# クラスタと**KMIP**サーバの相互認証

ONTAP 9

NetApp
February 12, 2026

# 目次

# クラスタとKMIPサーバの相互認証

## ONTAPクラスタとKMIPサーバの相互認証の概要

クラスタと外部キーマネージャ（Key Management Interoperability Protocol（KMIP）サーバなど）を相互認証することで、キーマネージャはSSL経由のKMIPを使用してクラスタと通信できるようになります。これは、アプリケーションまたは特定の機能（ストレージ暗号化機能など）が、安全なデータアクセスを提供するために安全なキーを必要とする場合に行います。

## ONTAP でクラスタの証明書署名要求を生成する

セキュリティ証明書 `generate-csr`コマンドを使用して、証明書署名要求（CSR）を生成できます。要求が処理されると、証明機関（CA）が署名されたデジタル証明書を送信します。

開始する前に

このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。

手順

1. CSRを生成します。

```
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
```

`security certificate generate-csr`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-certificate-generate-csr.html["ONTAPコマンド リファレンス"^]をご覧ください。

次のコマンドは、SHA256ハッシュ関数で生成される2,048ビット秘密鍵を使用して、CSRを作成します。この証明書は、米国カリフォルニア州のサニーベールにある企業（カスタム共通名server1.companyname.com）のIT部門のソフトウェア グループが使用します。SVM担当管理者のEメール アドレスは\web@example.comです。出力にはCSRと秘密鍵が表示されます。

```
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. CSR出力の証明書要求をデジタル形式（Eメールなど）で信頼できるサードパーティのCAに送信し、署名を求めます。

   要求が処理されると、署名済みのデジタル証明書がCAから送信されます。秘密鍵とCA署名デジタル証明書のコピーを保管する必要があります。

# ONTAPクラスタ用のCA署名サーバ証明書をインストールする

SSLサーバがクラスタまたはStorage Virtual Machine（SVM）をSSLクライアントとして認証できるようにするには、クラスタまたはSVMにクライアント タイプのデジタル証明書をインストールします。次に、SSLサーバ管理者にclient-ca証明書を提供し、サーバにインストールしてもらいます。

開始する前に

`server-ca`証明書タイプを使用して、クラスタまたはSVMに
SSLサーバのルート証明書がすでにインストールされている必要があります。

手順

1. クライアント認証に自己署名デジタル証明書を使用するには、 `type client`パラメータを指定して `security certificate create`コマンドを使用します。

   `security certificate create`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-certificate-create.html["ONTAPコマンド リファレンス"^]をご覧ください。

2. クライアント認証にCA署名デジタル証明書を使用するには、次の手順を実行します：

a. security certificate `generate-csr`コマンドを使用して、デジタル証明書署名要求（CSR）を生成します。

   ONTAP は、証明書要求と秘密キーを含む CSR 出力を表示し、将来の参照用に出力をファイルにコピーするように通知します。

b. CSR 出力からの証明書要求を電子形式（電子メールなど）で信頼できる CA に送信し、署名を依頼します。

   将来の参照用に、秘密キーと CA 署名証明書のコピーを保管しておく必要があります。

要求が処理されると、署名済みのデジタル証明書がCAから送信されます。

a. `-type client`パラメータを指定した `security certificate install`コマンドを使用して、CA署名証明書をインストールします。
b. プロンプトが表示されたら証明書と秘密キーを入力し、*Enter*キーを押します。
c. プロンプトが表示されたら追加のルート証明書または中間証明書を入力し、*Enter*キーを押します。

   信頼されたルートCAから始まり、お客様に発行されたSSL証明書で終わる証明書チェーンに中間証明書がない場合は、クラスタまたはSVMに中間証明書をインストールします。中間証明書は、エンドエンティティサーバ証明書を発行するために信頼されたルートCAによって発行される従属証明書です。その結果、信頼されたルートCAから始まり、中間証明書を経由して、お客様に発行されたSSL証明書で終わる証明書チェーンが作成されます。

3. クラスタまたは SVM の `client-ca`証明書を SSL サーバーの管理者に提供し、サーバーにインストールしてもらいます。

   `-instance`および `-type client-ca`パラメータを指定した `security certificate show` コマンドは、 `client-ca`証明書情報を表示します。

関連情報

- "security certificate install"
- "セキュリティ証明書の表示"

# ONTAPにKMIPサーバー用のCA署名付きクライアント証明書をインストールする

Key Management Interoperability Protocol（KMIP）の証明書サブタイプ（-subtype kmip-certパラメータ）は、clientおよびserver-caタイプとともに、証明書がクラスタとKMIPサーバなどの外部キー マネージャとの相互認証に使用されることを指定します。

タスク概要

KMIP 証明書をインストールして、KMIP サーバーをクラスタの SSL サーバーとして認証します。

手順

1. `-type server-ca`および `-subtype kmip-cert`パラメータを指定した `security certificate install`コマンドを使

用して、KMIPサーバーのKMIP証明書をインストールします。

2. プロンプトが表示されたら、証明書を入力し、Enterキーを押します。

   ONTAP は、将来の参照用に証明書のコピーを保管しておくように通知します。

```
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::>
```

関連情報

- "security certificate install"

## 著作権に関する情報



## 商標に関する情報