액세스 제어 역할을 관리합니다
ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/ontap/authentication/manage-access-control-roles-concept.html on February 12, 2026. Always check docs.netapp.com for the latest.

목차

액세스 제어 역할을 관리합니다

ONTAP 액세스 제어 역할 관리에 대해 알아봅니다

관리자에게 할당된 역할에 따라 관리자가 액세스할 수 있는 명령이 결정됩니다. 관리자 계정을 만들 때 역할을 할당합니다. 필요에 따라 다른 역할을 할당하거나 사용자 지정 역할을 정의할 수 있습니다.

ONTAP 관리자에게 할당된 역할을 수정합니다

명령을 사용하여 클러스터 또는 SVM 관리자 계정의 역할을 변경할 수 있습니다 `security login modify`. 미리 정의된 역할 또는 사용자 지정 역할을 할당할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 클러스터 또는 SVM 관리자의 역할 변경:

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

   "로그인 계정 생성 또는 수정"

   다음 명령을 실행하면 AD 클러스터 관리자 계정 DOMAIN1\guest1 의 역할이 미리 정의된 "재만" 역할로 변경됩니다.

   ```
   cluster1::>security login modify -vserver engCluster -user-or-group-name
   DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
   ```

   다음 명령을 실행하면 AD 그룹 계정 DOMAIN1\adgroup의 SVM 관리자 계정 역할이 사용자 지정 "vol_role" 역할로 변경됩니다.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
   ```

   에 대한 자세한 내용은 `security login modify` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 관리자를 위한 사용자 지정 역할 정의

명령을 사용하여 사용자 지정 역할을 정의할 수 `security login role create` 있습니다. 역할에 연결할 기능을 정확하게 조합하기 위해 필요한 만큼 명령을 실행할 수 있습니다.

이 작업에 대해

- 사전 정의되거나 사용자 지정되거나 관계 없이 역할은 ONTAP 명령 또는 명령 디렉터리에 대한 액세스를 허용하거나 거부합니다.

  명령 디렉토리(예: 볼륨)는 관련 명령 및 명령 하위 디렉토리 그룹입니다. 이 절차에서 설명한 경우를 제외하고 명령 디렉터리에 대한 액세스 권한을 부여하거나 거부하면 디렉터리 및 해당 하위 디렉터리의 각 명령에 대한 액세스 권한이 부여되거나 거부됩니다.

- 특정 명령 액세스 또는 하위 디렉토리 액세스는 상위 디렉토리 액세스보다 우선합니다.

  역할이 명령 디렉토리로 정의된 후 특정 명령이나 상위 디렉토리의 하위 디렉토리에 대해 다른 액세스 수준으로 다시 정의된 경우 명령 또는 하위 디렉토리에 지정된 액세스 수준이 상위 명령의 액세스 수준을 재정의합니다.

> "admin" 클러스터 관리자만 사용할 수 있는 명령 또는 명령 디렉토리에 대한 액세스를 제공하는 SVM 관리자 역할을 할당할 수 없습니다. 예를 들어, 'security' 명령 디렉토리입니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 사용자 지정 역할 정의:

   'Security login role create -vserver SVM_name -role role -cmddirname command_or_directory_name -access access_level -query'

   다음 명령을 실행하면 'volume' 명령 디렉토리의 명령에 대한 'vol_role' 역할이 전체 액세스되고 'volume snapshot' 하위 디렉토리의 명령에 대한 읽기 전용 액세스가 부여됩니다.

   ```
   cluster1::>security login role create -role vol_role -cmddirname
   "volume" -access all

   cluster1::>security login role create -role vol_role -cmddirname "volume
   snapshot" -access readonly
   ```

   다음 명령어를 통해 'storage' 명령 디렉토리의 명령에 대한 'vm_storage' 역할 읽기 전용 액세스, 'storage encryption' 하위 디렉토리의 명령에 대한 액세스 권한 없음, 'storage aggregate offline' 비내장 명령에 대한 전체 액세스 권한을 부여한다.

   ```
   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage" -access readonly

   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage encryption" -access none

