



액세스 제어 역할을 관리합니다

ONTAP 9

NetApp
April 24, 2024

목차

액세스 제어 역할을 관리합니다	1
액세스 제어 역할 관리 개요	1
관리자에게 할당된 역할을 수정합니다	1
사용자 지정 역할을 정의합니다	1
클러스터 관리자를 위한 사전 정의된 역할	3
SVM 관리자를 위한 사전 정의된 역할	5
관리자 액세스 제어	6

액세스 제어 역할을 관리합니다

액세스 제어 역할 관리 개요

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.

관리자에게 할당된 역할을 수정합니다

'security login modify' 명령을 사용하여 클러스터 또는 SVM 관리자 계정의 역할을 변경할 수 있습니다. 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 -AuthMethod authentication_method -role role role-comment

전체 명령 구문은 을 참조하십시오 ["워크시트"](#).

["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
```

사용자 지정 역할을 정의합니다

'Security login role create' 명령을 사용하여 사용자 지정 역할을 정의할 수 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 디렉토리에 대한 액세스를 허용하거나 거부합니다.

명령 디렉토리(예: 볼륨)는 관련 명령 및 명령 하위 디렉토리 그룹입니다. 이 절차에서 설명한 경우를 제외하고 명령 디렉토리에 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'
```

전체 명령 구문은 을 참조하십시오 ["워크시트"](#).

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
```

클러스터 관리자를 위한 사전 정의된 역할

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	<ul style="list-style-type: none"> 모든 명령 디렉토리(기본값) security login rest-role security login role

읽기 전용	<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • '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
<ul style="list-style-type: none"> • '보안 로그인 비밀번호 <p>사용자 계정 로컬 암호 및 키 정보 관리에만 사용됩니다</p> <ul style="list-style-type: none"> • '세트' 	없음	'보안'
읽기 전용	기타 모든 명령 디렉토리(기본값)	없음



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.

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	<ul style="list-style-type: none"> • 사용자 계정 로컬 암호 및 키 정보 관리 • 볼륨 이동을 제외한 볼륨 관리 • 할당량, Qtree, 스냅샷 복사본 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	<ul style="list-style-type: none"> • 사용자 계정 로컬 암호 및 키 정보 관리 • 볼륨 이동을 포함한 볼륨 관리 • 할당량, Qtree, 스냅샷 복사본 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 사용자 계정 로컬 암호 및 키 정보 관리 • NDMP 작업 관리 • 복구된 볼륨을 읽기/쓰기로 만듭니다 • SnapMirror 관계 및 Snapshot 복사본 관리 • 볼륨 및 네트워크 정보 보기
vsadmin - SnapLock	<ul style="list-style-type: none"> • 사용자 계정 로컬 암호 및 키 정보 관리 • 볼륨 이동을 제외한 볼륨 관리 • 할당량, Qtree, 스냅샷 복사본 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	<ul style="list-style-type: none"> • 사용자 계정 로컬 암호 및 키 정보 관리 • SVM 상태 모니터링 • 네트워크 인터페이스 모니터링 • 볼륨 및 LUN 보기 • 서비스 및 프로토콜 보기

관리자 액세스 제어

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. 를 선택합니다 → 사용자 및 역할 * 옆에 있습니다.
3. 를 선택합니다 + Add 사용자 * 아래.
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 을 클릭합니다 : 사용자 이름 옆에 표시됩니다.
3. 편집 * 을 클릭합니다.
4. 드롭다운 메뉴에서 * 역할 * 의 역할을 선택합니다.

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.