



로그인 계정을 만듭니다

ONTAP 9

NetApp
April 24, 2024

목차

로그인 계정을 만듭니다	1
로그인 계정 생성 개요	1
로컬 계정 액세스를 설정합니다	2
Active Directory 계정 액세스를 설정합니다	11
LDAP 또는 NIS 계정 액세스를 설정합니다	13

로그인 계정을 만듭니다

로그인 계정 생성 개요

로컬 또는 원격 클러스터 및 SVM 관리자 계정을 활성화할 수 있습니다. 로컬 계정은 계정 정보, 공개 키 또는 보안 인증서가 스토리지 시스템에 상주하는 계정입니다. AD 계정 정보는 도메인 컨트롤러에 저장됩니다. LDAP 및 NIS 계정은 LDAP 및 NIS 서버에 상주합니다.

클러스터 및 **SVM** 관리자

클러스터 관리자는 _ 클러스터에 대한 admin SVM에 액세스합니다. 클러스터 설정 시 admin이라는 예약 이름의 클러스터 관리자와 SVM 관리자가 자동으로 생성됩니다.

기본 'admin' 역할을 가진 클러스터 관리자는 전체 클러스터와 리소스를 관리할 수 있습니다. 클러스터 관리자는 필요에 따라 서로 다른 역할을 가진 추가 클러스터 관리자를 생성할 수 있습니다.

SVM 관리자는 _ 데이터 SVM에 액세스합니다. 클러스터 관리자가 필요에 따라 데이터 SVM 및 SVM 관리자를 생성합니다.

SVM 관리자는 기본적으로 'vsadmin' 역할이 할당됩니다. 클러스터 관리자는 필요에 따라 SVM 관리자에게 다양한 역할을 할당할 수 있습니다.

명명 규칙

다음 일반 이름은 원격 클러스터 및 SVM 관리자 계정에 사용할 수 없습니다.

- "아담"
- "출력함"
- "CLI"
- "데몬"
- "FTP"
- "게임"
- "중지"
- "lp"
- "메일"
- "남자"
- "나루트"
- "NetApp"
- "뉴스"
- "없음"
- "연산자"
- "루트"

- "종료"
- "sshd"
- "동기화"
- "시스템"
- "우프"
- "www"

병합된 역할

동일한 사용자에게 여러 원격 계정을 사용하도록 설정하면 계정에 지정된 모든 역할의 조합이 사용자에게 할당됩니다. 즉, LDAP 또는 NIS 계정에 vsadmin 역할이 할당되고 같은 사용자의 AD 그룹 계정에 vsadmin-volume 역할이 할당되면 AD 사용자는 보다 포괄적인 vsadmin 기능으로 로그인합니다. 역할은 _ 병합 _ 이라고 합니다.

로컬 계정 액세스를 설정합니다

로컬 계정 액세스 개요를 활성화합니다

로컬 계정은 계정 정보, 공개 키 또는 보안 인증서가 스토리지 시스템에 상주하는 계정입니다. 'Security login create' 명령을 사용하여 로컬 계정에서 admin 또는 data SVM에 액세스할 수 있습니다.

암호 계정 액세스를 활성화합니다

'Security login create' 명령을 사용하면 관리자 계정에서 admin 또는 data SVM에 암호를 사용하여 액세스할 수 있습니다. 명령을 입력하면 암호를 묻는 메시지가 표시됩니다.

이 작업에 대해

로그인 계정에 할당할 액세스 제어 역할을 잘 모르는 경우 '보안 로그인 수정' 명령을 사용하여 나중에 역할을 추가할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 로컬 관리자 계정에서 암호를 사용하여 SVM에 액세스:

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role role -comment
comment
```

전체 명령 구문은 을 참조하십시오 ["워크시트"](#).

다음 명령을 사용하면 미리 정의된 백업 역할을 가진 클러스터 관리자 계정 admin1이 암호를 사용하여 SVM "engCluster"에 액세스할 수 있습니다. 명령을 입력하면 암호를 묻는 메시지가 표시됩니다.

