



Autenticare reciprocamente il cluster e un server KMIP

ONTAP 9

NetApp
February 12, 2026

Sommario

- Autenticare reciprocamente il cluster e un server KMIP 1
 - Autenticazione reciproca del cluster ONTAP e panoramica del server KMIP 1
 - Generare una richiesta di firma del certificato per il cluster in ONTAP 1
 - Installare un certificato server firmato da CA per il cluster ONTAP 2
 - Installare un certificato client firmato da CA per il server KMIP in ONTAP 3

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

Copyright © 2026 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.