



클러스터와 **KMIP** 서버를 상호 인증합니다

ONTAP 9

NetApp
April 24, 2024

목차

클러스터와 KMIP 서버를 상호 인증합니다	1
클러스터 및 KMIP 서버 개요를 상호 인증	1
클러스터에 대한 인증서 서명 요청을 생성합니다	1
클러스터에 대한 CA 서명 서버 인증서를 설치합니다	2
KMIP 서버용 CA 서명 클라이언트 인증서를 설치합니다	3

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-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGx1LmNvbTELMakGA1UEBhMCVVMx
CTAHBgNVBAgtADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxC TAHBgNVBAStADEPMA0G
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJbmXuj6U3alwoUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBcWUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJb
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+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.

ONTAP은 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.

ONTAP은 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  
2JhucwNhkcV8sEVAbkSdjbCxlRhLQ2pRdKkkirWmnWXbj9T/UWZyB2oK0z5XqcJ  
2HUw19JlYDln1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
```

...

-----END CERTIFICATE-----

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

```
cluster1::>
```

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.