```
cluster1::>security login create -vserver engCluster -user-or-group-name
admin1 -application ssh -authmethod password -role backup
```

SSH 공개 키 계정을 활성화합니다

'Security login create' 명령을 사용하면 관리자 계정이 SSH 공개 키로 admin 또는 data SVM에 액세스할 수 있습니다.

이 작업에 대해

- 계정이 SVM에 액세스하려면 먼저 공개 키를 계정에 연결해야 합니다.

공개 키를 사용자 계정과 연결

계정 액세스를 활성화하기 전이나 후에 이 작업을 수행할 수 있습니다.

- 로그인 계정에 할당할 액세스 제어 역할을 잘 모르는 경우 '보안 로그인 수정' 명령을 사용하여 나중에 역할을 추가할 수 있습니다.

클러스터에서 FIPS 모드를 활성화하려면 지원되는 키 알고리즘이 없는 기존 SSH 공개 키 계정을 지원되는 키 유형으로 재구성해야 합니다. FIPS를 사용하도록 설정하기 전에 계정을 다시 구성해야 하며 그렇지 않으면 관리자 인증이 실패합니다.

다음 표에는 ONTAP SSH 연결에 지원되는 호스트 키 유형 알고리즘이 나와 있습니다. 이러한 키 유형은 SSH 공개 인증 구성에 적용되지 않습니다.

ONTAP 릴리즈	FIPS 모드에서 지원되는 키 유형입니다	FIPS 이외의 모드에서 지원되는 키 유형입니다
9.11.1 이상	ECDSA-SHA2-nistp256	ECDSA-SHA2-nistp256+RSA-SHA2-512+RSA-SHA2-256+ssh-ed25519+ssh-dss+ssh-ssh-rsa
9.10.1 이하	ECDSA-SHA2-nistp256+ssh-ed25519	ECDSA-SHA2-nistp256+ssh-ed25519+ssh-dss+ssh-rsa



ONTAP 9.11.1부터 ssh-ed25519 호스트 키 알고리즘에 대한 지원이 제거되었습니다.

자세한 내용은 을 참조하십시오 ["FIPS를 사용하여 네트워크 보안을 구성합니다"](#).

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 로컬 관리자 계정이 SSH 공개 키를 사용하여 SVM에 액세스할 수 있도록 합니다.

'보안 로그인 생성 - vserver_SVM_name_-user-or-group-name user_or_group_name-application_application_-AuthMethod_authentication_method_-role_role_-comment_comment_'

전체 명령 구문은 을 참조하십시오 ["워크시트"](#).

다음 명령을 실행하면 SSH 공개 키를 사용하여 SVM "engData1"에 액세스할 수 있도록 사전 정의된 "vsadmin-volume" 역할이 있는 SVM 관리자 계정의 vmadmin1이 활성화됩니다.

