



# **ONTAP tools for VMware vSphere 구성**

## **ONTAP tools for VMware vSphere 10**

NetApp  
November 04, 2025

# 목차

ONTAP tools for VMware vSphere 구성 .....	1
vCenter Server 인스턴스 추가 .....	1
vCenter Server 인스턴스에 VASA 공급자 등록 .....	1
NFS VAAI 플러그인을 설치하세요 .....	2
ESXi 호스트 설정 구성 .....	3
ESXi 서버 다중 경로 및 시간 초과 설정 구성 .....	3
ESXi 호스트 값 설정 .....	4
ONTAP 사용자 역할 및 권한 구성 .....	5
SVM 집계 매핑 요구 사항 .....	5
ONTAP 사용자 및 역할을 수동으로 생성 .....	6
ONTAP tools for VMware vSphere 업그레이드 .....	14
ONTAP tools for VMware vSphere 업그레이드 .....	16
스토리지 백엔드 추가 .....	16
vCenter Server 인스턴스와 스토리지 백엔드 연결 .....	17
네트워크 액세스 구성 .....	18
데이터 저장소 만들기 .....	18

# ONTAP tools for VMware vSphere 구성

## vCenter Server 인스턴스 추가

vCenter Server 환경에서 가상 데이터스토어를 구성, 관리 및 보호하기 위해 ONTAP tools for VMware vSphere 에 vCenter Server 인스턴스를 추가합니다. 여러 vCenter Server 인스턴스를 추가하는 경우 ONTAP 도구와 각 vCenter Server 간의 보안 통신을 위해 사용자 지정 CA 인증서가 필요합니다.

이 작업에 관하여

ONTAP 도구를 vCenter와 통합하면 프로비저닝, 스냅샷, 데이터 보호와 같은 스토리지 작업을 vSphere 클라이언트에서 직접 수행할 수 있으므로 별도의 스토리지 관리 콘솔로 전환할 필요가 없습니다.

단계

1. 웹 브라우저를 열고 다음 URL로 이동하세요. <https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. **vCenters** > \*Add\*를 선택하여 vCenter Server 인스턴스를 온보딩합니다. vCenter IP 주소 또는 호스트 이름, 사용자 이름, 비밀번호 및 포트 세부 정보를 제공하세요.



ONTAP 도구에 vCenter 인스턴스를 추가하는 데 관리자 계정은 필요하지 않습니다. 관리자 계정 없이도 제한된 권한으로 사용자 정의 역할을 만들 수 있습니다. 참조하다 ["ONTAP tools for VMware vSphere 와 함께 vCenter Server RBAC 사용"](#) 자세한 내용은.

ONTAP 도구에 vCenter Server 인스턴스를 추가하면 다음 작업이 자동으로 트리거됩니다.

- vCenter 클라이언트 플러그인은 원격 플러그인으로 등록됩니다.
- 플러그인과 API에 대한 사용자 정의 권한은 vCenter Server 인스턴스에 적용됩니다.
- 사용자를 관리하기 위해 사용자 정의 역할이 생성됩니다.
- 플러그인은 vSphere 사용자 인터페이스에 바로가기로 나타납니다.

## vCenter Server 인스턴스에 VASA 공급자 등록

ONTAP tools for VMware vSphere 사용하여 vCenter Server 인스턴스에 VASA 공급자를 등록할 수 있습니다. VASA 공급자 설정 섹션에는 선택한 vCenter Server에 대한 VASA 공급자 등록 상태가 표시됩니다. 다중 vCenter 배포에서는 각 vCenter Server 인스턴스에 사용자 지정 CA 인증서가 있는지 확인하세요.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 플러그인 섹션에서 바로가기 > \*NetApp ONTAP 도구\*를 선택합니다.
3. 설정 > \*VASA 공급자 설정\*을 선택하세요. VASA 공급자 등록 상태가 등록되지 않음으로 표시됩니다.

4. VASA 공급자를 등록하려면 등록 버튼을 선택하세요.
5. VASA 공급자의 이름과 자격 증명을 입력하세요. 사용자 이름에는 문자, 숫자, 밑줄만 사용할 수 있습니다. 비밀번호 길이는 8자에서 256자 사이여야 합니다.
6. \*등록\*을 선택하세요.
7. 등록이 성공적으로 완료되고 페이지가 새로 고쳐지면 등록된 VASA 공급자의 상태, 이름, 버전이 표시됩니다. 등록 후 등록 취소 작업이 활성화됩니다.

다음은 무엇입니까?

vCenter 클라이언트에서 온보딩된 VASA 공급자가 VASA 공급자 아래에 나열되어 있는지 확인하세요.

단계

1. vCenter Server 인스턴스로 이동합니다.
2. 관리자 자격 증명으로 로그인하세요.
3. 저장소 공급자 > \*구성\*을 선택합니다. 등록된 VASA 공급자가 올바르게 나열되어 있는지 확인하세요.

