# 관리자 계정을 관리합니다

## ONTAP 9

NetApp
September 12, 2024

# 목차

# 관리자 계정을 관리합니다

## 관리자 계정 관리 개요

계정 액세스를 설정한 방법에 따라 공개 키를 로컬 계정에 연결하거나, CA 서명 서버 디지털 인증서를 설치하거나, AD, LDAP 또는 NIS 액세스를 구성해야 할 수 있습니다. 계정 액세스를 활성화하기 전이나 후에 이러한 모든 작업을 수행할 수 있습니다.

## 공개 키를 관리자 계정에 연결합니다

SSH 공개 키 인증의 경우 계정에서 SVM에 액세스할 수 있으려면 먼저 공개 키를 관리자 계정과 연결해야 합니다. 'Security login publickey create' 명령어를 이용하여 관리자 계정에 키를 연결할 수 있다.

이 작업에 대해

암호 및 SSH 공개 키로 SSH를 통해 계정을 인증하면 먼저 공개 키로 계정이 인증됩니다.

시작하기 전에

- SSH 키를 생성해야 합니다.
- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. 공개 키를 관리자 계정에 연결:

   '보안 로그인 공개 키 생성 - vserver_SVM_name_-username_user_name_-index_index_-publickey_certificate_-comment_comment_'

   전체 명령 구문은 에 대한 워크시트 참조를 참고하십시오 "공개 키를 사용자 계정과 연결".

2. 공개 키를 확인하여 변경 사항을 확인합니다.

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

예

다음 명령을 실행하면 공용 키가 SVM 관리자 계정에 연결됩니다 `svmadmin1` SVM을 위해 `engData1`. 공개 키에는 인덱스 번호 5가 할당됩니다.

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

# 관리자 계정에 대한 SSH 공개 키와 X.509 인증서를 관리합니다

관리자 계정으로 SSH 인증 보안을 강화하기 위해 를 사용할 수 있습니다 `security login publickey` SSH 공개 키 및 X.509 인증서와의 연결을 관리하는 명령 집합입니다.

## 공개 키와 X.509 인증서를 관리자 계정에 연결합니다

ONTAP 9.13.1 부터는 X.509 인증서를 관리자 계정과 연결된 공개 키와 연결할 수 있습니다. 이렇게 하면 해당 계정에 대한 SSH 로그인 시 인증서 만료 또는 해지 확인을 추가로 보호할 수 있습니다.

이 작업에 대해

SSH 공개 키와 X.509 인증서를 모두 사용하여 SSH를 통해 계정을 인증하는 경우 ONTAP는 SSH 공개 키로 인증하기 전에 X.509 인증서의 유효성을 검사합니다. 인증서가 만료되거나 해지되면 SSH 로그인이 거부되고 공개 키는 자동으로 비활성화됩니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.
- SSH 키를 생성해야 합니다.
- X.509 인증서만 만료 여부를 확인해야 하는 경우 자체 서명된 인증서를 사용할 수 있습니다.
- X.509 인증서의 만료 및 해지 여부를 확인해야 하는 경우:
  - CA(인증 기관)로부터 인증서를 받아야 합니다.
  - 를 사용하여 인증서 체인(중간 및 루트 CA 인증서)을 설치해야 합니다 `security certificate install` 명령.
  - SSH용 OCSP를 활성화해야 합니다. 을 참조하십시오 "디지털 인증서가 OCSP를 사용하여 유효한지 확인합니다" 를 참조하십시오.

단계

1. 공개 키와 X.509 인증서를 관리자 계정에 연결합니다.

   ```
   security login publickey create -vserver SVM_name -username user_name -index
   index -publickey certificate -x509-certificate install
   ```

   전체 명령 구문은 에 대한 워크시트 참조를 참고하십시오 "공개 키를 사용자 계정과 연결".

2. 공개 키를 확인하여 변경 사항을 확인합니다.

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

예

다음 명령을 실행하면 공용 키와 X.509 인증서가 SVM 관리자 계정에 연결됩니다 `svmadmin2` SVM을 위해 `engData2`. 공개 키에는 인덱스 번호 6이 할당됩니다.

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

## 관리자 계정의 **SSH** 공개 키에서 인증서 연결을 제거합니다

공개 키를 유지하면서 계정의 SSH 공개 키에서 현재 인증서 연결을 제거할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. 관리자 계정에서 X.509 인증서 연결을 제거하고 기존 SSH 공개 키를 유지합니다.

   `security login publickey modify -vserver SVM_name -username user_name -index index -x509-certificate delete`

2. 공개 키를 확인하여 변경 사항을 확인합니다.

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

예

다음 명령을 실행하면 SVM 관리자 계정에서 X.509 인증서 연결이 제거됩니다 `svmadmin2` SVM을 위해 `engData2` 인덱스 번호 6.

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -index 6 -x509-certificate delete
```

## 관리자 계정에서 공개 키 및 인증서 연결을 제거합니다

계정에서 현재 공개 키 및 인증서 구성을 제거할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. 관리자 계정에서 공개 키와 X.509 인증서 연결을 제거합니다.

   `security login publickey delete -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

2. 공개 키를 확인하여 변경 사항을 확인합니다.

```
security login publickey show -vserver SVM_name -username user_name -index
index
```

예

다음 명령을 실행하면 SVM 관리자 계정에서 공개 키와 X.509 인증서가 제거됩니다 `svmadmin3` SVM을 위해 `engData3` 인덱스 번호 7.

