale