Autenticare reciprocamente il cluster e un server KMIP

ONTAP 9

NetApp
February 12, 2026

Sommario

Autenticare reciprocamente il cluster e un server KMIP

Autenticazione reciproca del cluster ONTAP e panoramica del server KMIP

L'autenticazione reciproca del cluster e di un gestore di chiavi esterno, ad esempio un server KMIP (Key Management Interoperability Protocol), consente al gestore di chiavi di comunicare con il cluster utilizzando KMIP su SSL. Ciò avviene quando un'applicazione o una determinata funzionalità (ad esempio, la funzionalità Storage Encryption) richiede chiavi sicure per fornire un accesso sicuro ai dati.

Generare una richiesta di firma del certificato per il cluster in ONTAP

È possibile utilizzare il certificato di protezione `generate-csr` Comando per generare una richiesta di firma del certificato (CSR). Una volta elaborata la richiesta, l'autorità di certificazione (CA) invia il certificato digitale firmato.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

Fasi

1. Generare una CSR:

```
security certificate generate-csr -common-name <FQDN_or_common_name>
-size 512|1024|1536|2048 -country <country> -state <state> -locality
<locality> -organization <organization> -unit <unit> -email-addr
<email_of_contact> -hash-function SHA1|SHA256|MD5
```

Ulteriori informazioni su `security certificate generate-csr` nella "Riferimento al comando ONTAP".

Il seguente comando crea una CSR con una chiave privata a 2,048 bit generata dalla funzione di hashing SHA256 per l'utilizzo da parte del gruppo Software nel reparto IT di una società il cui nome comune personalizzato è server1.companyname.com, con sede a Sunnyvale, California, USA. L'indirizzo e-mail dell'amministratore del contatto SVM è web@example.com. Il sistema visualizza la CSR e la chiave privata nell'output.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. Copiare la richiesta di certificato dall'output CSR, quindi inviarla in formato elettronico (ad esempio tramite e-mail) a una CA di terze parti attendibile per la firma.

   Una volta elaborata la richiesta, la CA invia il certificato digitale firmato. Conservare una copia della chiave privata e del certificato digitale firmato dalla CA.

Installare un certificato server firmato da CA per il cluster ONTAP

Per consentire a un server SSL di autenticare la macchina virtuale del cluster o dello storage (SVM) come client SSL, installare un certificato digitale con il tipo di client sul cluster o SVM. Quindi, fornire il certificato client-ca all'amministratore del server SSL per l'installazione sul server.

Prima di iniziare

È necessario aver già installato il certificato root del server SSL sul cluster o SVM con `server-ca` tipo di certificato.

Fasi

1. Per utilizzare un certificato digitale autofirmato per l'autenticazione del client, utilizzare `security certificate create` con il `type client` parametro.

   Ulteriori informazioni su `security certificate create` nella "Riferimento al comando ONTAP".

2. Per utilizzare un certificato digitale con firma CA per l'autenticazione del client, attenersi alla seguente procedura:

   a. Generare una richiesta di firma del certificato digitale (CSR) utilizzando il certificato di sicurezza `generate-csr` comando.

      ONTAP visualizza l'output CSR, che include una richiesta di certificato e una chiave privata, e ricorda

di copiare l'output in un file per riferimenti futuri.

b. Inviare la richiesta di certificato dall'output CSR in un formato elettronico (ad esempio un'e-mail) a una CA attendibile per la firma.

   Conservare una copia della chiave privata e del certificato firmato dalla CA per riferimenti futuri.

Una volta elaborata la richiesta, la CA invia il certificato digitale firmato.

a. Installare il certificato firmato dalla CA utilizzando `security certificate install` con il `-type client` parametro.
b. Quando richiesto, immettere il certificato e la chiave privata, quindi premere **Invio**.
c. Quando richiesto, immettere eventuali certificati root o intermedi aggiuntivi, quindi premere **Invio**.

   Se una catena di certificati che inizia dalla CA principale attendibile e termina con il certificato SSL emesso, non dispone dei certificati intermedi, è necessario installare un certificato intermedio sul cluster o sulla SVM. Un certificato intermedio è un certificato subordinato emesso dalla radice attendibile in modo specifico per il rilascio di certificati server di entità finale. Il risultato è una catena di certificati che inizia dalla CA principale attendibile, passa attraverso il certificato intermedio e termina con il certificato SSL emesso.

3. Fornire il `client-ca` Certificato del cluster o SVM all'amministratore del server SSL per l'installazione sul server.

   Il comando show del certificato di protezione con `-instance` e. `-type client-ca` parameters (parametri): visualizza `client-ca` informazioni sul certificato.

Informazioni correlate

- "installazione del certificato di sicurezza"
- "mostra certificato di sicurezza"

Installare un certificato client firmato da CA per il server KMIP in ONTAP

Il sottotipo di certificato del protocollo KMIP (Key Management Interoperability Protocol) (il parametro -subtype kmip-cert), insieme ai tipi client e server-ca, specifica che il certificato viene utilizzato per l'autenticazione reciproca del cluster e di un gestore di chiavi esterno, ad esempio un server KMIP.

A proposito di questa attività

Installare un certificato KMIP per autenticare un server KMIP come server SSL nel cluster.

Fasi

1. Utilizzare `security certificate install` con il `-type server-ca` e. `-subtype kmip-cert` Parametri per installare un certificato KMIP per il server KMIP.
2. Quando richiesto, immettere il certificato, quindi premere Invio.

   ONTAP ricorda di conservare una copia del certificato per riferimenti futuri.

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>
```

Informazioni correlate

- "installazione del certificato di sicurezza"

Informazioni sul copyright

Informazioni sul marchio commerciale