   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage aggregate plex offline" -access all
   ```

에 대한 자세한 내용은 `security login role create` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "보안 로그인 역할이 생성됩니다"
- "스토리지 애그리게이트 플렉스를 오프라인 상태로 설정합니다"
- "스토리지 암호화"

ONTAP 클러스터 관리자를 위한 사전 정의된 역할입니다

클러스터 관리자를 위한 사전 정의된 역할은 대부분의 요구사항을 충족해야 합니다. 필요에 따라 사용자 지정 역할을 만들 수 있습니다. 기본적으로 클러스터 관리자에게는 미리 정의된 "admin" 역할이 할당됩니다.

다음 표에는 클러스터 관리자를 위한 사전 정의된 역할이 나와 있습니다.

이 역할은…	이 수준의 액세스 권한…	명령 또는 명령 디렉토리로 이동합니다
관리자	모두	모든 명령 디렉토리(기본값)
Admin-NO-FSA(ONTAP 9.12.1부터 사용 가능)	읽기/쓰기	• 모든 명령 디렉토리(기본값) • `security login rest-role` • `security login role`

읽기 전용	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	없음
`volume file show-disk-usage`	AutoSupport	모두
• '세트' • '시스템 노드 AutoSupport	없음	기타 모든 명령 디렉토리(기본값)
백업	모두	'vserver services ndmp'
읽기 전용	'볼륨'	없음
기타 모든 명령 디렉토리(기본값)	읽기 전용	모두
• '보안 로그인 비밀번호 사용자 계정 로컬 암호 및 키 정보 관리에만 사용됩니다 • '세트'	• ONTAP 9.8부터 읽기 전용입니다 • ONTAP 9.8 이전 버전에서는 없음	'보안'
읽기 전용	기타 모든 명령 디렉토리(기본값)	SnapLock

모두	• '세트' • '볼륨 생성' • 볼륨 수정 • `volume move` • '볼륨 쇼'	없음
• `volume move governor` • `volume move recommend`	없음	기타 모든 명령 디렉토리(기본값)
없음	없음	모든 명령 디렉토리(기본값)

AutoSupport 역할은 AutoSupport OnDemand가 사용하는 미리 정의된 AutoSupport 계정에 할당됩니다. ONTAP에서는 AutoSupport 계정을 수정하거나 삭제할 수 없습니다. 또한 ONTAP에서는 다른 사용자 계정에 'AutoSupport' 역할을 할당할 수 없습니다.

관련 정보

- "보안 로그인"
- "설정"
- "볼륨"
- "SVM 서비스 NDMP"

ONTAP SVM 관리자를 위한 사전 정의된 역할

SVM 관리자를 위한 사전 정의된 역할은 대부분의 요구사항을 충족해야 합니다. 필요에 따라 사용자 지정 역할을 만들 수 있습니다. 기본적으로 SVM 관리자는 사전 정의된 "vsadmin" 역할이 할당됩니다.

다음 표에는 SVM 관리자를 위한 사전 정의된 역할이 나와 있습니다.

역할 이름	제공합니다

vsadmin을 선택합니다	• 사용자 계정 로컬 암호 및 키 정보 관리 • 볼륨 이동을 제외한 볼륨 관리 • 할당량, qtree, 스냅샷 및 파일 관리 • LUN 관리 • 권한 있는 삭제를 제외한 SnapLock 작업 수행 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • 서비스 구성: DNS, LDAP 및 NIS • 작업 모니터링 • 네트워크 연결 및 네트워크 인터페이스 모니터링 • SVM 상태 모니터링
vsadmin - 볼륨	• 사용자 계정 로컬 암호 및 키 정보 관리 • 볼륨 이동을 제외한 볼륨 관리 • 할당량, qtree, 스냅샷 및 파일 관리 • LUN 관리 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • 서비스 구성: DNS, LDAP 및 NIS • 네트워크 인터페이스 모니터링 • SVM 상태 모니터링
vsadmin - 프로토콜	• 사용자 계정 로컬 암호 및 키 정보 관리 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • 서비스 구성: DNS, LDAP 및 NIS • LUN 관리 • 네트워크 인터페이스 모니터링 • SVM 상태 모니터링