```
cluster1::> security login publickey delete -vserver engData3 -username
svmadmin3 -index 7
```

# SSH 로그인에 Cisco Duo 2FA를 구성합니다

ONTAP 9.14.1부터 SSH 로그인 시 2FA(2단계 인증)에 Cisco Duo를 사용하도록 ONTAP를 구성할 수 있습니다. 클러스터 수준에서 Duo를 구성하면 기본적으로 모든 사용자 계정에 적용됩니다. 또는 스토리지 VM(이전에는 가상 머신이라고 함) 레벨에서 Duo를 구성할 수 있습니다. 이 경우 스토리지 VM의 사용자에게만 적용됩니다. Duo를 활성화하고 구성하면 모든 사용자에 대한 기존 방법을 보완하는 추가 인증 방법으로 사용됩니다.

SSH 로그인에 대해 Duo 인증을 사용하는 경우 사용자는 다음에 SSH를 사용하여 로그인할 때 장치를 등록해야 합니다. 등록 정보는 Cisco Duo를 참조하십시오 "등록 문서".

ONTAP 명령줄 인터페이스를 사용하여 Cisco Duo에서 다음 작업을 수행할 수 있습니다.

- Cisco Duo를 구성합니다
- Cisco Duo 구성을 변경합니다
- Cisco Duo 구성을 제거합니다
- Cisco Duo 구성을 봅니다
- Duo 그룹을 제거합니다
- Duo 그룹 보기
- 사용자를 위한 Duo 인증 우회

## Cisco Duo를 구성합니다

를 사용하여 전체 클러스터 또는 특정 스토리지 VM(ONTAP CLI에서 가상 서버라고 함)에 대한 Cisco Duo 구성을 생성할 수 있습니다 `security login duo create` 명령. 이렇게 하면 이 클러스터 또는 스토리지 VM에 대한 SSH 로그인에 Cisco Duo가 활성화됩니다.

단계

1. Cisco Duo Admin Panel에 로그인합니다.
2. 애플리케이션 > UNIX 애플리케이션 * 으로 이동합니다.
3. 통합 키, 비밀 키 및 API 호스트 이름을 기록합니다.
4. SSH를 사용하여 ONTAP 계정에 로그인합니다.

5. 이 스토리지 VM에 대해 Cisco Duo 인증을 사용하도록 설정하고, 환경 정보를 괄호 안의 값으로 대체합니다.

```
security login duo create \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME>
```

이 명령의 필수 및 선택적 매개 변수에 대한 자세한 내용은 을 참조하십시오 "관리자 인증 및 RBAC 구성을 위한 워크시트".

## Cisco Duo 구성을 변경합니다

Cisco Duo가 사용자를 인증하는 방법(예: 받은 인증 프롬프트 수 또는 사용된 HTTP 프록시)을 변경할 수 있습니다. 스토리지 VM(ONTAP CLI에서 가상 서버로 표시됨)에 대한 Cisco Duo 구성을 변경해야 하는 경우 를 사용할 수 있습니다 `security login duo modify` 명령.

단계

1. Cisco Duo Admin Panel에 로그인합니다.
2. 애플리케이션 > UNIX 애플리케이션 * 으로 이동합니다.
3. 통합 키, 비밀 키 및 API 호스트 이름을 기록합니다.
4. SSH를 사용하여 ONTAP 계정에 로그인합니다.
5. 이 스토리지 VM에 대한 Cisco Duo 구성을 변경하여 환경의 업데이트된 정보를 괄호 안의 값으로 대체합니다.

```
security login duo modify \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME> \
-pushinfo true|false \
-http-proxy <HTTP_PROXY_URL> \
-autopush true|false \
-prompts 1|2|3 \
-max-unenrolled-logins <NUM_LOGINS> \
-is-enabled true|false \
-fail-mode safe|secure
```

## Cisco Duo 구성을 제거합니다

Cisco Duo 구성을 제거하면 SSH 사용자가 로그인할 때 Duo를 사용하여 인증할 필요가 없습니다. 스토리지 VM에 대한 Cisco Duo 구성(ONTAP CLI에서 가상 서버라고 함)을 제거하려면 을 사용합니다 `security login duo delete` 명령.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. 스토리지 VM 이름을 로 대체하여 이 스토리지 VM에 대한 Cisco Duo 구성을 제거합니다 `<STORAGE_VM_NAME>`:

```
security login duo delete  -vserver <STORAGE_VM_NAME>
```

이렇게 하면 이 스토리지 VM에 대한 Cisco Duo 구성이 영구적으로 삭제됩니다.

## Cisco Duo 구성을 봅니다

를 사용하여 스토리지 VM(ONTAP CLI에서 가상 서버로 지칭)에 대한 기존 Cisco Duo 구성을 볼 수 있습니다 `security login duo show` 명령.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. 이 스토리지 VM에 대한 Cisco Duo 구성을 표시합니다. 필요한 경우 를 사용할 수 있습니다 `vserver` 스토리지 VM 이름을 로 대체하는 스토리지 VM을 지정하는 매개 변수입니다 `<STORAGE_VM_NAME>`:

```
security login duo show -vserver <STORAGE_VM_NAME>
```

다음과 유사한 출력이 표시됩니다.

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

## Duo 그룹을 생성합니다

Cisco Duo에 특정 Active Directory, LDAP 또는 로컬 사용자 그룹의 사용자만 Duo 인증 프로세스에 포함하도록 지시할 수 있습니다. Duo 그룹을 생성하는 경우 해당 그룹의 사용자만 Duo 인증을 요구합니다. 를 사용하여 Duo 그룹을 만들 수 있습니다 `security login duo group create` 명령. 그룹을 생성할 때 필요에 따라 해당 그룹의

특정 사용자를 Duo 인증 프로세스에서 제외할 수 있습니다.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. 환경의 정보를 대괄호로 묶은 값으로 대체하여 Duo 그룹을 만듭니다. 를 생략할 경우 `-vserver` 매개 변수로, 그룹이 클러스터 레벨에서 생성됩니다.

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -exclude-users <USER1, USER2>
```

Duo 그룹의 이름은 Active Directory, LDAP 또는 로컬 그룹과 일치해야 합니다. 옵션을 사용하여 지정하는 사용자입니다 `-exclude-users` 매개변수는 Duo 인증 프로세스에 포함되지 않습니다.