## NFS VAAI 플러그인을 설치하세요

NFS vStorage API for Array Integration(NFS VAAI) 플러그인은 VMware vSphere와 NFS 스토리지 어레이를 통합하는 소프트웨어 구성 요소입니다. ONTAP tools for VMware vSphere 사용하여 NFS VAAI 플러그인을 설치하면 NFS 스토리지 어레이의 고급 기능을 활용하여 ESXi 호스트에서 스토리지 어레이 자체로 특정 스토리지 관련 작업을 오프로드할 수 있습니다.

시작하기 전에

- 다운로드 "[VMware VAAI용 NetApp NFS 플러그인](#)" 설치 패키지.
- ESXi 호스트와 vSphere 7.0U3 최신 패치 이상 버전, ONTAP 9.14.1 이상 버전이 있는지 확인하세요.
- NFS 데이터 저장소를 마운트합니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 플러그인 섹션에서 바로가기 > \*NetApp ONTAP 도구\*를 선택합니다.
3. 설정 > \*NFS VAAI 도구\*를 선택합니다.
4. VAAI 플러그인이 vCenter Server에 업로드되면 기존 버전 섹션에서 변경\*을 선택합니다. **VAAI** 플러그인이 **vCenter Server**에 업로드되지 않은 경우 \*업로드 버튼을 선택합니다.
5. 탐색하고 선택하세요 .vib 파일을 선택하고 \*업로드\*를 선택하여 ONTAP 도구에 파일을 업로드합니다.
6. \*ESXi 호스트에 설치\*를 선택하고, NFS VAAI 플러그인을 설치할 ESXi 호스트를 선택한 다음, \*설치\*를 선택합니다.

플러그인 설치에 적합한 ESXi 호스트만 표시됩니다. vSphere Web Client의 최근 작업 섹션에서 설치 진행 상황을 모니터링할 수 있습니다.

7. 설치 후 ESXi 호스트를 수동으로 다시 시작합니다.

VMware 관리자가 ESXi 호스트를 다시 시작하면 ONTAP tools for VMware vSphere NFS VAAI 플러그인을

자동으로 감지하고 활성화합니다.

다음은 무엇인가요?

NFS VAAI 플러그인을 설치하고 ESXi 호스트를 재부팅한 후 VAAI 복사 오프로드에 대한 올바른 NFS 내보내기 정책을 구성해야 합니다. NFS 환경에서 VAAI를 구성할 때 다음 요구 사항을 염두에 두고 내보내기 정책 규칙을 구성하세요.

- 해당 ONTAP 볼륨은 NFSv4 호출을 허용해야 합니다.
- 루트 사용자는 루트로 유지되어야 하며 모든 집합 부모 볼륨에서 NFSv4가 허용되어야 합니다.
- VAAI 지원 옵션은 해당 NFS 서버에서 설정해야 합니다.

절차에 대한 자세한 내용은 다음을 참조하세요. ["VAAI 복사 오프로드를 위한 올바른 NFS 내보내기 정책 구성"](#) KB 문서.

관련 정보

["NFS를 통한 VMware vStorage 지원"](#)

["NFSv4.0 활성화 또는 비활성화"](#)

["NFSv4.2에 대한 ONTAP 지원"](#)

## ESXi 호스트 설정 구성

ESXi 서버의 다중 경로 및 시간 초과 설정을 구성하면 기본 경로에 장애가 발생할 경우 백업 스토리지 경로로 원활하게 전환할 수 있어 높은 가용성과 데이터 무결성이 보장됩니다.

### ESXi 서버 다중 경로 및 시간 초과 설정 구성

ONTAP tools for VMware vSphere NetApp 스토리지 시스템에서 가장 잘 작동하는 ESXi 호스트 다중 경로 설정과 HBA 시간 초과 설정을 확인하고 설정합니다.

이 작업에 관하여

구성 및 시스템 부하에 따라 이 프로세스는 오랜 시간이 걸릴 수 있습니다. 작업 진행 상황은 최근 작업 패널에 표시됩니다.

단계

1. VMware vSphere Web 클라이언트 홈페이지에서 \*호스트 및 클러스터\*를 선택합니다.
2. 호스트를 마우스 오른쪽 버튼으로 클릭하고 \* NetApp ONTAP 도구\* > \*호스트 데이터 업데이트\*를 선택합니다.
3. VMware vSphere Web 클라이언트의 바로가기 페이지에서 플러그인 섹션 아래에 있는 \* NetApp ONTAP 도구\*를 선택합니다.
4. ONTAP tools for VMware vSphere 의 개요(대시보드)에서 **ESXi** 호스트 규정 준수 카드로 이동합니다.
5. 권장 설정 적용 링크를 선택합니다.
6. 권장 호스트 설정 적용 창에서 NetApp 권장 설정을 준수하도록 업데이트할 호스트를 선택하고 \*다음\*을 선택합니다.



ESXi 호스트를 확장하여 현재 값을 확인할 수 있습니다.

7. 설정 페이지에서 필요에 따라 권장되는 값을 선택하세요.
8. 요약 창에서 값을 확인하고 \*마침\*을 선택합니다. 최근 작업 패널에서 진행 상황을 추적할 수 있습니다.