vsadmin - 백업	• 사용자 계정 로컬 암호 및 키 정보 관리 • NDMP 작업 관리 • 복구된 볼륨을 읽기/쓰기로 만듭니다 • SnapMirror 관계 및 스냅샷 관리 • 볼륨 및 네트워크 정보 보기

vsadmin - SnapLock	• 사용자 계정 로컬 암호 및 키 정보 관리 • 볼륨 이동을 제외한 볼륨 관리 • 할당량, qtree, 스냅샷 및 파일 관리 • 권한 있는 삭제를 포함한 SnapLock 작업 수행 • 프로토콜 구성: NFS 및 SMB • 서비스 구성: DNS, LDAP 및 NIS • 작업 모니터링 • 네트워크 연결 및 네트워크 인터페이스 모니터링
vsadmin - 읽기 전용입니다	• 사용자 계정 로컬 암호 및 키 정보 관리 • SVM 상태 모니터링 • 네트워크 인터페이스 모니터링 • 볼륨 및 LUN 보기 • 서비스 및 프로토콜 보기

System Manager를 사용하여 ONTAP 관리자 액세스 관리

관리자에게 할당된 역할에 따라 관리자가 System Manager에서 수행할 수 있는 기능이 결정됩니다. 클러스터 관리자 및 스토리지 VM 관리자를 위한 사전 정의된 역할은 System Manager에서 제공합니다. 관리자 계정을 만들 때 역할을 할당하거나 나중에 다른 역할을 할당할 수 있습니다.

계정 액세스를 설정한 방법에 따라 다음 중 하나를 수행해야 할 수 있습니다.

- 공개 키를 로컬 계정에 연결합니다.
- CA 서명 서버 디지털 인증서를 설치합니다.
- AD, LDAP 또는 NIS 액세스를 구성합니다.

계정 액세스를 활성화하기 전이나 후에 이러한 작업을 수행할 수 있습니다.

관리자에게 역할 할당

다음과 같이 관리자에게 역할을 할당합니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. 사용자 및 역할 * 옆에 있는 을 → 선택합니다.
3. 사용자 * 아래에서 를 선택합니다 + Add .
4. 사용자 이름을 지정하고 * 역할 * 의 드롭다운 메뉴에서 역할을 선택합니다.

5. 사용자의 로그인 방법 및 암호를 지정합니다.

관리자 역할 변경

다음과 같이 관리자의 역할을 변경합니다.

단계

1. 클러스터 > 설정 * 을 클릭합니다.
2. 역할을 변경할 사용자의 이름을 선택한 다음 사용자 이름 옆에 나타나는 을 클릭합니다 ⋮ .
3. 편집 * 을 클릭합니다.
4. 드롭다운 메뉴에서 * 역할 * 의 역할을 선택합니다.

ONTAP 에서 JIT 권한 상승에 액세스

ONTAP 9.17.1부터 클러스터 관리자는 다음을 수행할 수 있습니다. "JIT(Just-In-Time) 권한 상승 구성" ONTAP 사용자가 특정 작업을 수행할 수 있도록 일시적으로 권한을 상승시킬 수 있도록 합니다. JIT가 사용자에 대해 구성된 경우, 사용자는 작업을 수행하는 데 필요한 권한이 있는 역할로 일시적으로 권한을 상승시킬 수 있습니다. 세션이 만료되면 사용자는 원래 액세스 수준으로 돌아갑니다.

클러스터 관리자는 사용자가 JIT 권한 상승에 액세스할 수 있는 기간을 구성할 수 있습니다. 예를 들어, 클러스터 관리자는 사용자 권한 상승에 대한 액세스를 세션당 30분(세션 유효 기간)으로 설정하고 30일(JIT 유효 기간) 동안 사용할 수 있도록 구성할 수 있습니다. 30일 동안 사용자는 필요한 만큼 권한을 상승시킬 수 있지만, 각 세션은 30분으로 제한됩니다.

이 작업에 대해

- JIT 권한 승격은 SSH를 통해 ONTAP 에 액세스하는 사용자에게만 제공됩니다. 승격된 권한은 현재 SSH 세션 내에서만 사용할 수 있지만, 필요한 만큼의 동시 SSH 세션 내에서 권한을 승격할 수 있습니다.
- JIT 권한 승격은 비밀번호, nsswitch 또는 도메인 인증을 사용하여 로그인하는 사용자에게만 지원됩니다. 다중 요소 인증(MFA)은 JIT 권한 승격에 지원되지 않습니다.
- 구성된 세션 또는 JIT 유효 기간이 만료되거나 클러스터 관리자가 사용자의 JIT 액세스 권한을 취소하면 사용자의 JIT 세션이 종료됩니다.

시작하기 전에

- JIT 권한 승격에 액세스하려면 클러스터 관리자가 사용자 계정에 대한 JIT 액세스를 구성해야 합니다. 클러스터 관리자는 권한을 승격할 수 있는 역할과 승격된 권한에 액세스할 수 있는 기간을 결정합니다.

단계

1. 구성된 역할에 대한 권한을 일시적으로 상승시킵니다.