## Duo 그룹 보기

를 사용하여 기존 Cisco Duo 그룹 항목을 볼 수 있습니다 `security login duo group show` 명령.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. 환경의 정보를 대괄호로 묶은 값으로 대체하여 Duo 그룹 항목을 표시합니다. 를 생략할 경우 `-vserver` 매개 변수로, 그룹이 클러스터 레벨에 표시됩니다.

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -exclude-users <USER1, USER2>
```

Duo 그룹의 이름은 Active Directory, LDAP 또는 로컬 그룹과 일치해야 합니다. 옵션을 사용하여 지정하는 사용자입니다 `-exclude-users` 매개 변수가 표시되지 않습니다.

## Duo 그룹을 제거합니다

를 사용하여 Duo 그룹 항목을 제거할 수 있습니다 `security login duo group delete` 명령. 그룹을 제거하면 해당 그룹의 사용자가 Duo 인증 프로세스에 더 이상 포함되지 않습니다.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. Duo 그룹 항목을 제거하여 환경의 정보를 대괄호 안의 값으로 대체합니다. 를 생략할 경우 `-vserver` 매개 변수로, 그룹이 클러스터 레벨에서 제거됩니다.

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME>
```

Duo 그룹의 이름은 Active Directory, LDAP 또는 로컬 그룹과 일치해야 합니다.

### 사용자를 위한 **Duo** 인증 우회

Duo SSH 인증 프로세스에서 모든 사용자 또는 특정 사용자를 제외할 수 있습니다.

#### 모든 **Duo** 사용자를 제외합니다

모든 사용자에 대해 Cisco Duo SSH 인증을 비활성화할 수 있습니다.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. SSH 사용자에 대해 Cisco Duo 인증을 사용하지 않도록 설정하고 SVM 이름을 로 바꿉니다 `<STORAGE_VM_NAME>`:

```
security login duo -vserver <STORAGE_VM_NAME> -is-duo-enabled-false
```

#### **Duo** 그룹 사용자를 제외합니다

Duo 그룹에 속한 특정 사용자를 Duo SSH 인증 프로세스에서 제외할 수 있습니다.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. 그룹의 특정 사용자에 대해 Cisco Duo 인증을 비활성화합니다. 제외할 그룹 이름 및 사용자 목록을 대괄호 안의 값으로 대체합니다.

```
security login group modify -group-name <GROUP_NAME> -exclude-users
<USER1, USER2>
```

Duo 그룹의 이름은 Active Directory, LDAP 또는 로컬 그룹과 일치해야 합니다. 로 지정한 사용자 `-exclude -users` 매개변수는 Duo 인증 프로세스에 포함되지 않습니다.

#### 로컬 **Duo** 사용자를 제외합니다

Cisco Duo Admin Panel을 사용하여 특정 로컬 사용자를 Duo 인증을 사용하지 않도록 제외할 수 있습니다. 자세한 내용은 를 참조하십시오 "Cisco Duo 설명서".

## **CA** 서명 서버 인증서 개요 생성 및 설치

운영 시스템에서 클러스터 또는 SVM을 SSL 서버로 인증하는 데 사용할 CA 서명 디지털 인증서를 설치하는 것이 좋습니다. 'Security certificate generate -csr' 명령어를 이용하여 CSR(certificate signing request)과 'security certificate install' 명령어를 이용하여 인증 기관으로부터 받은 인증서를 설치할 수 있다.

## 인증서 서명 요청을 생성합니다

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

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. CSR 생성:

   'Security certificate generate - csr -common -name FQDN_or_common_name - size 512 | 1024 | 1536 | 2048 - 국가-주-시/도-구/군-기관-조직-단위 장치-전자 메일_of_contact-hash-function SHA1 | SHA256 | MD5'

   다음 명령은 미국 캘리포니아주 서니베일에 위치한 'server1.companyname.com`" 사용자 정의 공통 이름을 가진 회사의 IT 부서의 '소프트웨어' 그룹에서 'sha256' 해시 기능에서 생성된 2048비트 개인 키로 CSR을 만듭니다. SVM 담당자 관리자의 이메일 주소는 ""web@example.com""입니다. 출력에 CSR과 개인 키가 표시됩니다.

**CSR** 생성 예

```
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 :
-----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.

## **CA** 서명 서버 인증서를 설치합니다

'보안 인증서 설치' 명령을 사용하여 SVM에 CA 서명 서버 인증서를 설치할 수 있습니다. ONTAP는 서버 인증서의 인증서 체인을 형성하는 CA(인증 기관) 루트 및 중간 인증서를 입력하라는 메시지를 표시합니다.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. CA 서명 서버 인증서 설치:

   ```
   security certificate install -vserver SVM_name -type certificate_type
   ```

   전체 명령 구문은 을 참조하십시오 "워크시트".

   > ONTAP 서버 인증서의 인증서 체인을 형성하는 CA 루트 및 중간 인증서를 입력하라는 메시지가 표시됩니다. 체인은 서버 인증서를 발급한 CA의 인증서로 시작되며 CA의 루트 인증서까지 범위가 될 수 있습니다. 누락된 중간 인증서는 서버 인증서 설치에 실패합니다.

   다음 명령을 실행하면 CA 서명 서버 인증서와 중간 인증서가 SVM ""engData2""에 설치됩니다.

**CA** 서명 서버 인증서 중간 인증서 설치 예

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADEJMAcGA1UECxMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuSl8U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEAr1mnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAzt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRoZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
```

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0
IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENs
YXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDExhodHRw
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: n

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

# System Manager를 사용하여 인증서를 관리합니다

## ONTAP 9.10.1부터 시스템 관리자를 사용하여 신뢰할 수 있는 인증서 기관, 클라이언트/서버 인증서 및 로컬(온보드) 인증서 기관을 관리할 수 있습니다.

System Manager를 사용하면 다른 응용 프로그램에서 받은 인증서를 관리할 수 있으므로 해당 응용 프로그램의 통신을 인증할 수 있습니다. 시스템을 다른 응용 프로그램에 식별하는 고유한 인증서를 관리할 수도 있습니다.