## ESXi 호스트 값 설정

ONTAP tools for VMware vSphere 사용하면 ESXi 호스트에서 시간 초과 및 기타 값을 설정하여 최상의 성능과 성공적인 장애 조치를 보장할 수 있습니다. ONTAP tools for VMware vSphere 설정하는 값은 NetApp 내부 테스트를 기반으로 합니다.

ESXi 호스트에서 다음 값을 설정할 수 있습니다.

### HBA/CNA 어댑터 설정

다음 매개변수를 기본값으로 설정합니다.

- 디스크.QFullSampleSize
- 디스크.QFullThreshold
- Emulex FC HBA 타임아웃
- QLogic FC HBA 시간 초과

### MPIO 설정

MPIO 설정은 NetApp 스토리지 시스템의 기본 경로를 정의합니다. 이들은 사용 가능한 경로 중 어떤 것이 최적화된지 (인터커넥트 케이블을 통과하는 최적화되지 않은 경로와 대조적으로)를 결정하고 해당 경로 중 하나를 기본 경로로 설정합니다.

고성능 환경이나 단일 LUN 데이터 저장소로 성능을 테스트하는 경우 라운드 로빈(VMW\_PSP\_RR) 경로 선택 정책(PSP)의 부하 분산 설정을 기본 IOPS 설정인 1000에서 값 1로 변경하는 것을 고려하세요.



MPIO 설정은 NVMe, NVMe/FC 및 NVMe/TCP 프로토콜에는 적용되지 않습니다.

### NFS 설정

매개변수	이 값을 다음과 같이 설정합니다...
Net.TcpipHeapSize	32
Net.TcpipHeapMax	1024MB
NFS.최대 볼륨	256
NFS41.MaxVolumes	256
NFS.MaxQueueDepth	128 이상
NFS.HeartbeatMaxFailures	10
NFS.하트비트 빈도	12
NFS.하트비트타임아웃	5

# ONTAP 사용자 역할 및 권한 구성

ONTAP tools for VMware vSphere 및 ONTAP System Manager용 ONTAP 도구와 함께 제공되는 JSON 파일을 사용하여 스토리지 백엔드를 관리하기 위한 새로운 사용자 역할과 권한을 구성할 수 있습니다.

시작하기 전에

- `_https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip` 을 사용하여 ONTAP tools for VMware vSphere 에서 ONTAP 권한 파일을 다운로드했어야 합니다.
- ONTAP 도구에서 ONTAP Privileges 파일을 다운로드했어야 합니다.  
`https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip`.



클러스터 또는 스토리지 가상 머신(SVM) 수준에서 직접 사용자를 생성할 수 있습니다. `user_roles.json` 파일을 사용하지 않고도 사용자를 생성할 수 있으며, 그렇게 하려면 SVM 수준에서 최소한의 권한이 필요합니다.

- 저장소 백엔드에 관리자 권한으로 로그인했어야 합니다.

단계

1. 다운로드한 `https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip` 파일을 추출합니다.
2. 클러스터의 클러스터 관리 IP 주소를 사용하여 ONTAP System Manager에 액세스합니다.
3. 관리자 권한으로 클러스터에 로그인합니다. 사용자를 구성하려면 다음 단계를 수행하세요.
  - a. 클러스터 ONTAP 도구 사용자를 구성하려면 클러스터 > 설정 > 사용자 및 역할 창을 선택합니다.
  - b. SVM ONTAP 도구 사용자를 구성하려면 저장소 **SVM** > 설정 > 사용자 및 역할 창을 선택합니다.
  - c. 사용자에서 \*추가\*를 선택합니다.
  - d. 사용자 추가 대화 상자에서 \*가상화 제품\*을 선택합니다.
  - e. \*찾아보기\*하여 ONTAP Privileges JSON 파일을 선택하고 업로드합니다.  
  
제품 필드는 자동으로 채워집니다.
  - f. 드롭다운에서 제품 기능을 \*VSC, VASA 공급자 및 SRA\*로 선택합니다.  
  
역할 필드는 선택한 제품 기능에 따라 자동으로 채워집니다.
  - g. 필요한 사용자 이름과 비밀번호를 입력하세요.
  - h. 사용자에게 필요한 권한(검색, 저장소 생성, 저장소 수정, 저장소 삭제, NAS/SAN 역할)을 선택한 다음 \*추가\*를 선택합니다.

새로운 역할과 사용자가 추가되고, 구성된 역할에 따라 자세한 권한을 볼 수 있습니다.

## SVM 집계 매핑 요구 사항

데이터 저장소 프로비저닝에 SVM 사용자 자격 증명을 사용하기 위해 ONTAP tools for VMware vSphere 데이터 저장소 POST API에 지정된 집계에 볼륨을 내부적으로 생성합니다. ONTAP SVM 사용자 자격 증명을 사용하여 SVM의 매핑되지 않은 집계에 볼륨을 생성하는 것을 허용하지 않습니다. 이 문제를 해결하려면 여기에 설명된 대로

ONTAP REST API 또는 CLI를 사용하여 SVM을 집계와 매핑해야 합니다.

REST API:

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```

ONTAP CLI:

```
still15_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver      Aggregate      State      Size Type      SnapLock
Type-----
-----svm_test      still15_vsim_ucs630f_aggr1
online      10.11GB vmdisk  non-snaplock
```

## ONTAP 사용자 및 역할을 수동으로 생성

JSON 파일을 사용하지 않고 수동으로 사용자와 역할을 생성하려면 이 섹션의 지침을 따르세요.

1. 클러스터의 클러스터 관리 IP 주소를 사용하여 ONTAP System Manager에 액세스합니다.
2. 관리자 권한으로 클러스터에 로그인합니다.
  - a. 클러스터 ONTAP 도구 역할을 구성하려면 클러스터 > 설정 > 사용자 및 역할 창을 선택합니다.
  - b. 클러스터 SVM ONTAP 도구 역할을 구성하려면 저장소 **SVM** > 설정 > 사용자 및 역할 창을 선택하세요.

### 3. 역할 생성:

- a. 역할 표에서 \*추가\*를 선택합니다.
- b. 역할 이름\*과 \*역할 속성 세부 정보를 입력하세요.

드롭다운에서 \*REST API 경로\*와 해당 액세스를 추가합니다.

- c. 필요한 API를 모두 추가하고 변경 사항을 저장합니다.

### 4. 사용자 생성:

- a. 사용자 테이블에서 \*추가\*를 선택합니다.
- b. 사용자 추가 대화 상자에서 \*시스템 관리자\*를 선택합니다.
- c. \*사용자 이름\*을 입력하세요.
- d. 위의 역할 만들기 단계에서 만든 옵션 중에서 \*역할\*을 선택합니다.
- e. 접근 권한을 부여할 응용프로그램과 인증 방법을 입력하세요. 필수 애플리케이션은 ONTAPI와 HTTP이고, 인증 유형은 \*비밀번호\*입니다.
- f. \*사용자 비밀번호\*를 설정하고 사용자를 \*저장\*합니다.



## 관리자가 아닌 글로벌 범위 클러스터 사용자에게 필요한 최소 권한 목록

이 섹션에는 users JSON 파일을 사용하지 않고 생성된 비관리자 글로벌 범위 클러스터 사용자에게 필요한 최소 권한이 나와 있습니다. 로컬 범위에서 클러스터를 추가하는 경우, ONTAP tools for VMware vSphere ONTAP 프로비저닝에 읽기 권한 이상의 권한을 요구하므로 JSON 파일을 사용하여 사용자를 생성하는 것이 좋습니다.

### API 사용:

API	접근 수준	에 사용됨
/api/클러스터	읽기 전용	클러스터 구성 검색
/api/cluster/licensing/licenses	읽기 전용	프로토콜별 라이선스에 대한 라이선스 확인
/api/클러스터/노드	읽기 전용	플랫폼 유형 검색
/api/보안/계정	읽기 전용	권한 검색
/api/보안/역할	읽기 전용	권한 검색
/api/storage/aggregates	읽기 전용	데이터 저장소/볼륨 프로비저닝 중 집계 공간 확인
/api/storage/cluster	읽기 전용	클러스터 수준 공간 및 효율성 데이터를 얻으려면
/api/storage/disks	읽기 전용	집계에 연결된 디스크를 가져오려면
/api/storage/qos/정책	읽기/생성/수정	QoS 및 VM 정책 관리
/api/svm/svms	읽기 전용	클러스터가 로컬로 추가된 경우 SVM 구성을 가져옵니다.
/api/네트워크/ip/인터페이스	읽기 전용	스토리지 백엔드 추가 - 관리 LIF 범위가 클러스터/SVM인지 식별합니다.
/api/storage/availability-zones	읽기 전용	SAZ 디스커버리. ONTAP 9.16.1 릴리스 이상 및 ASA r2 시스템에 적용됩니다.

## VMware vSphere ONTAP API 기반 클러스터 범위 사용자를 ONTAP tools for VMware vSphere 생성



데이터 저장소에 오류가 발생한 경우 PATCH 작업과 자동 롤백을 수행하려면 검색, 생성, 수정 및 삭제 Privileges 필요합니다. 이러한 모든 권한이 부족하면 작업 흐름이 중단되고 정리에 문제가 발생합니다.

검색, 스토리지 생성, 스토리지 수정, 스토리지 삭제 권한이 있는 ONTAP tools for VMware vSphere ONTAP API 기반 사용자를 위한 ONTAP 도구를 생성하면 검색을 시작하고 ONTAP 도구 워크플로를 관리할 수 있습니다.

위에 언급된 모든 권한을 가진 클러스터 범위 사용자를 생성하려면 다음 명령을 실행하세요.

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all

security login rest-role create -role <role-name> -api
```

```

/api/private/cli/snapmirror -access all

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all

security login rest-role create -role <role-name> -api /api/storage/luns
-access all

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all

security login rest-role create -role <role-name> -api
/api/storage/qos/policies -access all

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create

```

```

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify

security login rest-role create -role <role-name> -api /api/cluster
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/licensing/licenses -access readonly

security login rest-role create -role <role-name> -api /api/cluster/nodes
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly

```

```

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/aggregates -access readonly

security login rest-role create -role <role-name> -api
/api/storage/cluster -access readonly

security login rest-role create -role <role-name> -api /api/storage/disks
-access readonly

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly

```

또한 ONTAP 버전 9.16.0 이상의 경우 다음 명령을 실행합니다.