```
security jit-privilege elevate
```

이 명령을 입력하면 로그인 비밀번호를 입력하라는 메시지가 표시됩니다. 계정에 JIT 액세스가 구성된 경우, 설정된 세션 기간 동안 권한이 상승됩니다. 세션 기간이 만료되면 원래 액세스 수준으로 돌아갑니다. 설정된 JIT 유효 기간 내에 필요한 만큼 권한을 상승시킬 수 있습니다.

2. JIT 세션의 남은 시간을 확인하세요.

```
security jit-privilege show-remaining-time
```

현재 JIT 세션에 있는 경우 이 명령은 남은 시간을 표시합니다.

3. 필요한 경우 JIT 세션을 일찍 종료하세요.

```
security jit-privilege reset
```

현재 JIT 세션에 있는 경우 이 명령을 실행하면 JIT 세션이 종료되고 원래 액세스 수준이 복원됩니다.

ONTAP 에서 JIT 권한 상승 구성

ONTAP 9.17.1부터 클러스터 관리자는 JIT(Just-In-Time) 권한 상승을 구성하여 ONTAP 사용자가 특정 작업을 수행할 수 있도록 일시적으로 권한을 상승시킬 수 있습니다. JIT가 사용자에 대해 구성된 경우, "그들의 특권을 높이다" 작업을 수행하는 데 필요한 권한이 있는 역할로 전환됩니다. 세션 기간이 만료되면 사용자는 원래 액세스 수준으로 돌아갑니다.

클러스터 관리자는 사용자가 JIT 권한 상승에 액세스할 수 있는 기간을 구성할 수 있습니다. 예를 들어, 사용자 JIT 권한 상승 액세스를 세션당 30분(세션 유효 기간)으로 설정하고 30일(JIT 유효 기간) 동안 사용할 수 있도록 구성할 수 있습니다. 30일 동안 사용자는 필요한 만큼 권한을 상승시킬 수 있지만, 각 세션은 30분으로 제한됩니다.

JIT 권한 승격은 최소 권한 원칙을 지원하여 사용자가 승격된 권한이 필요한 작업을 수행할 때 해당 권한을 영구적으로 부여하지 않아도 되도록 합니다. 이를 통해 무단 접근이나 실수로 인한 시스템 변경 위험을 줄일 수 있습니다. 다음 예시에서는 JIT 권한 승격의 일반적인 사용 사례를 설명합니다.

- 임시 액세스를 허용합니다. `security login create` 그리고 `security login delete` 사용자의 온보딩 및 오프보딩을 가능하게 하는 명령입니다.
- 임시 액세스 허용 `system node image update` 그리고 `system node upgrade-revert` 업데이트 기간 동안. 업데이트가 완료되면 명령 액세스가 취소됩니다.
- 임시 액세스 허용 `cluster add-node` , `cluster remove-node` , 그리고 `cluster modify` 클러스터 확장 또는 재구성을 활성화합니다. 클러스터 변경이 완료되면 명령 액세스가 취소됩니다.
- 임시 액세스 허용 `volume snapshot restore` 복원 작업 및 백업 대상 관리를 활성화합니다. 복원 또는 구성이 완료되면 명령 액세스 권한이 취소됩니다.
- 임시 액세스 허용 `security audit log show` 규정 준수 검사 중에 감사 로그 검토 및 내보내기를 활성화합니다.

일반적인 JIT 사용 사례에 대한 더 자세한 목록은 다음을 참조하세요. 일반적인 JIT 사용 사례 .

클러스터 관리자는 ONTAP 사용자에 대한 JIT 액세스를 설정하고, 클러스터 전체 또는 특정 SVM에 대해 기본 JIT 유효 기간을 구성할 수 있습니다.

이 작업에 대해

- JIT 권한 승격은 SSH를 통해 ONTAP 에 액세스하는 사용자에게만 제공됩니다. 승격된 권한은 사용자의 현재 SSH

세션 내에서만 사용할 수 있지만, 필요한 만큼의 동시 SSH 세션 내에서 권한을 승격할 수 있습니다.

- JIT 권한 승격은 비밀번호, nsswitch 또는 도메인 인증을 사용하여 로그인하는 사용자에게만 지원됩니다. 다중 요소 인증(MFA)은 JIT 권한 승격에 지원되지 않습니다.

시작하기 전에

- ONTAP 클러스터 관리자여야 합니다. `admin` 다음 작업을 수행하기 위한 권한 수준입니다.

글로벌 **JIT** 설정 수정

ONTAP 클러스터 전체 또는 특정 SVM에 대해 기본 JIT 설정을 수정할 수 있습니다. 이러한 설정은 JIT 액세스 권한이 구성된 사용자의 기본 세션 유효 기간과 최대 JIT 유효 기간을 결정합니다.

이 작업에 대해

- 기본값 `default-session-validity-period` 값은 1시간입니다. 이 설정은 사용자가 JIT 세션에서 상승된 권한에 액세스할 수 있는 시간을 결정합니다. 이 시간이 지나면 다시 상승해야 합니다.
- 기본값 `max-jit-validity-period` 값은 90일입니다. 이 설정은 구성된 시작일 이후 사용자가 JIT 권한 상승에 액세스할 수 있는 최대 기간을 결정합니다. 개별 사용자별로 JIT 유효 기간을 설정할 수 있지만, 최대 JIT 유효 기간을 초과할 수 없습니다.

단계

1. 현재 JIT 설정을 확인하세요.