### 인증서 정보를 봅니다

System Manager를 사용하면 클러스터에 저장된 신뢰할 수 있는 인증서 기관, 클라이언트/서버 인증서 및 로컬 인증서 기관을 볼 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 영역으로 스크롤합니다. 인증서 * 섹션에 다음 세부 정보가 표시됩니다.
   - 저장된 신뢰할 수 있는 인증 기관의 수입니다.
   - 저장된 클라이언트/서버 인증서 수
   - 저장된 로컬 인증 기관의 수입니다.
3. 인증서 범주에 대한 세부 정보를 보려면 숫자를 선택하고, 모든 범주에 대한 정보가 포함된 * 인증서 * 페이지를 열려면 선택합니다 → . 이 목록에는 전체 클러스터에 대한 정보가 표시됩니다. 특정 스토리지 VM에 대한 정보만 표시하려면 다음 단계를 수행하십시오.
   a. 스토리지 > 스토리지 VM * 을 선택합니다.
   b. 스토리지 VM을 선택합니다.
   c. 설정 * 탭으로 전환합니다.

d. 인증서 * 섹션에 표시된 번호를 선택합니다.

다음 단계

- 인증서 * 페이지에서 을(를) 사용할 수 있습니다 인증서 서명 요청을 생성합니다.
- 인증서 정보는 세 개의 탭으로 구분됩니다. 각 범주마다 하나씩 있습니다. 각 탭에서 다음 작업을 수행할 수 있습니다.

| 이 탭에서… | 다음 절차를 수행할 수 있습니다… |
|---|---|
| • 신뢰할 수 있는 인증 기관 * | • [install-trusted-cert]<br>• 신뢰할 수 있는 인증 기관을 삭제합니다<br>• 신뢰할 수 있는 인증 기관을 갱신합니다 |
| • 클라이언트/서버 인증서 * | • [install-cs-cert]<br>• [gen-cs-cert]<br>• [delete-cs-cert]<br>• [renew-cs-cert] |
| • 로컬 인증 기관 * | • 새 로컬 인증 기관을 생성합니다<br>• 로컬 인증 기관을 사용하여 인증서에 서명합니다<br>• 로컬 인증 기관을 삭제합니다<br>• 로컬 인증 기관을 갱신합니다 |

## 인증서 서명 요청을 생성합니다

인증서 * 페이지의 아무 탭에서나 System Manager를 사용하여 CSR(인증서 서명 요청)을 생성할 수 있습니다. 개인 키와 해당하는 CSR이 생성되며, 이 키는 인증 기관을 통해 서명하여 공용 인증서를 생성할 수 있습니다.

단계

1. 인증서 * 페이지를 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. CSR 생성 * 을 선택합니다.
3. 주체 이름에 대한 정보를 입력합니다.
   a. 일반 이름 * 을 입력합니다.
   b. 국가 * 를 선택합니다.
   c. 조직 * 을 입력합니다.
   d. 조직 단위 * 를 입력합니다.
4. 기본값을 무시하려면 * 추가 옵션 * 을 선택하고 추가 정보를 제공합니다.

## 신뢰할 수 있는 인증 기관을 설치(추가)합니다

신뢰할 수 있는 인증 기관을 System Manager에 추가로 설치할 수 있습니다.

단계

1. 신뢰할 수 있는 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 을 + Add 선택합니다.
3. 신뢰할 수 있는 인증 기관 추가* 패널에서 다음을 수행하십시오.
   - 이름 * 을 입력합니다.
   - 범위 * 에서 스토리지 VM을 선택합니다.
   - 일반 이름 * 을 입력합니다.
   - 유형 * 을 선택합니다.
   - 인증서 세부 정보 * 를 입력하거나 가져옵니다.

## 신뢰할 수 있는 인증 기관을 삭제합니다

System Manager를 사용하면 신뢰할 수 있는 인증 기관을 삭제할 수 있습니다.

ONTAP에 사전 설치된 신뢰할 수 있는 인증 기관은 삭제할 수 없습니다.

단계

1. 신뢰할 수 있는 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 신뢰할 수 있는 인증 기관의 이름을 선택합니다.
3. 이름 옆에 있는 을 ⋮ 선택한 다음 * 삭제 * 를 선택합니다.

## 신뢰할 수 있는 인증 기관을 갱신합니다

System Manager를 사용하면 만료되었거나 곧 만료될 신뢰할 수 있는 인증 기관을 갱신할 수 있습니다.

단계

1. 신뢰할 수 있는 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 신뢰할 수 있는 인증 기관의 이름을 선택합니다.
3. 인증서 이름 옆에 있는 * 갱신 * 을 선택합니다 ⋮ .

## 클라이언트/서버 인증서를 설치(추가)합니다

System Manager를 사용하면 추가 클라이언트/서버 인증서를 설치할 수 있습니다.

단계

1. 클라이언트/서버 인증서 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 을 + Add 선택합니다.
3. 클라이언트/서버 인증서 추가 * 패널에서 다음을 수행하십시오.
   - 인증서 이름 * 을 입력합니다.
   - 범위 * 에서 스토리지 VM을 선택합니다.

- 일반 이름 * 을 입력합니다.
- 유형 * 을 선택합니다.
- 인증서 세부 정보 * 를 입력하거나 가져옵니다. 텍스트 파일에서 인증서 세부 정보를 작성하거나 복사하여 붙여 넣거나 * Import *(가져오기 *)를 클릭하여 인증서 파일에서 텍스트를 가져올 수 있습니다.
- 개인 키 * 를 입력합니다.
  텍스트 파일에서 개인 키를 작성하거나 복사하여 붙여 넣거나 * Import *(가져오기 *)를 클릭하여 개인 키 파일에서 텍스트를 가져올 수 있습니다.