```

security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all

```

ONTAP 버전 9.16.1 이상의 ASA r2 시스템의 경우 다음 명령을 실행합니다.

```
security login rest-role create -role <role-name> -api  
/api/storage/availability-zones -access readonly
```

## VMware vSphere ONTAP API 기반 SVM 범위 사용자를 ONTAP tools for VMware vSphere 생성

모든 권한을 가진 SVM 범위 사용자를 생성하려면 다음 명령을 실행하세요.

```
security login rest-role create -role <role-name> -api  
/api/application/consistency-groups -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/private/cli/snapmirror -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/igroups -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/lun-maps -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/snapmirror/relationships -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/storage/volumes -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api /api/storage/luns  
-access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/storage/namespaces -access all -vserver <vserver-name>
```

```

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly -vserver <vserver-
name>

```

```

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly -vserver <vserver-name>

```

또한 ONTAP 버전 9.16.0 이상의 경우 다음 명령을 실행합니다.

```

security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all -vserver <vserver-name>

```

위에서 생성한 API 기반 역할을 사용하여 새로운 API 기반 사용자를 생성하려면 다음 명령을 실행하세요.

```

security login create -user-or-group-name <user-name> -application http
-authentication-method password -role <role-name> -vserver <cluster-or-
vserver-name>

```

예:

```
security login create -user-or-group-name testvpsraall -application http
-authentication-method password -role
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver C1_stil60-cluster_
```

계정 잠금을 해제하고 관리 인터페이스에 대한 액세스를 활성화하려면 다음 명령을 실행하세요.

```
security login unlock -user <user-name> -vserver <cluster-or-vserver-name>
```

예:

```
security login unlock -username testvpsraall -vserver C1_stil60-cluster
```

## ONTAP tools for VMware vSphere 업그레이드

JSON 파일을 사용하여 클러스터 범위 사용자를 생성한 ONTAP tools for VMware vSphere 의 경우, 사용자 관리자 권한으로 다음 ONTAP CLI 명령을 사용하여 10.3 릴리스로 업그레이드합니다.

제품 기능에 대해서는 다음을 참조하세요.

- VSC
- VSC 및 VASA 공급자
- VSC와 SRA
- VSC, VASA 공급자 및 SRA.

클러스터 권한:

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 네임스페이스 표시" -access all*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 하위 시스템 표시" -access all*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 하위 시스템 호스트 표시" -access all*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 하위 시스템 맵 표시" -access all*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme show-interface" -access read*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 하위 시스템 호스트 추가" -access all*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 하위 시스템 맵 추가" -access all*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 네임스페이스 삭제" -access all*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 하위 시스템 삭제" -access all*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 하위 시스템 호스트 제거" -access all*



보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 하위 시스템 맵 제거" -access all*

json 파일을 사용하여 생성된 SVM 범위 사용자가 있는 ONTAP tools for VMware vSphere 의 경우, 관리자 권한으로 ONTAP CLI 명령을 사용하여 10.3 릴리스로 업그레이드합니다.

SVM 권한:

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 네임스페이스 표시" -access all -vserver <vserver 이름>*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 하위 시스템 표시" -access all -vserver <vserver 이름>*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 하위 시스템 호스트 표시" -access all -vserver <vserver 이름>*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 하위 시스템 맵 표시" -access all -vserver <vserver 이름>*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme show-interface" -access read -vserver <vserver 이름>*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 하위 시스템 호스트 추가" -access all -vserver <vserver 이름>*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 하위 시스템 맵 추가" -access all -vserver <vserver 이름>*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 네임스페이스 삭제" -access all -vserver <vserver 이름>*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 하위 시스템 삭제" -access all -vserver <vserver 이름>*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 하위 시스템 호스트 제거" -access all -vserver <vserver 이름>*

보안 로그인 역할 생성 *-role <기존 역할 이름> -cmddirname "vserver nvme 하위 시스템 맵 제거" -access all -vserver <vserver 이름>*

기존 역할에 *vserver nvme namespace show* 및 *vserver nvme subsystem show* 명령을 추가하면 다음 명령이 추가됩니다.