```
cluster1::>security login create -vserver engData1 -user-or-group-name  
svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
```

작업을 마친 후

공개 키를 관리자 계정에 연결하지 않은 경우, 계정이 SVM에 액세스하려면 먼저 연결해야 합니다.

공개 키를 사용자 계정과 연결

다단계 인증(MFA) 계정 활성화

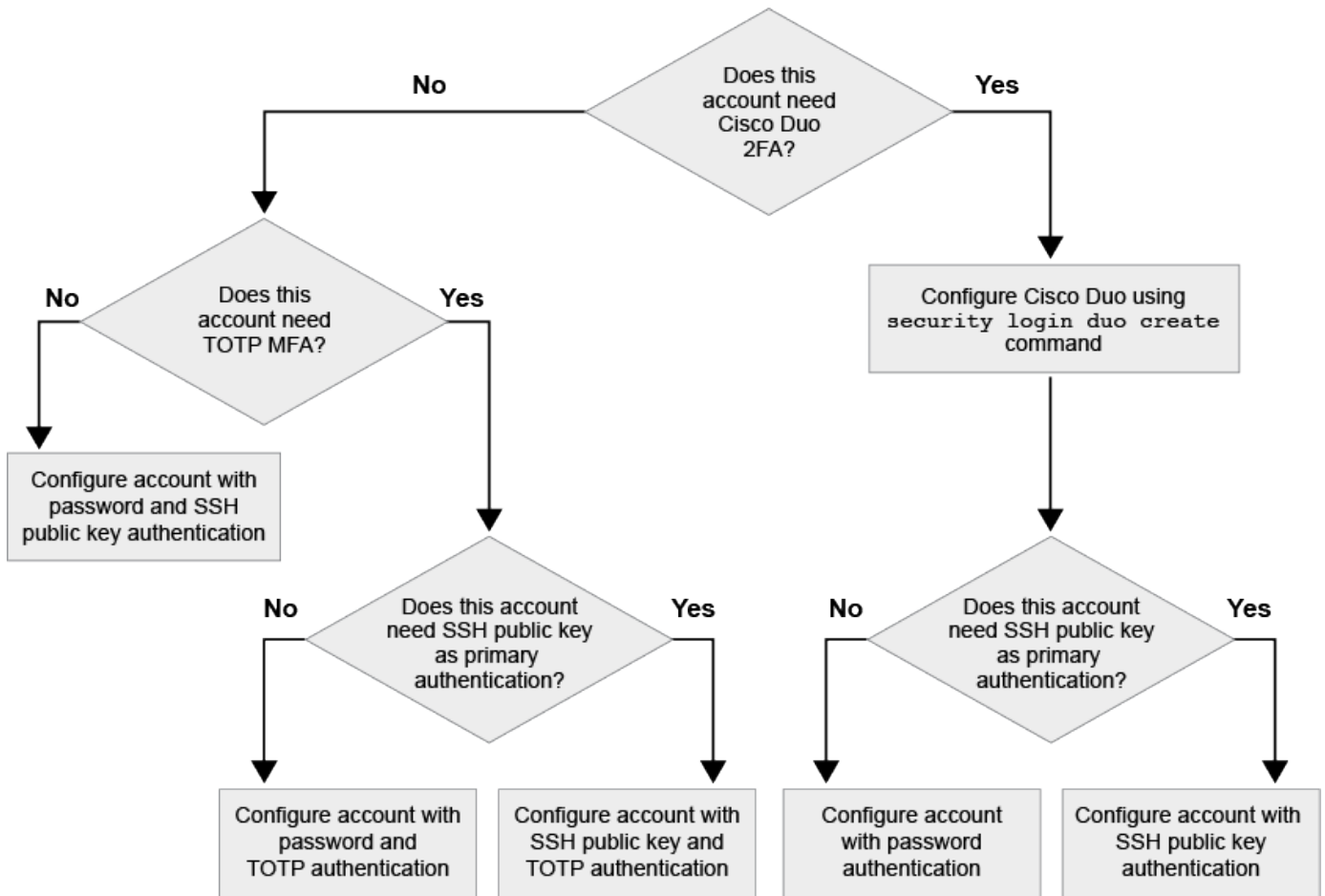
다단계 인증 개요

다단계 인증(MFA)을 사용하면 사용자에게 관리자 또는 데이터 스토리지 VM에 로그인하기 위한 두 가지 인증 방법을 제공하도록 요구하여 보안을 강화할 수 있습니다.

ONTAP 버전에 따라 다단계 인증을 위해 SSH 공개 키, 사용자 암호 및 시간 기반 TOTP(일회성 암호)를 함께 사용할 수 있습니다. Cisco Duo(ONTAP 9.14.1 이상)를 활성화 및 구성하면 모든 사용자에게 대한 기존 방법을 보완하는 추가 인증 방법으로 사용됩니다.

다음으로 시작...	첫 번째 인증 방법입니다	두 번째 인증 방법입니다
ONTAP 9.14.1	SSH 공개 키	토평
	사용자 암호	토평
	SSH 공개 키	Cisco 듀오
	사용자 암호입니다	Cisco 듀오
ONTAP 9.13.1	SSH 공개 키	토평
	사용자 암호입니다	토평
ONTAP 9.3	SSH 공개 키	사용자 암호입니다

MFA가 구성된 경우 클러스터 관리자가 먼저 로컬 사용자 계정을 사용하도록 설정한 다음 로컬 사용자가 계정을 구성해야 합니다.



다단계 인증 을 활성화합니다

다단계 인증(MFA)을 사용하면 사용자가 admin 또는 data SVM에 로그인하기 위한 두 가지 인증 방법을 제공하도록 요구하여 보안을 강화할 수 있습니다.

이 작업에 대해

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 로그인 계정에 할당할 액세스 제어 역할을 잘 모르는 경우 '보안 로그인 수정' 명령을 사용하여 나중에 역할을 추가할 수 있습니다.

"관리자에게 할당된 역할 수정"

- 인증을 위해 공개 키를 사용하는 경우, 계정이 SVM에 액세스하려면 먼저 공개 키를 계정에 연결해야 합니다.

"공개 키를 사용자 계정에 연결합니다"

계정 액세스를 활성화하기 전이나 후에 이 작업을 수행할 수 있습니다.

- ONTAP 9.12.1부터 FIDO2(Fast Identity Online) 또는 PIV(Personal Identity Verification) 인증 표준을 사용하여 SSH 클라이언트 MFA에 Yubikey 하드웨어 인증 장치를 사용할 수 있습니다.

SSH 공개 키 및 사용자 암호로 **MFA**를 사용하도록 설정합니다

ONTAP 9.3부터 클러스터 관리자는 SSH 공개 키 및 사용자 암호를 사용하여 MFA로 로그인하도록 로컬 사용자 계정을

설정할 수 있습니다.

1. SSH 공개 키 및 사용자 암호를 사용하여 로컬 사용자 계정에서 MFA를 사용하도록 설정합니다.

