クラスタと**KMIP**サーバの相互認証

ONTAP 9

NetApp
April 24, 2024

目次

クラスタとKMIPサーバの相互認証

クラスタと KMIP サーバの相互認証の概要

Key Management Interoperability Protocol （ KMIP ）サーバなど、クラスタと外部キー管理ツールを相互認証することで、キー管理ツールが SSL を介した KMIP を使用してクラスタと通信できるようになります。この設定は、特定のアプリケーションや機能（ストレージ暗号化機能など）で、データアクセスの安全性を確保するためにセキュアなキーが必要とされる場合に使用します。

クラスタの証明書署名要求を生成します

セキュリティ証明書を使用できます `generate-csr` 証明書署名要求（CSR）を生成するコマンド。要求が処理されると、署名済みのデジタル証明書が認証局（ CA ）から送信されます。

必要なもの

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

   コマンド構文全体については、マニュアルページを参照してください。

   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 CSR は、米国カリフォルニア州のサニーベールにある server1.companyname.com というカスタム共通名の企業の 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。CSR と秘密鍵が出力に表示されます。

```
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-----
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. 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は保管する必要があります。

クラスタの **CA** 署名済みサーバ証明書をインストールします

SSL サーバでクラスタまたは Storage Virtual Machine （ SVM ）を SSL クライアントとして認証するためには、 client タイプのデジタル証明書をクラスタまたは SVM にインストールします。次に、 client-ca 証明書をその SSL サーバの管理者に渡してインストールしてもらいます。

必要なもの

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をインストールしておく必要があります `server-ca` 証明書のタイプ。

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、を使用します `security certificate create` コマンドにを指定します `type client` パラメータ
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. セキュリティ証明書を使用して、証明書署名要求（CSR）を生成します `generate-csr` コマンドを実行します

      証明書要求と秘密鍵を含む CSR 出力が表示され、今後の参照用にファイルにコピーするよう求められます。 ONTAP

   b. 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 CA に送信し、署名を求めます。

      秘密鍵と CA 署名証明書のコピーは今後の参照用として保管しておいてください。

   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. を使用してCA署名証明書をインストールします `security certificate install` コマンドにを指定します `-type client` パラメータ
   b. プロンプトが表示されたら証明書と秘密鍵を入力し、 * 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。

      信頼できるルート CA から発行された SSL 証明書に至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、問題のエンドエンティティのサーバ証明書専用に信頼できるルートから発行される、副次的な証明書です。この結果、信頼できるルート CA から始まり、中間証明書を経て、発行された SSL 証明書で終わる証明書チェーンが形成されます。

3. を指定します `client-ca` クラスタまたはSVMの証明書。サーバにインストールするためのSSLサーバの管理者への証明書。

   security certificate showコマンドとを使用します `-instance` および `-type client-ca` が表示されます `client-ca` 証明書情報。

KMIP サーバの CA 署名済みクライアント証明書をインストールします

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 のタイプと組み合わせて適用され、クラスタと外部キー管理ツール（ KMIP サーバなど）の相互認証に使用される証明書であることを示します。

このタスクについて

KMIP サーバをクラスタに対して SSL サーバとして認証する KMIP 証明書をインストールします。

手順

1. を使用します `security certificate install` コマンドにを指定します `-type server-ca` および

`-subtype kmip-cert` KMIPサーバ用のKMIP証明書をインストールするためのパラメータ。

2. プロンプトが表示されたら、証明書を入力して Enter キーを押します。

   今後の参照用として証明書のコピーを保管するように ONTAP から求められます。

```
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::>
```