```
vserver nvme namespace create
```

```
vserver nvme namespace modify
```

```
vserver nvme subsystem create
```

```
vserver nvme subsystem modify
```

## ONTAP tools for VMware vSphere 업그레이드

ONTAP 9.16.1부터 ONTAP tools for VMware vSphere 10.4 사용자로 업그레이드하세요.

JSON 파일과 ONTAP 버전 9.16.1 이상을 사용하여 생성된 클러스터 범위 사용자를 가진 ONTAP tools for VMware vSphere 의 경우, 관리자 권한으로 ONTAP CLI 명령을 사용하여 10.4 릴리스로 업그레이드합니다.

제품 기능에 대해서는 다음을 참조하세요.

- VSC
- VSC 및 VASA 공급자
- VSC와 SRA
- VSC, VASA 공급자 및 SRA.

클러스터 권한:

```
security login role create -role <existing-role-name> -cmddirname "storage  
availability-zone show" -access all
```

## 스토리지 백엔드 추가

스토리지 백엔드를 추가하면 ONTAP 클러스터를 온보딩할 수 있습니다.

이 작업에 관하여

vCenter가 연관된 SVM이 있는 테넌트 역할을 하는 다중 테넌시 설정의 경우 ONTAP 도구 관리자를 사용하여 클러스터를 추가합니다. 스토리지 백엔드를 vCenter Server와 연결하여 온보딩된 vCenter Server 인스턴스에 전역적으로 매핑합니다. vCenter 테넌트는 원하는 스토리지 가상 머신(SVM)을 온보딩해야 합니다. 이를 통해 SVM 사용자는 vVols 데이터 저장소를 프로비저닝할 수 있습니다. SVM을 사용하여 vCenter에 스토리지를 추가할 수 있습니다.

ONTAP 도구 사용자 인터페이스를 사용하여 클러스터 또는 SVM 자격 증명으로 로컬 스토리지 백엔드를 추가합니다. 이러한 스토리지 백엔드는 단일 vCenter로 제한됩니다. 로컬에서 클러스터 자격 증명을 사용하는 경우 연관된 SVM은 자동으로 vCenter에 매핑되어 vVols 또는 VMFS를 관리합니다. SRA를 포함한 VMFS 관리의 경우 ONTAP 도구는 글로벌 클러스터가 필요 없이 SVM 자격 증명을 지원합니다.

## ONTAP 도구 관리자 사용



멀티 테넌트 설정에서는 스토리지 백엔드 클러스터를 전역적으로 추가하고 SVM을 로컬로 추가하여 SVM 사용자 자격 증명을 사용할 수 있습니다.

### 단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 사이드바에서 \*스토리지 백엔드\*를 선택합니다.
4. 스토리지 백엔드를 추가하고 서버 IP 주소 또는 FQDN, 사용자 이름 및 비밀번호 세부 정보를 제공합니다.



IPv4 및 IPv6 주소 관리 LIF가 지원됩니다.

## vSphere 클라이언트 사용자 인터페이스 사용



vSphere 클라이언트 사용자 인터페이스를 통해 스토리지 백엔드를 구성하는 경우 vVols 데이터스토어는 SVM 사용자를 직접 추가하는 것을 지원하지 않는다는 점에 유의하는 것이 중요합니다.

1. vSphere 클라이언트에 로그인합니다.
2. 바로가기 페이지에서 플러그인 섹션 아래에 있는 \*NetApp ONTAP 도구\*를 선택합니다.
3. 사이드바에서 \*스토리지 백엔드\*를 선택합니다.
4. 스토리지 백엔드를 추가하고 서버 IP 주소, 사용자 이름, 비밀번호, 포트 세부 정보를 제공합니다.



SVM 사용자를 직접 추가하려면 클러스터 기반 자격 증명과 IPv4 및 IPv6 주소 관리 LIF를 추가하거나 SVM 관리 LIF와 함께 SVM 기반 자격 증명을 제공할 수 있습니다.

다음은 무엇인가요?

목록이 새로 고쳐지고, 목록에서 새로 추가된 스토리지 백엔드를 볼 수 있습니다.

## vCenter Server 인스턴스와 스토리지 백엔드 연결

스토리지 백엔드를 vCenter Server에 연결하여 스토리지 백엔드와 온보딩된 vCenter Server 인스턴스 간에 전역적으로 매핑을 생성합니다.

### 단계

1. 웹 브라우저에서 ONTAP 도구 관리자를 실행합니다.  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 로 로그인합니다.
3. 사이드바에서 vCenter를 선택합니다.
4. 스토리지 백엔드와 연결할 vCenter Server 인스턴스에 대한 세로 줄임표를 선택합니다.

5. 드롭다운에서 스토리지 백엔드를 선택하여 vCenter Server 인스턴스를 필요한 스토리지 백엔드와 연결합니다.