```
security login create -vserver <svm_name> -user-or-group-name  
<user_name> -application ssh -authentication-method <password|publickey>  
-role admin -second-authentication-method <password|publickey>
```

다음 명령을 수행하려면 미리 정의된 "admin" 역할을 가진 SVM 관리자 계정 "admin2"가 SSH 공개 키와 사용자 암호를 사용하여 SVM "engData1"에 로그인해야 합니다.

```
cluster-1::> security login create -vserver engData1 -user-or-group-name  
admin2 -application ssh -authentication-method publickey -role admin  
-second-authentication-method password  
  
Please enter a password for user 'admin2':  
Please enter it again:  
Warning: To use public-key authentication, you must create a public key  
for user "admin2".
```

TOTP로 MFA를 활성화합니다

ONTAP 9.13.1 부터는 로컬 사용자가 SSH 공개 키 또는 사용자 암호와 TOTP(Time-Based One-Time Password)를 사용하여 admin 또는 data SVM에 로그인하도록 하여 보안을 강화할 수 있습니다. TOTP로 MFA에 대해 계정을 활성화한 후 로컬 사용자는 에 로그인해야 합니다 ["구성을 완료합니다"](#).

TOTP는 현재 시간을 사용하여 1회 암호를 생성하는 컴퓨터 알고리즘입니다. TOTP를 사용하는 경우 SSH 공개 키 또는 사용자 암호 뒤에 항상 두 번째 인증 형태입니다.

시작하기 전에

이러한 작업을 수행하려면 스토리지 관리자여야 합니다.

단계

사용자 암호 또는 SSH 공개 키를 사용하여 MFA를 에 설정하고 TOTP를 두 번째 인증 방법으로 설정할 수 있습니다.

사용자 암호 및 **TOTP**로 **MFA**를 활성화합니다

1. 사용자 암호 및 TOTP를 사용하여 다단계 인증을 위한 사용자 계정을 활성화합니다.

◦ 신규 사용자 계정의 경우 *

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

◦ 기존 사용자 계정의 경우 *

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

2. TOTP로 MFA가 활성화되었는지 확인합니다.

```
security login show
```

SSH 공개 키 및 **TOTP**로 **MFA**를 활성화합니다

1. SSH 공개 키 및 TOTP를 사용하여 다단계 인증을 위한 사용자 계정을 활성화합니다.

◦ 신규 사용자 계정의 경우 *

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role>  
-comment <comment>
```

◦ 기존 사용자 계정의 경우 *

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

2. TOTP로 MFA가 활성화되었는지 확인합니다.

```
security login show
```

작업을 마친 후

- 공개 키를 관리자 계정에 연결하지 않은 경우, 계정이 SVM에 액세스하려면 먼저 연결해야 합니다.