## 자체 서명된 클라이언트/서버 인증서를 생성(추가)합니다

System Manager를 사용하면 자체 서명된 클라이언트/서버 인증서를 추가로 생성할 수 있습니다.

단계

1. 클라이언트/서버 인증서 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 선택 * + 자체 서명 인증서 생성 *.
3. 자체 서명된 인증서 생성 * 패널에서 다음을 수행합니다.
   - 인증서 이름 * 을 입력합니다.
   - 범위 * 에서 스토리지 VM을 선택합니다.
   - 일반 이름 * 을 입력합니다.
   - 유형 * 을 선택합니다.
   - 해시 함수 * 를 선택합니다.
   - 키 크기 * 를 선택합니다.
   - 스토리지 VM * 을 선택합니다.

## 클라이언트/서버 인증서를 삭제합니다

System Manager를 사용하면 클라이언트/서버 인증서를 삭제할 수 있습니다.

단계

1. 클라이언트/서버 인증서 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 클라이언트/서버 인증서의 이름을 선택합니다.
3. 이름 옆에 있는 을 선택한 ⋮ 다음 * 삭제 * 를 클릭합니다.

## 클라이언트/서버 인증서를 갱신합니다

System Manager를 사용하면 만료되었거나 곧 만료될 클라이언트/서버 인증서를 갱신할 수 있습니다.

단계

1. 클라이언트/서버 인증서 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 클라이언트/서버 인증서의 이름을 선택합니다.
3. 이름 옆에 있는 을 ⋮ 선택한 다음 * 갱신 * 을 클릭합니다.

## 새 로컬 인증 기관을 생성합니다

System Manager를 사용하여 새 로컬 인증 기관을 만들 수 있습니다.

단계

1. 로컬 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 을 + Add 선택합니다.
3. [로컬 인증 기관 추가]* 패널에서 다음 작업을 수행하십시오.
   - 이름 * 을 입력합니다.
   - 범위 * 에서 스토리지 VM을 선택합니다.
   - 일반 이름 * 을 입력합니다.
4. 기본값을 무시하려면 * 추가 옵션 * 을 선택하고 추가 정보를 제공합니다.

## 로컬 인증 기관을 사용하여 인증서에 서명합니다

System Manager에서 로컬 인증 기관을 사용하여 인증서에 서명할 수 있습니다.

단계

1. 로컬 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 로컬 인증 기관의 이름을 선택합니다.
3. 이름 옆에 있는 * 인증서 서명 * 을 선택합니다 ⋮ .
4. 인증서 서명 요청 * 양식 을 작성합니다.
   - 인증서 서명 콘텐츠를 붙여 넣거나 * 가져오기 * 를 클릭하여 인증서 서명 요청 파일을 가져올 수 있습니다.
   - 인증서가 유효한 일 수를 지정합니다.

## 로컬 인증 기관을 삭제합니다

System Manager를 사용하면 로컬 인증 기관을 삭제할 수 있습니다.

단계

1. 로컬 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 로컬 인증 기관의 이름을 선택합니다.
3. 이름 옆에 있는 을 ⋮ 선택한 다음 * Delete * 를 선택합니다.

## 로컬 인증 기관을 갱신합니다

System Manager를 사용하면 만료되었거나 곧 만료될 로컬 인증 기관을 갱신할 수 있습니다.

단계

1. 로컬 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 로컬 인증 기관의 이름을 선택합니다.

3. 이름 옆에 있는 을 ⋮ 선택한 다음 * 갱신 * 을 클릭합니다.

# Active Directory 도메인 컨트롤러 액세스 개요 구성

AD 계정이 SVM에 액세스하려면 먼저 클러스터 또는 SVM에 대한 AD 도메인 컨트롤러 액세스를 구성해야 합니다. 데이터 SVM을 위해 SMB 서버를 이미 구성한 경우, SVM을 클러스터에 대한 AD 액세스를 위한 게이트웨이 또는 _tunnel_로 구성할 수 있습니다. SMB 서버를 구성하지 않은 경우 AD 도메인에서 SVM에 대한 컴퓨터 계정을 생성할 수 있습니다.

ONTAP는 다음과 같은 도메인 컨트롤러 인증 서비스를 지원합니다.

- Kerberos
- LDAP를 지원합니다
- Netlogon
- 로컬 보안 기관(LSA)

ONTAP는 보안 Netlogon 연결을 위해 다음 세션 키 알고리즘을 지원합니다.

| 세션 키 알고리즘입니다 | 다음으로 시작… |
|---|---|
| HMAC-SHA256, AES(Advanced Encryption Standard) 기반<br><br>클러스터에서 ONTAP 9.9.1 이하를 실행하고 도메인 컨트롤러가 보안 Netlogon 서비스를 위해 AES를 적용하는 경우 연결이 실패합니다. 이 경우 ONTAP와의 강력한 키 연결을 허용하도록 도메인 컨트롤러를 다시 구성해야 합니다. | ONTAP 9.10.1 |
| Des 및 HMAC-MD5(강력한 키가 설정된 경우) | 모든 ONTAP 9 릴리스 |

Netlogon 보안 채널을 설정하는 동안 AES 세션 키를 사용하려면 SVM에서 AES가 활성화되어 있는지 확인해야 합니다.

- ONTAP 9.14.1부터 AES는 SVM을 생성할 때 기본적으로 사용하도록 설정되며, Netlogon 보안 채널 설정 중에 AES 세션 키를 사용하도록 SVM의 보안 설정을 수정할 필요가 없습니다.
- ONTAP 9.10.1~9.13.1에서는 SVM을 생성할 때 AES가 기본적으로 사용하지 않도록 설정됩니다. 다음 명령을 사용하여 AES를 사용하도록 설정해야 합니다.

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```

ONTAP 9.14.1 이상으로 업그레이드할 때 이전 ONTAP 릴리즈와 함께 생성된 기존 SVM에 대한 AES 설정이 자동으로 변경되지 않습니다. 하지만 이러한 SVM에서 AES를 사용하도록 설정하려면 이 설정의 값을 업데이트해야 합니다.