## 네트워크 액세스 구성

네트워크 액세스를 구성하지 않은 경우 ESXi 호스트에서 검색된 모든 IP 주소가 기본적으로 내보내기 정책에 추가됩니다. 특정 IP 주소 몇 개만 내보내기 정책에 추가하고 나머지는 제외하도록 구성할 수 있습니다. 그러나 제외된 ESXi 호스트에서 마운트 작업을 수행하면 작업이 실패합니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 플러그인 섹션 아래의 바로가기 페이지에서 \* NetApp ONTAP 도구\*를 선택합니다.
3. ONTAP 도구의 왼쪽 창에서 설정 > 네트워크 액세스 관리 > \*편집\*으로 이동합니다.

여러 개의 IP 주소를 추가하려면 싹표, 범위, CIDR(Classless Inter-Domain Routing) 또는 이 세 가지를 조합하여 목록을 구분하세요.

4. \*저장\*을 선택하세요.

## 데이터 저장소 만들기

호스트 클러스터 수준에서 데이터 저장소를 생성하면 대상의 모든 호스트에 데이터 저장소가 생성되어 마운트되고, 현재 사용자에게 실행 권한이 있는 경우에만 작업이 활성화됩니다.

**vCenter Server** 및 **ONTAP** 도구로 관리되는 데이터스토어와 기본 데이터스토어 간 상호 운용성

ONTAP tools for VMware vSphere 데이터스토어에 대한 중첩된 igroup을 생성하며, 부모 igroup은 데이터스토어에 특정하고 자식 igroup은 호스트에 매핑됩니다. ONTAP 시스템 관리자에서 플랫폼 igroup을 만들고 ONTAP 도구를 사용하지 않고도 이를 사용하여 VMFS 데이터 저장소를 만들 수 있습니다. 참조하다 ["SAN 이니시에이터 및 igroup 관리"](#) 자세한 내용은.

스토리지에 ONTAP 도구에 온보딩되고 데이터 저장소 검색이 실행되면 플랫폼 igroup과 VMFS 데이터 저장소가 ONTAP 도구에서 관리되고 중첩된 igroup으로 변환됩니다. 이전의 플랫폼 igroup을 사용하여 새로운 데이터 저장소를 생성할 수 없습니다. 중첩된 igroup을 재사용하려면 ONTAP 도구 사용자 인터페이스나 REST API를 사용해야 합니다.

## vVols 데이터 저장소 만들기

ONTAP tools for VMware vSphere 부터 ASA r2 시스템에 thin.vVol이라는 공간 효율성을 갖춘 vVols 데이터 저장소를 생성할 수 있습니다. VASA 공급자는 vVol 데이터 저장소를 생성하는 동안 컨테이너와 원하는 프로토콜 엔드포인트를 생성합니다. 이 컨테이너에는 백업 볼륨이 없습니다.

### 시작하기 전에

- 루트 집계가 SVM에 매핑되지 않았는지 확인하세요.
- 선택한 vCenter에 VASA 공급자가 등록되어 있는지 확인하세요.
- ASA r2 스토리지 시스템에서는 SVM이 SVM 사용자에게 대한 집계에 매핑되어야 합니다.

### 단계

1. vSphere 클라이언트에 로그인합니다.
2. 호스트 시스템, 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 \* NetApp ONTAP 도구\* > \*데이터 저장소 만들기\*를 선택합니다.
3. vVols \*데이터 저장소 유형\*을 선택합니다.
4. 데이터 저장소 이름\*과 \*프로토콜 정보를 입력하세요.



ASA r2 시스템은 vVols 대한 iSCSI 및 FC 프로토콜을 지원합니다.

5. 데이터스토어를 생성할 스토리지 VM을 선택하세요.
6. 고급 옵션:
  - \*사용자 지정 내보내기 정책\*을 선택하는 경우 모든 개체에 대해 vCenter에서 검색을 실행해야 합니다. 이 옵션은 사용하지 않는 것이 좋습니다.
  - iSCSI 및 FC 프로토콜에 대해 사용자 지정 이니시에이터 그룹 이름을 선택할 수 있습니다.



ASA r2 스토리지 시스템 유형 SVM에서는 데이터 저장소가 논리적 컨테이너일 뿐이므로 스토리지 단위(LUN/네임스페이스)가 생성되지 않습니다.

7. 저장소 속성 창에서 새 볼륨을 만들거나 기존 볼륨을 사용할 수 있습니다. 하지만 이 두 유형의 볼륨을 결합하여 vVols 데이터 저장소를 만들 수는 없습니다.

새 볼륨을 생성할 때 데이터 저장소에서 QoS를 활성화할 수 있습니다. 기본적으로 LUN 생성 요청마다 볼륨이 하나씩 생성됩니다. 이 단계는 ASA r2 스토리지 시스템을 사용하는 vVols 데이터 저장소에는 적용되지 않습니다.

8. 요약 창에서 선택 사항을 검토하고 \*마침\*을 선택하세요.

## NFS 데이터 저장소 만들기

VMware 네트워크 파일 시스템(NFS) 데이터 저장소는 NFS 프로토콜을 사용하여 네트워크를 통해 ESXi 호스트를 공유 스토리지 장치에 연결합니다. NFS 데이터 저장소는 일반적으로 VMware vSphere 환경에서 사용되며 단순성, 유연성 등 여러 가지 이점을 제공합니다.

### 단계

1. vSphere 클라이언트에 로그인합니다.