"공개 키를 사용자 계정과 연결"

- TOTP로 MFA 구성을 완료하려면 로컬 사용자가 로그인해야 합니다.

"TOTP로 MFA에 대한 로컬 사용자 계정을 구성합니다"

관련 정보

에 대해 자세히 알아보십시오 ["ONTAP 9의 다단계 인증\(TR-4647\)"](#).

TOTP로 MFA에 대한 로컬 사용자 계정을 구성합니다

ONTAP 9.13.1 부터는 TOTP(Time-Based One-Time Password)를 사용하여 MFA(Multifactor Authentication)로 사용자 계정을 구성할 수 있습니다.

시작하기 전에

- 스토리지 관리자는 을(를) 사용해야 합니다 ["TOTP로 MFA를 활성화합니다"](#) 사용자 계정에 대한 두 번째 인증 방법입니다.
- 기본 사용자 계정 인증 방법은 사용자 암호 또는 공용 SSH 키여야 합니다.
- TOTP 앱이 스마트폰과 연동되도록 구성하고 TOTP 비밀 키를 만들어야 합니다.

TOTP는 Google Authenticator와 같은 다양한 인증 앱에서 지원됩니다.

단계

1. 현재 인증 방법으로 사용자 계정에 로그인합니다.

현재 인증 방법은 사용자 암호 또는 SSH 공개 키여야 합니다.

2. 계정에 TOTP 구성을 생성합니다.

```
security login totp create -vserver "<svm_name>" -username  
"<account_username >"
```

3. TOTP 구성이 계정에서 활성화되어 있는지 확인합니다.

```
security login totp show -vserver "<svm_name>" -username  
"<account_username>"
```

TOTP 비밀 키를 재설정합니다

계정 보안을 보호하려면 TOTP 비밀 키가 손상되었거나 손실된 경우 이를 비활성화하고 새 키를 만들어야 합니다.

키가 손상된 경우 **TOTP**를 재설정합니다

TOTP 비밀 키가 손상되었지만 여전히 액세스할 수 있는 경우 손상된 키를 제거하고 새 키를 만들 수 있습니다.

1. 사용자 암호 또는 SSH 공개 키 및 손상된 TOTP 비밀 키를 사용하여 사용자 계정에 로그인합니다.
2. 손상된 TOTP 암호 키를 제거합니다.

```
security login totp delete -vserver <svm_name> -username  
<account_username>
```

3. 새 TOTP 암호 키 생성:

```
security login totp create -vserver <svm_name> -username  
<account_username>
```

4. TOTP 구성이 계정에서 활성화되어 있는지 확인합니다.

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

키를 분실한 경우 **TOTP**를 재설정합니다

TOTP 암호 키가 분실된 경우 스토리지 관리자에게 문의하십시오 "**키를 사용하지 않도록 설정합니다**". 키를 비활성화한 후 첫 번째 인증 방법을 사용하여 새 TOTP에 로그인하고 구성할 수 있습니다.

시작하기 전에

TOTP 암호 키는 스토리지 관리자가 해제해야 합니다. 저장소 관리자 계정이 없는 경우 저장소 관리자에게 문의하여 키를 사용하지 않도록 설정합니다.

단계

1. 스토리지 관리자가 TOTP 암호를 비활성화한 후 기본 인증 방법을 사용하여 로컬 계정에 로그인합니다.
2. 새 TOTP 암호 키 생성:

```
security login totp create -vserver <svm_name> -username  
<account_username >
```

3. TOTP 구성이 계정에서 활성화되어 있는지 확인합니다.

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

로컬 계정에 대해 **TOTP** 암호 키를 비활성화합니다

로컬 사용자의 TOTP(Time-based One-Time Password) 비밀 키를 분실한 경우 저장소 관리자가 손실된 키를 비활성화해야 새 TOTP 비밀 키를 생성할 수 있습니다.

이 작업에 대해

이 작업은 클러스터 관리자 계정에서만 수행할 수 있습니다.

단계

1. TOTP 암호 키 비활성화:

```
security login totp delete -vserver "<svm_name>" -username  
"<account_username>"
```

SSL 인증서 계정을 활성화합니다

'보안 로그인 생성' 명령을 사용하면 관리자 계정이 SSL 인증서를 통해 관리자 또는 데이터 SVM에 액세스할 수 있습니다.