```
security jit-privilege show -vserver <svm_name>
```

`-vserver` 는 선택 사항입니다. SVM을 지정하지 않으면 명령은 전역 JIT 설정을 표시합니다.

2. JIT 설정을 전역적으로 또는 SVM에 대해 수정합니다.

```
security jit-privilege modify -vserver <svm_name> -default-session
-validity-period <period> -max-jit-validity-period <period>
```

SVM을 지정하지 않으면 명령이 전역 JIT 설정을 수정합니다. 다음 예제는 SVM의 기본 JIT 세션 기간을 45분으로, 최대 JIT 기간을 30일로 설정합니다. `svm1` :
`security jit-privilege modify -vserver svm1 -default-session-validity-period 45m -max-jit-validity-period 30d`

이 예에서 사용자는 한 번에 45분 동안 JIT 권한 상승에 액세스할 수 있으며 구성된 시작 날짜로부터 최대 30일 동안 JIT 세션을 시작할 수 있습니다.

사용자에 대한 **JIT** 권한 승격 액세스 구성

ONTAP 사용자에게 JIT 권한 상승 액세스를 할당할 수 있습니다.

단계

1. 사용자의 현재 JIT 액세스를 확인하세요.

```
security jit-privilege user show -username <username>
```

`-username` 는 선택 사항입니다. 사용자 이름을 지정하지 않으면 모든 사용자의 JIT 액세스 권한이 표시됩니다.

2. 사용자에게 새로운 JIT 액세스 권한 할당:

```
security jit-privilege create -username <username> -vserver <svm_name>
-role <rbac_role> -session-validity-period <period> -jit-validity-period
<period> -start-time <date>
```

   - 만약에 `-vserver` 지정되지 않으면 JIT 액세스는 클러스터 수준에서 할당됩니다.
   - `-role` 사용자가 승격될 RBAC 역할입니다. 지정하지 않으면 `-role` 기본값으로 설정됨 `admin` .
   - `-session-validity-period` 사용자가 새 JIT 세션을 시작하기 전에 승격된 역할에 액세스할 수 있는 기간입니다. 지정하지 않으면 전역 또는 SVM `default-session-validity-period` 사용됩니다.
   - `-jit-validity-period` 구성된 시작 날짜 이후 사용자가 JIT 세션을 시작할 수 있는 최대 기간입니다. 지정하지 않으면 `session-validity-period` 사용됩니다. 이 매개변수는 전역 또는 SVM을 초과할 수 없습니다. `max-jit-validity-period` .
   - `-start-time` 사용자가 JIT 세션을 시작할 수 있는 날짜와 시간입니다. 지정하지 않으면 현재 날짜와 시간이 사용됩니다.

     다음 예제에서는 다음을 허용합니다. `ontap_user` 에 접근하려면 `admin` 새로운 JIT 세션을 시작하기 전에 1시간 동안 역할을 수행해야 합니다. `ontap_user` 2025년 7월 1일 오후 1시부터 60일 동안 JIT 세션을 시작할 수 있습니다.
     `security jit-privilege user create -username ontap_user -role admin -session -validity-period 1h -jit-validity-period 60d -start-time "7/1/25 13:00:00"`

3. 필요한 경우 사용자의 JIT 액세스를 취소합니다.