## 인증 터널을 구성합니다

데이터 SVM을 위해 SMB 서버를 이미 구성한 경우 'security login domain-tunnel create' 명령을 사용하여 SVM을 게이트웨이로 구성하거나, AD에서 클러스터에 액세스하도록 _tunnel_을 사용할 수 있습니다.

시작하기 전에

- 데이터 SVM을 위해 SMB 서버를 구성해야 합니다.
- 클러스터의 admin SVM에 액세스하려면 AD 도메인 사용자 계정을 활성화해야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

ONTAP 9.10.1부터 AD 액세스를 위한 SVM 게이트웨이(도메인 터널)가 있는 경우 AD 도메인에서 NTLM을 비활성화한 경우 관리자 인증에 Kerberos를 사용할 수 있습니다. 이전 릴리즈에서는 SVM 게이트웨이에 대한 관리자 인증을 사용하여 Kerberos를 지원하지 않았습니다. 이 기능은 기본적으로 사용할 수 있으며 구성이 필요하지 않습니다.

> Kerberos 인증은 항상 먼저 시도됩니다. 오류가 발생하면 NTLM 인증이 시도됩니다.

단계

1. 클러스터에 대한 AD 도메인 컨트롤러 액세스를 위한 인증 터널로 SMB 지원 데이터 SVM 구성:

   `security login domain-tunnel create -vserver svm_name`

   전체 명령 구문은 을 참조하십시오 "워크시트".

   > 사용자가 인증을 받으려면 SVM이 실행 중이어야 합니다.

   다음 명령은 SMB 지원 데이터 SVM ""engData""를 인증 터널로 구성합니다.

   ```
   cluster1::>security login domain-tunnel create -vserver engData
   ```

## 도메인에서 **SVM** 컴퓨터 계정을 생성합니다

데이터 SVM용으로 SMB 서버를 구성하지 않은 경우 'vserver active-directory create' 명령을 사용하여 도메인의 SVM에 대한 컴퓨터 계정을 생성할 수 있습니다.

이 작업에 대해

'vserver active-directory create' 명령을 입력하면 도메인의 지정된 조직 단위에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 AD 사용자 계정에 대한 자격 증명을 제공하라는 메시지가 표시됩니다. 계정의 암호는 비워둘 수 없습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. AD 도메인에서 SVM을 위한 컴퓨터 계정을 생성합니다.

   'vserver active-directory create-vserver_SVM_name_-account-name_NetBIOS_account_name_-domain_domain_-ou_조직_unit_'

전체 명령 구문은 을 참조하십시오 "워크시트".

다음 명령을 실행하면 SVM ""engData"" 도메인인 ""example.com`""ADSERVER1""이라는 컴퓨터 계정이 생성됩니다. 명령을 입력한 후 AD 사용자 계정 자격 증명을 입력하라는 메시지가 표시됩니다.

```
cluster1::>vserver active-directory create -vserver engData -account
-name ADSERVER1 -domain example.com

In order to create an Active Directory machine account, you must supply
the name and password of a Windows account with sufficient privileges to
add computers to the "CN=Computers" container within the "example.com"
domain.

Enter the user name: Administrator

Enter the password:
```

# LDAP 또는 NIS 서버 액세스 개요를 구성합니다

LDAP 또는 NIS 계정이 SVM에 액세스하려면 먼저 SVM에 대한 LDAP 또는 NIS 서버 액세스를 구성해야 합니다. 스위치 기능을 사용하면 LDAP 또는 NIS를 대체 이름 서비스 소스로 사용할 수 있습니다.

## LDAP 서버 액세스를 구성합니다

LDAP 계정이 SVM에 액세스하려면 SVM에 대한 LDAP 서버 액세스를 구성해야 합니다. SVM에서 'vserver services name-service ldap client create' 명령을 사용하여 LDAP 클라이언트 구성을 생성할 수 있습니다. 그런 다음 "vserver services name-service ldap create" 명령을 사용하여 LDAP 클라이언트 구성을 SVM과 연결할 수 있습니다.

이 작업에 대해

대부분의 LDAP 서버는 ONTAP에서 제공하는 기본 스키마를 사용할 수 있습니다.

- MS-AD-BIS(대부분의 Windows 2012 이상 AD 서버에 대한 기본 스키마)
- AD-IDMU(Windows 2008, Windows 2016 이상 AD 서버)
- AD-SFU(Windows 2003 및 이전 AD 서버)
- RFC-2307(UNIX LDAP 서버)

그렇지 않으면 기본 스키마를 사용하는 것이 가장 좋습니다. 이 경우 기본 스키마를 복사하고 복사본을 수정하여 고유한 스키마를 만들 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- "NFS 구성"
- "NetApp 기술 보고서 4835: ONTAP에서 LDAP를 구성하는 방법"

시작하기 전에

- 을(를) 설치해야 합니다 "CA 서명 서버 디지털 인증서" SVM에서.

- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. SVM에서 LDAP 클라이언트 구성을 생성합니다.

   `vserver services name-service ldap client create -vserver SVM_name -client -config client_configuration -servers LDAP_server_IPs -schema schema -use -start-tls true|false`

   > 시작 TLS는 데이터 SVM에 대한 액세스에만 지원됩니다. 관리 SVM에 대한 액세스는 지원되지 않습니다.

   전체 명령 구문은 을 참조하십시오 "워크시트".

   다음 명령을 실행하면 SVM ""engData""에 ""corp""라는 LDAP 클라이언트 구성이 생성됩니다. 클라이언트는 IP 주소 172.160.0.100 및 172.16.0.101을 사용하여 LDAP 서버에 익명 바인딩합니다. 클라이언트는 RFC-2307 스키마를 사용하여 LDAP 쿼리를 만듭니다. 클라이언트와 서버 간의 통신은 시작 TLS를 사용하여 암호화됩니다.