이 작업에 대해

- 계정이 SVM에 액세스하려면 CA 서명 서버 디지털 인증서를 설치해야 합니다.

CA 서명 서버 인증서 생성 및 설치

계정 액세스를 활성화하기 전이나 후에 이 작업을 수행할 수 있습니다.

- 로그인 계정에 할당할 액세스 제어 역할을 잘 모르는 경우 나중에 '보안 로그인 수정' 명령을 사용하여 역할을 추가할 수 있습니다.

관리자에게 할당된 역할 수정



클러스터 관리자 계정의 경우 에서 인증서 인증이 지원됩니다 http, ontapi, 및 rest 응용 프로그램. SVM 관리자 계정의 경우 인증서 인증은 을 통해서만 지원됩니다 ontapi 및 rest 응용 프로그램.

단계

1. 로컬 관리자 계정이 SSL 인증서를 사용하여 SVM에 액세스할 수 있도록 지원:

```
'보안 로그인 생성 - vserver SVM_name -user -or -group -name user_or_group_name -application  
application application -AuthMethod authentication_method -role role role-comment'
```

전체 명령 구문은 을 참조하십시오 ["ONTAP man 페이지를 릴리스별로 표시합니다"](#).

다음 명령을 실행하면 SSL 디지털 인증서를 사용하여 SVM "engData2"에 액세스할 수 있는 기본 "vsadmin" 역할을 가진 SVM 관리자 계정 'vmadmin2'가 활성화됩니다.

```
cluster1::>security login create -vserver engData2 -user-or-group-name  
svmadmin2 -application ontapi -authmethod cert
```

작업을 마친 후

CA 서명 서버 디지털 인증서를 설치하지 않은 경우 계정이 SVM에 액세스하려면 먼저 인증서를 설치해야 합니다.

CA 서명 서버 인증서 생성 및 설치

Active Directory 계정 액세스를 설정합니다

'보안 로그인 생성' 명령을 사용하여 AD(Active Directory) 사용자 또는 그룹 계정을 활성화하여 admin 또는 data SVM에 액세스할 수 있습니다. AD 그룹의 모든 사용자는 그룹에 할당된 역할을 통해 SVM에 액세스할 수 있습니다.

이 작업에 대해

- 계정이 SVM에 액세스하려면 먼저 클러스터 또는 SVM에 대한 AD 도메인 컨트롤러 액세스를 구성해야 합니다.

Active Directory 도메인 컨트롤러 액세스 구성

계정 액세스를 활성화하기 전이나 후에 이 작업을 수행할 수 있습니다.

- ONTAP 9.13.1 부터는 SSH 공개 키를 AD 사용자 암호와 함께 기본 또는 보조 인증 방법으로 사용할 수 있습니다.

SSH 공개 키를 기본 인증으로 사용하도록 선택하면 AD 인증이 수행되지 않습니다.

- ONTAP 9.11.1부터 를 사용할 수 있습니다 "nsswitch 인증을 위한 LDAP 빠른 바인딩" AD LDAP 서버에서 지원하는 경우
- 로그인 계정에 할당할 액세스 제어 역할을 잘 모르는 경우 '보안 로그인 수정' 명령을 사용하여 나중에 역할을 추가할 수 있습니다.

관리자에게 할당된 역할 수정



AD 그룹 계정 액세스는 에서만 지원됩니다 SSH, ontapi, 및 rest 응용 프로그램. 다단계 인증에는 일반적으로 사용되는 SSH 공개 키 인증에서는 AD 그룹이 지원되지 않습니다.