```
security jit-privilege user delete -username <username> -vserver
<svm_name>
```

사용자의 JIT 액세스를 취소합니다. `-vserver` 지정되지 않으면 JIT 액세스가 클러스터 수준에서 취소됩니다. 사용자가 활성 JIT 세션에 있는 경우 세션이 종료됩니다.

일반적인 **JIT** 사용 사례

다음 표에는 JIT 권한 승격의 일반적인 사용 사례가 나와 있습니다. 각 사용 사례에 대해 관련 명령에 대한 액세스를 제공하도록 RBAC 역할을 구성해야 합니다. 각 명령은 ONTAP 명령 참조에 연결되어 있으며, 해당 명령 및 매개변수에 대한 자세한 정보를 제공합니다.

사용 사례	명령	세부
사용자 및 역할 관리	• '보안 로그인 생성' • '보안 로그인 삭제	온보딩 또는 오프보딩 중에 사용자를 추가/제거하거나 역할을 변경하기 위해 일시적으로 권한을 상승시킵니다.
인증서 관리	• `security certificate create` • `security certificate install`	인증서 설치 또는 갱신을 위해 단기 액세스 권한을 부여합니다.
SSH/CLI 액세스 제어	• `security login create -application ssh`	문제 해결이나 공급업체 지원을 위해 일시적으로 SSH 액세스를 허용합니다.
라이센스 관리	• `system license add` • `system license delete`	기능 활성화 또는 비활성화 중에 라이선스를 추가하거나 제거할 수 있는 권한을 부여합니다.
시스템 업그레이드 및 패치	• `system node image update` • `system node upgrade-revert`	업그레이드 창에 대한 권한을 높인 다음 취소합니다.
네트워크 보안 설정	• `security login role create` • `security login role modify`	네트워크 관련 보안 역할에 대한 임시 변경을 허용합니다.
클러스터 관리	• `cluster add-node` • `cluster remove-node` • `cluster modify`	클러스터 확장이나 재구성을 위해 Elevate를 사용합니다.
SVM 관리	• `vserver create` • `vserver delete` • `vserver modify`	SVM에 프로비저닝 또는 서비스 해제를 위한 관리자 권한을 일시적으로 부여합니다.
볼륨 관리	• '볼륨 생성' • '볼륨 삭제' • 볼륨 수정	볼륨 프로비저닝, 크기 조정 또는 제거를 위해 높이십시오.

사용 사례	명령	세부
스냅샷 관리	• '볼륨 스냅샷 생성' • '볼륨 스냅샷 삭제' • '볼륨 스냅샷 복원'	복구 중에 스냅샷을 삭제하거나 복원하려면 Elevate를 사용합니다.
네트워크 구성	• `network interface create` • `network port vlan create`	유지 관리 기간 동안 네트워크 변경에 대한 권한을 부여합니다.
디스크/집계 관리	• `storage disk assign` • `storage aggregate create` • '스토리지 집계 추가 디스크'	디스크를 추가, 제거하거나 집계를 관리하기 위해 Elevate를 사용합니다.
데이터 보호	• 스냅미러 생성 • `snapmirror modify` • `snapmirror restore`	SnapMirror 관계를 구성하거나 복원하기 위해 일시적으로 상승합니다.
성능 튜닝	• `qos policy-group create` • `qos policy-group modify`	성능 문제 해결이나 튜닝을 위해 Elevate를 활용하세요.
감사 로그 액세스	• 보안 감사 로그 쇼	규정 준수 검사 중에 감사 로그 검토 또는 내보내기를 위해 일시적으로 상승합니다.
이벤트 및 알림 관리	• `event notification create` • `event notification modify`	이벤트 알림이나 SNMP 트랩을 구성하거나 테스트하기 위해 Elevate를 사용합니다.
규정 준수 기반 데이터 액세스	• '볼륨 쇼' • 보안 감사 로그 쇼	감사자가 민감한 데이터나 로그를 검토할 수 있도록 일시적으로 읽기 전용 액세스 권한을 부여합니다.
특권 액세스 검토	• '보안 로그인 쇼' • `security login role show`	일시적으로 권한을 승격하여 권한 있는 접근 권한을 검토하고 보고합니다. 제한된 시간 동안 읽기 전용의 권한 승격된 접근 권한을 부여합니다.

관련 정보

- "클러스터"
- "이벤트 알림"

- "회로망"
- "qos 정책 그룹"
- "보안"
- "SnapMirror를 참조하십시오"
- "내부"
- "시스템"
- "볼륨"
- "SVM"

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 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 라이센스와 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 라이센스도 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 라이센스를 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 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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