   ```
   cluster1::> vserver services name-service ldap client create
   -vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
   -schema RFC-2307 -use-start-tls true
   ```

   > ONTAP 9.2부터 -ldap-servers 필드가 -servers 필드를 대체합니다. 이 새 필드는 LDAP 서버의 호스트 이름 또는 IP 주소를 사용할 수 있습니다.

2. LDAP 클라이언트 구성을 SVM에 연결: `vserver services name-service ldap create -vserver SVM_name -client-config client_configuration -client-enabled true|false`

   전체 명령 구문은 을 참조하십시오 "워크시트".

   다음 명령은 LDAP 클라이언트 구성을 연결합니다 `corp` SVM을 사용합니다 `engData`및 는 SVM에서 LDAP 클라이언트를 활성화합니다.

   ```
   cluster1::>vserver services name-service ldap create -vserver engData
   -client-config corp -client-enabled true
   ```

   > ONTAP 9.2부터 'vserver services name-service ldap create' 명령은 자동 구성 검증을 수행하고 ONTAP가 이름 서버에 연결할 수 없는 경우 오류 메시지를 보고합니다.

3. vserver services name-service ldap check 명령을 사용하여 이름 서버의 상태를 확인합니다.

   다음 명령을 실행하면 SVM vs0에서 LDAP 서버를 검증합니다.

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                    |
| Client Configuration Name: c1                                   |
| LDAP Status: up                                                 |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                  |
```

이름 서비스 확인 명령은 ONTAP 9.2부터 사용할 수 있습니다.

## NIS 서버 액세스를 구성합니다

NIS 계정이 SVM에 액세스하려면 먼저 SVM에 대한 NIS 서버 액세스를 구성해야 합니다. SVM에 NIS 도메인 구성을 생성하려면 'vserver services name-service nis-domain create' 명령을 사용할 수 있습니다.

이 작업에 대해

여러 NIS 도메인을 생성할 수 있습니다. NIS 도메인은 한 번에 하나만 '활성'으로 설정할 수 있습니다.

시작하기 전에

- SVM에서 NIS 도메인을 구성하기 전에 구성된 모든 서버를 사용할 수 있고 액세스할 수 있어야 합니다.
- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. SVM에서 NIS 도메인 구성 생성:

   `vserver services name-service nis-domain create -vserver` *`SVM_name`* `-domain client_configuration -active true|false -nis-servers` *`NIS_server_IPs`*

   전체 명령 구문은 을 참조하십시오 "워크시트".

   > ONTAP 9.2부터, 필드 '-NIS-SERS'는 필드 '-SERVers'를 대체합니다. 이 새 필드는 NIS 서버의 호스트 이름 또는 IP 주소를 사용할 수 있습니다.

   다음 명령을 실행하면 SVM ""engData""에 NIS 도메인 구성이 생성됩니다. NIS 도메인입니다 `nisdomain` 생성 시 활성 상태이며 IP 주소 192.0.2.180을 사용하여 NIS 서버와 통신합니다.

