Authentifier mutuellement le cluster et un serveur KMIP

ONTAP 9

NetApp
April 24, 2024

Sommaire

Authentifier mutuellement le cluster et un serveur KMIP

Authentification mutuelle du cluster et présentation d'un serveur KMIP

L'authentification mutuelle du cluster et d'un gestionnaire de clés externe, tel qu'un serveur KMIP (Key Management Interoperability Protocol), permettent au gestionnaire de clés de communiquer avec le cluster via KMIP sur SSL. Dans ce cas, une application ou certaines fonctionnalités (par exemple, la fonctionnalité Storage Encryption) nécessitent des clés sécurisées pour assurer un accès sécurisé aux données.

Générer une demande de signature de certificat pour le cluster

Vous pouvez utiliser le certificat de sécurité `generate-csr` Commande pour générer une requête de signature de certificat (CSR). Après le traitement de votre demande, l'autorité de certification vous envoie le certificat numérique signé.

Ce dont vous avez besoin

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou un administrateur SVM.

Étapes

1. Générer une RSC :

   ```
   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
   ```

   Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

   La commande suivante crée une RSC avec une clé privée de 2,048 bits générée par la fonction de hachage SHA256, utilisée par le groupe Software dans LE département IT d'une société dont le nom commun personnalisé est server1.companyname.com, située à Sunnyvale (Californie), aux États-Unis. L'adresse e-mail de l'administrateur du contact SVM est web@example.com. Le système affiche la RSC et la clé privée dans la sortie.

```
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-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. Copiez la demande de certificat à partir de la sortie CSR, puis envoyez-la sous forme électronique (par exemple, un courriel) à une autorité de certification tierce approuvée pour signature.

   Après le traitement de votre demande, l'AC vous envoie le certificat numérique signé. Vous devez conserver une copie de la clé privée et du certificat numérique signé par l'autorité de certification.

Installez un certificat de serveur signé par l'autorité de certification pour le cluster

Pour permettre à un serveur SSL d'authentifier le cluster ou la machine virtuelle de stockage (SVM) en tant que client SSL, vous installez un certificat numérique avec le type client sur le cluster ou le SVM. Ensuite, vous fournissez le certificat client-CA à l'administrateur du serveur SSL pour l'installation sur le serveur.

Ce dont vous avez besoin

Vous devez déjà avoir installé le certificat root du serveur SSL sur le cluster ou SVM avec le `server-ca` type de certificat.

Étapes

1. Pour utiliser un certificat numérique auto-signé pour l'authentification client, utilisez le `security certificate create` commande avec `type client` paramètre.
2. Pour utiliser un certificat numérique signé par une autorité de certification pour l'authentification client, procédez comme suit :

   a. Générez une demande de signature de certificat numérique (RSC) à l'aide du certificat de sécurité `generate-csr` commande.

      ONTAP affiche la sortie CSR, qui comprend une demande de certificat et une clé privée, et vous rappelle de copier la sortie dans un fichier pour référence ultérieure.

   b. Envoyez la demande de certificat de la sortie CSR sous forme électronique (par exemple, un courriel) à une autorité de certification approuvée pour signature.

      Vous devez conserver une copie de la clé privée et du certificat signé par l'AC pour référence ultérieure.

   Après le traitement de votre demande, l'AC vous envoie le certificat numérique signé.

   a. Installez le certificat signé par l'autorité de certification à l'aide du `security certificate install` commande avec `-type client` paramètre.
   b. Entrez le certificat et la clé privée lorsque vous y êtes invité, puis appuyez sur **entrée**.
   c. Entrez tout certificat racine ou intermédiaire supplémentaire lorsque vous y êtes invité, puis appuyez sur **entrée**.

      Vous installez un certificat intermédiaire sur le cluster ou le SVM si une chaîne de certificats qui commence à l'autorité de certification racine de confiance et se termine par le certificat SSL qui vous est délivré, manque les certificats intermédiaires. Un certificat intermédiaire est un certificat subordonné délivré par la racine de confiance spécifiquement pour délivrer des certificats de serveur d'entité finale. Le résultat est une chaîne de certificats qui commence au niveau de l'autorité de certification racine de confiance, passe par le certificat intermédiaire et se termine par le certificat SSL qui vous a été délivré.

3. Fournir le `client-ca` Certificat du cluster ou SVM à l'administrateur du serveur SSL pour installation sur le serveur.

   Commande du certificat de sécurité show avec `-instance` et `-type client-ca` paramètres affiche le `client-ca` informations sur le certificat.

Installez un certificat client signé par une autorité de certification pour le serveur KMIP

Le sous-type de certificat du protocole KMIP (Key Management Interoperability Protocol) (paramètre -subtype kmip-cert), ainsi que les types client et serveur-ca, spécifie que le certificat est utilisé pour authentifier mutuellement le cluster et un gestionnaire de clés externe, comme un serveur KMIP.

Description de la tâche

Installez un certificat KMIP pour authentifier un serveur KMIP en tant que serveur SSL sur le cluster.

Étapes

1. Utilisez le `security certificate install` commande avec `-type server-ca` et `-subtype kmip-cert` Paramètres pour installer un certificat KMIP pour le serveur KMIP.
2. Lorsque vous y êtes invité, entrez le certificat, puis appuyez sur entrée.

   ONTAP vous rappelle de conserver une copie du certificat à des fins de référence ultérieure.

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

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG
2JhucwNhkcV8sEVAbkSdjbCxlnRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ
2HUw19JlYD1n1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
...
-----END CERTIFICATE-----


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

cluster1::>
```