Mutually authenticate the cluster and a KMIP server

ONTAP 9

NetApp
February 12, 2026

Table of Contents

Mutually authenticate the cluster and a KMIP server

Mutually authenticating the ONTAP cluster and a KMIP server overview

Mutually authenticating the cluster and an external key manager such as a Key Management Interoperability Protocol (KMIP) server enables the key manager to communicate with the cluster by using KMIP over SSL. You do so when an application or certain functionality (for example, the Storage Encryption functionality) requires secure keys to provide secure data access.

Generate a certificate signing request for the cluster in ONTAP

You can use the security certificate `generate-csr` command to generate a certificate signing request (CSR). After processing your request, the certificate authority (CA) sends you the signed digital certificate.

Before you begin

You must be a cluster administrator or SVM administrator to perform this task.

Steps

1. Generate a 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
```

Learn more about `security certificate generate-csr` in the ONTAP command reference.

The following command creates a CSR with a 2,048-bit private key generated by the SHA256 hashing function for use by the Software group in the IT department of a company whose custom common name is server1.companyname.com, located in Sunnyvale, California, USA. The email address of the SVM contact administrator is web@example.com. The system displays the CSR and the private key in the 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. Copy the certificate request from the CSR output, and then send it in electronic form (such as email) to a trusted third-party CA for signing.

   After processing your request, the CA sends you the signed digital certificate. You should keep a copy of the private key and the CA-signed digital certificate.

Install a CA-signed server certificate for the ONTAP cluster

To enable an SSL server to authenticate the cluster or storage virtual machine (SVM) as an SSL client, you install a digital certificate with the client type on the cluster or SVM. Then you provide the client-ca certificate to the SSL server administrator for installation on the server.

Before you begin

You must have already installed the root certificate of the SSL server on the cluster or SVM with the `server-ca` certificate type.

Steps

1. To use a self-signed digital certificate for client authentication, use the `security certificate create` command with the `type client` parameter.

   Learn more about `security certificate create` in the ONTAP command reference.

2. To use a CA-signed digital certificate for client authentication, complete the following steps:

   a. Generate a digital certificate signing request (CSR) by using the security certificate `generate-csr` command.

      ONTAP displays the CSR output, which includes a certificate request and private key, and reminds you to copy the output to a file for future reference.

   b. Send the certificate request from the CSR output in an electronic form (such as email) to a trusted CA

for signing.

You should keep a copy of the private key and the CA-signed certificate for future reference.

After processing your request, the CA sends you the signed digital certificate.

c. Install the CA-signed certificate by using the `security certificate install` command with the `-type client` parameter.

d. Enter the certificate and the private key when you are prompted, and then press **Enter**.

e. Enter any additional root or intermediate certificates when you are prompted, and then press **Enter**.

You install an intermediate certificate on the cluster or SVM if a certificate chain that begins at the trusted root CA, and ends with the SSL certificate issued to you, is missing the intermediate certificates. An intermediate certificate is a subordinate certificate issued by the trusted root specifically to issue end-entity server certificates. The result is a certificate chain that begins at the trusted root CA, goes through the intermediate certificate, and ends with the SSL certificate issued to you.

3. Provide the `client-ca` certificate of the cluster or SVM to the administrator of the SSL server for installation on the server.

The security certificate show command with the `-instance` and `-type client-ca` parameters displays the `client-ca` certificate information.

Related information

- security certificate install
- security certificate show

Install a CA-signed client certificate for the KMIP server in ONTAP

The certificate subtype of Key Management Interoperability Protocol (KMIP) (the -subtype kmip-cert parameter), along with the client and server-ca types, specifies that the certificate is used for mutually authenticating the cluster and an external key manager, such as a KMIP server.

About this task

Install a KMIP certificate to authenticate a KMIP server as an SSL server to the cluster.

Steps

1. Use the `security certificate install` command with the `-type server-ca` and `-subtype kmip-cert` parameters to install a KMIP certificate for the KMIP server.
2. When you are prompted, enter the certificate, and then press Enter.

ONTAP reminds you to keep a copy of the certificate for future reference.

```
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::>
```

Related information

- security certificate install

Copyright information

Trademark information