클러스터와 **KMIP** 서버를 상호 인증합니다

ONTAP 9

NetApp
April 24, 2024

목차

클러스터와 **KMIP** 서버를 상호 인증합니다

클러스터 및 **KMIP** 서버 개요를 상호 인증

KMIP(Key Management Interoperability Protocol) 서버와 같은 외부 키 관리자를 함께 사용하면 키 관리자가 SSL을 통해 KMIP를 사용하여 클러스터와 통신할 수 있습니다. 애플리케이션 또는 특정 기능(예: 스토리지 암호화 기능)에서 보안 데이터 액세스를 제공하기 위해 보안 키가 필요한 경우 이 작업을 수행합니다.

클러스터에 대한 인증서 서명 요청을 생성합니다

보안 인증서 'generate-csr' 명령을 사용하여 인증서 서명 요청(CSR)을 생성할 수 있습니다. 요청을 처리한 후 CA(인증 기관)에서 서명된 디지털 인증서를 보냅니다.

필요한 것

이 작업을 수행하려면 클러스터 관리자 또는 SVM 관리자여야 합니다.

단계

1. CSR 생성:

   '* 보안 인증서 생성 - csr-common-name_FQDN_or_common_name_-size 512 | 1024 | 1536 | 2048-country_country_-state_-지역성_-organization_organization_-unit_unit_-email-addr_email_of_contact_-hash-function SHA1 | SHA256 | MD5*'

   전체 명령 구문은 man 페이지를 참조하십시오.

   다음 명령은 SHA256 해싱 기능에 의해 생성된 2,048비트 개인 키를 가진 CSR을 생성하고, 사용자 정의 공통 이름이 server1.companyname.com 인 회사의 IT 부서에서 사용하는 사용자 정의 공용 키가 미국 캘리포니아주 서니베일에 있습니다. SVM 연락처 관리자의 이메일 주소는 web@example.com 입니다. 출력에 CSR과 개인 키가 표시됩니다.

```
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 출력에서 인증서 요청을 복사한 다음 전자 양식(예: 전자 메일)으로 신뢰할 수 있는 타사 CA로 보내 서명합니다.

   요청을 처리한 후 CA는 서명된 디지털 인증서를 보냅니다. 개인 키와 CA 서명 디지털 인증서의 복사본을 유지해야 합니다.

클러스터에 대한 **CA** 서명 서버 인증서를 설치합니다

SSL 서버에서 클러스터 또는 SVM(Storage Virtual Machine)을 SSL 클라이언트로 인증할 수 있도록 하려면 클러스터 또는 SVM에 클라이언트 유형과 함께 디지털 인증서를 설치합니다. 그런 다음 서버에 설치하기 위해 SSL 서버 관리자에게 클라이언트-CA 인증서를 제공합니다.

필요한 것

SSL 서버의 루트 인증서를 이미 클러스터 또는 SVM에 'server-ca' 인증서 유형으로 설치해야 합니다.

단계

1. 클라이언트 인증에 자체 서명된 디지털 인증서를 사용하려면 type client 매개 변수를 사용하여 Security certificate create 명령을 사용합니다.

2. 클라이언트 인증에 CA 서명 디지털 인증서를 사용하려면 다음 단계를 수행하십시오.

   a. 보안 인증서 'generate-csr' 명령을 사용하여 디지털 인증서 서명 요청(CSR)을 생성합니다.

      ONTAP는 인증서 요청과 개인 키가 포함된 CSR 출력을 표시하고 나중에 참조할 수 있도록 출력을 파일로 복사하도록 알려 줍니다.

   b. 전자 양식(예: 전자 메일)으로 CSR 출력에서 인증서 요청을 신뢰할 수 있는 CA로 보내 서명합니다.

      나중에 참조할 수 있도록 개인 키와 CA 서명 인증서의 복사본을 유지해야 합니다.

   요청을 처리한 후 CA는 서명된 디지털 인증서를 보냅니다.

   a. '-type client' 매개 변수와 함께 보안 인증서 설치 명령을 사용하여 CA 서명 인증서를 설치합니다.
   b. 메시지가 표시되면 인증서와 개인 키를 입력한 다음 * Enter * 키를 누릅니다.
   c. 메시지가 표시되면 추가 루트 또는 중간 인증서를 입력하고 * Enter * 를 누릅니다.

      신뢰할 수 있는 루트 CA에서 시작하고 사용자에게 발급된 SSL 인증서로 끝나는 인증서 체인이 중간 인증서를 누락하는 경우 클러스터나 SVM에 중간 인증서를 설치합니다. 중간 인증서는 최종 엔터티 서버 인증서를 발급하기 위해 신뢰할 수 있는 루트에서 발급하는 하위 인증서입니다. 그 결과 신뢰할 수 있는 루트 CA에서 시작하여 중간 인증서를 거쳐 사용자에게 발급된 SSL 인증서로 끝나는 인증서 체인이 만들어집니다.

3. 서버에 설치하기 위해 SSL 서버 관리자에게 클러스터 또는 SVM의 '클라이언트-CA' 인증서를 제공합니다.

   인스턴스, 클라이언트-CA 형식의 매개 변수를 가진 보안 인증서 표시 명령은 클라이언트-CA 인증서 정보를 표시합니다.

KMIP 서버용 CA 서명 클라이언트 인증서를 설치합니다

클라이언트 및 서버 CA 유형과 함께 KMIP(Key Management Interoperability Protocol)(-subtype KMIP-cert 매개 변수)의 인증서 하위 유형은 클러스터 및 KMIP 서버와 같은 외부 키 관리자를 상호 인증하는 데 인증서가 사용됨을 나타냅니다.

이 작업에 대해

KMIP 인증서를 설치하여 KMIP 서버를 클러스터에 대한 SSL 서버로 인증합니다.

단계

1. KMIP 서버용 KMIP 인증서를 설치하려면 '-type server-ca' 및 '-subtype KMIP-cert' 매개 변수와 함께 'Security certificate install' 명령을 사용하십시오.
2. 메시지가 표시되면 인증서를 입력한 다음 Enter 키를 누릅니다.

   ONTAP는 나중에 참조할 수 있도록 인증서 복사본을 보관하도록 알려 줍니다.

```
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::>
```