Configurare l'autenticazione basata su certificato

SnapCenter Software 5.0

NetApp
July 18, 2024

Sommario

Configurare l’autenticazione basata su certificato

Esportare i certificati dell’autorità di certificazione (CA) dal server SnapCenter

È necessario esportare i certificati CA dal server SnapCenter agli host plug-in utilizzando la console di gestione Microsoft.

Prima di iniziare

Il protocollo SSL bidirezionale dovrebbe essere stato configurato.

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 Snap-in certificati, selezionare l’opzione **computer account**, quindi fare clic su **fine**.
4. Fare clic su **Console root** > **certificati - computer locale** > **personale** > **certificati**.
5. Fare clic con il pulsante destro del mouse sul certificato CA procurato, utilizzato per il server SnapCenter, quindi selezionare **tutte le attività** > **Esporta** per avviare l’esportazione guidata.
6. Eseguire le seguenti operazioni nella procedura guidata.

Per questa opzione…	Effettuare le seguenti operazioni…
Esporta chiave privata	Selezionare **No, non esportare la chiave privata**, quindi fare clic su **Avanti**.
Formato file di esportazione	Fare clic su **Avanti**.
Nome file	Fare clic su **Browse** (Sfoglia) e specificare il percorso del file per il salvataggio del certificato, quindi fare clic su **Next** (Avanti).
Completamento dell’esportazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l’esportazione.

L’autenticazione basata su certificato non è supportata per le configurazioni SnapCenter ha e il plug-in SnapCenter per VMware vSphere.

Importa certificato CA (Certificate Authority) negli host plug-in di Windows

Per utilizzare il certificato della CA del server SnapCenter esportato, è necessario importare il certificato correlato negli host dei plug-in di SnapCenter 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 Snap-in certificati, selezionare l'opzione **computer account**, quindi fare clic su **fine**.
4. Fare clic su **Console root** > **certificati - computer locale** > **personale** > **certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Personal", quindi selezionare **All Tasks** > **Import** per avviare l'importazione guidata.
6. Eseguire le seguenti operazioni nella procedura guidata.

Per questa opzione…	Effettuare le seguenti operazioni…
Ubicazione del negozio	Fare clic su **Avanti**.
File da importare	Selezionare il certificato del server SnapCenter che termina con l'estensione .cer.
Archivio certificati	Fare clic su **Avanti**.
Completamento dell'esportazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'importazione.

Importare il certificato CA nei plug-in host UNIX e configurare i certificati root o intermedi nell'archivio di fiducia SPL

Importa certificato CA negli host plug-in UNIX

È necessario importare il certificato CA negli host plug-in UNIX.

A proposito di questa attività

- È possibile gestire la password per l'archivio chiavi SPL e l'alias della coppia di chiavi firmate CA in uso.
- La password per l'archivio chiavi SPL e per tutte le password alias associate della chiave privata deve essere la stessa.

Fasi

1. È possibile recuperare la password predefinita del keystore SPL dal file di proprietà SPL. È il valore corrispondente alla chiave `SPL_KEYSTORE_PASS`.
2. Modificare la password dell'archivio chiavi: `$ keytool -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 l'archivio chiavi: `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
4. Aggiornare lo stesso per la chiave SPL_KEYSTORE_PASS nel `spl.properties` file.

5. Riavviare il servizio dopo aver modificato la password.

Configurare i certificati root o intermedi per l'archivio di trust SPL

È necessario configurare i certificati root o intermedi in SPL trust-store. Aggiungere il certificato CA principale e i certificati CA intermedi.

Fasi

1. Passare alla cartella contenente il keystore SPL: `/var/opt/snapcenter/spl/etc`.
2. Individuare il file `keystore.jks`.
3. Elencare i certificati aggiunti nell'archivio chiavi: `$ keytool -list -v -keystore keystore.jks`
4. Aggiungere un certificato root o intermedio: `$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. Riavviare il servizio dopo aver configurato i certificati root o intermedi in SPL trust-store.

Configurare la coppia di chiavi con firma CA nell'archivio di trust SPL

È necessario configurare la coppia di chiavi firmate della CA in SPL trust-store.

Fasi

1. Passare alla cartella contenente il keystore di SPL `/var/opt/snapcenter/spl/etc`.
2. Individuare il file `keystore.jks`.
3. Elencare i certificati aggiunti nell'archivio chiavi: `$ keytool -list -v -keystore keystore.jks`
4. Aggiungere il certificato CA con chiave pubblica e privata. `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -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 dell'archivio chiavi SPL è il valore della chiave SPL_KEYSTORE_PASS nel `spl.properties` file.

   `$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
8. Se il nome dell'alias nel certificato CA è lungo e contiene spazi o caratteri speciali ("*",","), modificare il nome dell'alias con un nome semplice: `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
9. Configurare il nome alias dall'archivio chiavi presente nel `spl.properties` file. Aggiornare questo valore con la chiave SPL_CERTIFICATE_ALIAS.
10. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate della CA in SPL trust-store.

Abilitare l’autenticazione basata su certificato

Per abilitare l’autenticazione basata su certificato per il server SnapCenter e gli host plug-in Windows, eseguire il seguente cmdlet PowerShell. Per gli host plug-in Linux, l’autenticazione basata su certificato viene attivata quando si attiva il protocollo SSL bidirezionale.

- Per attivare l’autenticazione basata su certificati client:

```
Set-SmConfigSettings -Agent –configSettings
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- Per disattivare l’autenticazione basata su certificato del client:

```
Set-SmConfigSettings -Agent –configSettings
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
```