```
cluster1::>vserver services name-service nis-domain create
-vserver engData -domain nisdomain -active true -nis-servers 192.0.2.180
```

## 네임 서비스 스위치를 생성합니다

이름 서비스 스위치 기능을 사용하면 LDAP 또는 NIS를 대체 이름 서비스 소스로 사용할 수 있습니다. 'vserver services name-service ns-switch modify' 명령을 사용하여 이름 서비스 소스의 조회 순서를 지정할 수 있습니다.

시작하기 전에

- LDAP 및 NIS 서버 액세스를 구성해야 합니다.
- 이 작업을 수행하려면 클러스터 관리자 또는 SVM 관리자여야 합니다.

단계

1. 이름 서비스 원본에 대한 조회 순서를 지정합니다.

   `vserver services name-service ns-switch modify -vserver` *`SVM_name`* `-database` *`name_service_switch_database`* `-sources` *`name_service_source_order`*

   전체 명령 구문은 을 참조하십시오 "워크시트".

   다음 명령은 SVM ""engData""의 ""passwd"" 데이터베이스에 대한 LDAP 및 NIS 이름 서비스 소스의 조회 순서를 지정합니다.

   ```
   cluster1::>vserver services name-service ns-switch
   modify -vserver engData -database passwd -source files ldap,nis
   ```

# 관리자 암호를 변경합니다

처음 시스템에 로그인한 후 즉시 초기 암호를 변경해야 합니다. SVM 관리자는 '보안 로그인 비밀번호' 명령을 사용하여 비밀번호를 변경할 수 있습니다. 클러스터 관리자인 경우 '보안 로그인 암호' 명령을 사용하여 관리자 암호를 변경할 수 있습니다.

이 작업에 대해

새 암호는 다음 규칙을 준수해야 합니다.

- 사용자 이름은 포함할 수 없습니다
- 8자 이상이어야 합니다
- 하나 이상의 문자와 숫자를 포함해야 합니다
- 마지막 여섯 개의 암호와 같을 수 없습니다

> 를 사용할 수 있습니다 `security login role config modify` 지정된 역할과 연결된 계정의 암호 규칙을 수정하는 명령입니다. 자세한 내용은 를 참조하십시오 "명령 참조".

시작하기 전에

- 암호를 변경하려면 클러스터 또는 SVM 관리자여야 합니다.
- 다른 관리자의 암호를 변경하려면 클러스터 관리자여야 합니다.

단계

1. 관리자 암호 변경: `security login password -vserver` *`svm_name`* `-username` *`user_name`*

   다음 명령을 실행하면 SVM에 대한 관리자 admin의 암호( vs1.example.com`` )가 변경됩니다. 현재 암호를 입력하라는 메시지가 표시되면 새 암호를 입력하고 다시 입력합니다.

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

# 관리자 계정 잠금 및 잠금 해제

## 'Security login lock' 명령어를 이용하여 관리자 계정을 잠그고, 'Security login unlock' 명령어를 이용하여 계정 잠금을 해제할 수 있다.

시작하기 전에

이러한 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 관리자 계정 잠금:

   'Security login lock - vserver SVM_name - username user_name

   다음 명령을 실행하면 SVM에 대한 관리자 계정 admin1이 잠깁니다. vs1.example.com``:

   ```
   cluster1::>security login lock -vserver engData -username admin1
   ```

2. 관리자 계정 잠금 해제:

   'Security login unlock - vserver SVM_name - username user_name'

   다음 명령을 실행하면 SVM에 대한 관리자 계정 admin1의 잠금이 해제됩니다. vs1.example.com``:

   ```
   cluster1::>security login unlock -vserver engData -username admin1
   ```

# 실패한 로그인 시도를 관리합니다

## 로그인 시도가 반복적으로 실패하면 침입자가 스토리지 시스템을 액세스하려고 시도하는 것을 나타내는 경우가 있습니다. 침입이 발생하지 않도록 여러 단계를 수행할 수 있습니다.

### 로그인 시도가 실패했음을 어떻게 알 수 있습니다

이벤트 관리 시스템(EMS)은 매 시간마다 로그인 실패 사실을 알립니다. 'audit.log' 파일에서 실패한 로그인 시도 기록을 찾을 수 있습니다.

### 반복 로그인 시도가 실패하면 어떻게 해야 합니까

단기적으로는 침입 방지를 위한 여러 단계를 수행할 수 있습니다.

- 암호는 최소 대문자, 소문자, 특수 문자 및/또는 숫자로 구성되어야 합니다
- 로그인 시도 실패 후 지연을 적용합니다
- 허용되는 로그인 시도 실패 횟수를 제한하고 지정된 시도 실패 횟수 이후에 사용자를 잠급니다
- 지정된 일 수 동안 비활성 상태인 계정을 만료 및 잠급니다

'Security login role config modify' 명령어를 사용해 이 작업을 수행할 수 있다.

장기적으로 다음과 같은 추가 단계를 수행할 수 있습니다.

- 새로 생성된 모든 SVM에 대해 로그인 시도 실패 횟수를 제한하려면 'security ssh modify' 명령을 사용합니다.
- 사용자에게 암호를 변경하도록 요구하여 기존 MD5 알고리즘 계정을 보다 안전한 SHA-512 알고리즘으로 마이그레이션합니다.

# 관리자 계정 암호에 **SHA-2**를 적용합니다

## ONTAP 9.0 이전에 만든 관리자 계정은 암호를 수동으로 변경할 때까지 업그레이드 후 MD5 암호를 계속 사용합니다. MD5는 SHA-2보다 안전하지 않습니다. 따라서 업그레이드 후 MD5 계정 사용자에게 암호를 변경하여 기본 SHA-512 해시 기능을 사용하도록 해야 합니다.

이 작업에 대해

암호 해시 기능을 사용하면 다음을 수행할 수 있습니다.

- 지정된 해시 함수와 일치하는 사용자 계정을 표시합니다.
- 지정된 해시 기능(예: MD5)을 사용하는 계정을 만료하여 사용자가 다음 로그인 시 암호를 변경하도록 합니다.
- 암호가 지정된 해시 기능을 사용하는 계정을 잠급니다.
- ONTAP 9 이전 릴리즈로 되돌릴 때 이전 릴리즈에서 지원하는 MD5(해시 기능)와 호환되도록 클러스터 관리자의 자체 암호를 재설정합니다.

ONTAP는 NetApp Manageability SDK를 사용하여 해시된 SHA-2 암호만 허용합니다 (`security-login-create` 및 `security-login-modify-password`)를 클릭합니다.

단계

1. MD5 관리자 계정을 SHA-512 암호 해시 기능으로 마이그레이션합니다.
   a. MD5 관리자 계정 모두 만료: '보안 로그인 만료 - 암호 - vserver* - 사용자 이름* - 해시 - 기능 MD5'

      이렇게 하면 MD5 계정 사용자는 다음 로그인 시 암호를 변경해야 합니다.

   b. MD5 계정 사용자에게 콘솔 또는 SSH 세션을 통해 로그인하도록 요청합니다.

      계정이 만료되었음을 감지하고 사용자에게 암호를 변경하라는 메시지를 표시합니다. SHA-512는 변경된 암호에 기본적으로 사용됩니다.

2. 사용자가 로그인하지 않은 MD5 계정의 경우 일정 시간 내에 암호를 변경하려면 다음과 같이 계정 마이그레이션을 강제로 수행합니다.

   a. MD5 해시 기능(고급 권한 수준)을 계속 사용하는 계정 잠금: '보안 로그인 만료 - 암호 - vserver* - 사용자 이름 * - 해시 - 기능 md5 - 정수 후 잠금

      록애프터(lock-After)로 지정된 일 수가 지나면 MD5 계정에 액세스할 수 없습니다.

   b. 사용자가 암호를 변경할 준비가 되면 계정의 잠금을 해제합니다. `security login unlock -vserver svm_name -username user_name`

   c. 사용자가 콘솔 또는 SSH 세션을 통해 계정에 로그인하고 시스템에서 암호를 변경하도록 요청하는 경우 암호를 변경하도록 요청합니다.

# 파일 액세스 문제를 진단하고 해결합니다

단계

1. System Manager에서 * 스토리지 > 스토리지 VM * 을 선택합니다.
2. 추적을 수행할 스토리지 VM을 선택합니다.
3. ⋮More * 를 클릭합니다.
4. 추적 파일 액세스 * 를 클릭합니다.
5. 사용자 이름과 클라이언트 IP 주소를 입력한 다음 * 추적 시작 * 을 클릭합니다.

   추적 결과가 테이블에 표시됩니다. 이유 * 열은 파일에 액세스할 수 없는 이유를 제공합니다.

6. ⌄파일 액세스 권한을 보려면 결과 테이블의 왼쪽 열을 클릭합니다.