시작하기 전에

- 클러스터 시간은 AD 도메인 컨트롤러에서 5분 이내에 동기화되어야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. AD 사용자 또는 그룹 관리자 계정을 사용하여 SVM에 액세스:

◦ AD 사용자용: *

ONTAP 버전	기본 인증	보조 인증	명령
9.13.1 이상	공개 키	없음	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role></pre>
9.13.1 이상	도메인	공개 키	<p>• 신규 사용자용 *</p> <pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre> <p>• 기존 사용자의 경우 *</p> <pre>security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre>
9.0 이상	도메인	없음	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]</pre>

AD 그룹의 경우 *

ONTAP 버전입니다	기본 인증	보조 인증	명령
9.0 이상	도메인	없음	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap- fastbind true]</pre>

+ 전체 명령 구문은 을 참조하십시오 ["관리자 인증 및 RBAC 구성을 위한 워크시트"](#)

작업을 마친 후

AD 도메인 컨트롤러를 클러스터 또는 SVM에 액세스하도록 구성하지 않은 경우 계정이 SVM에 액세스하려면 먼저 액세스 권한을 구성해야 합니다.

[Active Directory 도메인 컨트롤러 액세스 구성](#)

LDAP 또는 NIS 계정 액세스를 설정합니다

'Security login create' 명령을 사용하여 LDAP 또는 NIS 사용자 계정이 admin 또는 data SVM에 액세스할 수 있도록 설정할 수 있습니다. SVM에 대한 LDAP 또는 NIS 서버 액세스를 구성하지 않은 경우, 계정이 SVM에 액세스하려면 먼저 액세스 권한을 구성해야 합니다.

이 작업에 대해

- 그룹 계정은 지원되지 않습니다.
- 계정이 SVM에 액세스하려면 먼저 SVM에 대한 LDAP 또는 NIS 서버 액세스를 구성해야 합니다.

[LDAP 또는 NIS 서버 액세스를 구성합니다](#)

계정 액세스를 활성화하기 전이나 후에 이 작업을 수행할 수 있습니다.

- 로그인 계정에 할당할 액세스 제어 역할을 잘 모르는 경우 '보안 로그인 수정' 명령을 사용하여 나중에 역할을 추가할 수 있습니다.

[관리자에게 할당된 역할 수정](#)

- ONTAP 9.4부터 LDAP 또는 NIS 서버를 통한 원격 사용자에게 대해 MFA(Multifactor Authentication)가 지원됩니다.
- ONTAP 9.11.1부터 를 사용할 수 있습니다 ["nsswitch 인증을 위한 LDAP 빠른 바인딩"](#) LDAP 서버에서 지원하는 경우
- 알려진 LDAP 문제로 인해 LDAP 사용자 계정 정보 필드(예: "gecos", "userPassword" 등)에 ":"(콜론) 문자를 사용해서는 안 됩니다. 그렇지 않으면 해당 사용자에게 대한 조회 작업이 실패합니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. LDAP 또는 NIS 사용자 또는 그룹 계정을 사용하여 SVM에 액세스:

'보안 로그인 생성 -vserver SVM_name -user -or -group -name user_name -application application -AuthMethod nsswitch -role role -comment comment comment -is -ns -switch -group yes | no [-is -ldap -fastbind true]'를 참조하십시오

전체 명령 구문은 을 참조하십시오 ["워크시트"](#).

["로그인 계정 생성 또는 수정"](#)

다음 명령을 실행하면 미리 정의된 백업 역할을 사용하여 LDAP 또는 NIS 클러스터 관리자 계정 guest2가 SVM "engCluster"에 액세스할 수 있습니다.

```
cluster1::>security login create -vserver engCluster -user-or-group-name  
guest2 -application ssh -authmethod nsswitch -role backup
```

2. LDAP 또는 NIS 사용자에게 대해 MFA 로그인 활성화:

"Security login modify -user -or -group -name rem_usr1 -application ssh-authentication -method nsswitch -role admin -is -ns -switch-group no-second-authentication-method publickey'

인증 방법은 홍보 키로, 두 번째 인증 방식은 nsswitch로 지정할 수 있습니다.

다음 예에서는 MFA 인증이 활성화되어 있는 것을 보여 줍니다.

```
cluster-1::*> security login modify -user-or-group-name rem_usr2  
-application ssh -authentication-method nsswitch -vserver  
cluster-1 -second-authentication-method publickey"
```

작업을 마친 후

SVM에 대한 LDAP 또는 NIS 서버 액세스를 구성하지 않은 경우, 계정이 SVM에 액세스하려면 먼저 액세스 권한을 구성해야 합니다.

[LDAP 또는 NIS 서버 액세스를 구성합니다](#)

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.