2. 호스트 시스템, 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 \*NetApp ONTAP 도구\* > \*데이터 저장소 만들기\*를 선택합니다.
3. 데이터 저장소 유형 필드에서 NFS를 선택합니다.
4. 이름 및 프로토콜 창에 데이터 저장소 이름, 크기 및 프로토콜 정보를 입력합니다. 고급 옵션에서 \*데이터 저장소 클러스터\*와 \*Kerberos 인증\*을 선택합니다.



Kerberos 인증은 NFS 4.1 프로토콜을 선택한 경우에만 사용할 수 있습니다.

5. 저장소 창에서 \*플랫폼\*과 \*저장소 VM\*을 선택합니다.
6. 고급 옵션에서 \*사용자 지정 내보내기 정책\*을 선택하면 모든 개체에 대해 vCenter에서 검색을 실행합니다. 이 옵션은 사용하지 않는 것이 좋습니다.



SVM의 기본/루트 볼륨 정책을 사용하여 NFS 데이터 저장소를 만들 수 없습니다.

- 고급 옵션에서 비대칭 토글 버튼은 플랫폼 드롭다운에서 성능이나 용량이 선택된 경우에만 표시됩니다.
  - 플랫폼 드롭다운에서 모든 옵션을 선택하면 플랫폼이나 비대칭 플래그에 관계없이 vCenter에 속한 SVM을 볼 수 있습니다.
7. 저장소 속성 창에서 볼륨 생성을 위한 집계를 선택합니다. 고급 옵션에서 필요에 따라 공간 예약 및 \*QoS 활성화\*를 선택합니다.
  8. 요약 창에서 선택 내용을 검토하고 \*마침\*을 선택합니다.

NFS 데이터 저장소가 생성되어 모든 호스트에 마운트됩니다.

#### VMFS 데이터 저장소 만들기

VMFS(가상 머신 파일 시스템)는 VMware vSphere 환경에서 가상 머신 파일을 저장하는 클러스터형 파일 시스템입니다. VMFS를 사용하면 여러 ESXi 호스트가 동일한 가상 머신 파일에 동시에 액세스할 수 있으므로 vMotion 및 고가용성과 같은 기능을 사용할 수 있습니다.

보호된 클러스터에서:

- VMFS 데이터 저장소만 생성할 수 있습니다. 보호된 클러스터에 VMFS 데이터 저장소를 추가하면 데이터 저장소가 자동으로 보호됩니다.
- 하나 이상의 보호된 호스트 클러스터가 있는 데이터 센터에는 데이터 저장소를 만들 수 없습니다.
- 부모 호스트 클러스터가 "자동화된 장애 조치 이중 정책" 유형(균일/비균일 구성) 관계로 보호되는 경우 ESXi 호스트에 데이터 저장소를 생성할 수 없습니다.
- 비동기 관계로 보호되는 ESXi 호스트에만 VMFS 데이터 저장소를 만들 수 있습니다. "자동화된 장애 조치 이중화" 정책으로 보호되는 호스트 클러스터의 일부인 ESXi 호스트에 데이터스토어를 만들고 마운트할 수 없습니다.

시작하기 전에

- ONTAP 스토리지 측에서 각 프로토콜에 대한 서비스와 LIF를 활성화합니다.
- ASA r2 스토리지 시스템의 SVM 사용자를 집계하기 위해 SVM을 매핑합니다.
- NVMe/TCP 프로토콜을 사용하는 경우 ESXi 호스트를 구성합니다.
  - a. 검토하다 ["VMware 호환성 가이드"](#)



VMware vSphere 7.0 U3 이상 버전은 NVMe/TCP 프로토콜을 지원합니다. 하지만 VMware vSphere 8.0 이상 버전을 권장합니다.

- b. 네트워크 인터페이스 카드(NIC) 공급업체가 NVMe/TCP 프로토콜을 사용하는 ESXi NIC를 지원하는지 확인합니다.
  - c. NIC 공급업체 사양에 따라 NVMe/TCP에 대한 ESXi NIC를 구성합니다.
  - d. VMware vSphere 7 릴리스를 사용하는 경우 VMware 사이트의 지침을 따르세요. ["NVMe over TCP 어댑터에 대한 VMkernel 바인딩 구성"](#) NVMe/TCP 포트 바인딩을 구성합니다. VMware vSphere 8 릴리스를 사용하는 경우 다음을 따르세요. ["ESXi에서 TCP를 통한 NVMe 구성"](#) NVMe/TCP 포트 바인딩을 구성합니다.
  - e. VMware vSphere 7 릴리스의 경우 페이지의 지침을 따르세요. ["NVMe over RDMA 또는 NVMe over TCP 소프트웨어 어댑터 활성화"](#) NVMe/TCP 소프트웨어 어댑터를 구성합니다. VMware vSphere 8 릴리스의 경우 다음을 따르세요. ["RDMA 또는 TCP 어댑터를 통한 NVMe 소프트웨어 추가"](#) NVMe/TCP 소프트웨어 어댑터를 구성합니다.
  - f. 달리다 ["스토리지 시스템 및 호스트 검색"](#) ESXi 호스트에 대한 작업입니다. 자세한 내용은 다음을 참조하세요. ["VMFS 데이터 저장소에 대해 vSphere 8.0 업데이트 1 및 ONTAP 9.13.1을 사용하여 NVMe/TCP를 구성하는 방법"](#).
- NVMe/FC 프로토콜을 사용하는 경우 다음 단계를 수행하여 ESXi 호스트를 구성하세요.
    - a. 아직 활성화되지 않았다면 ESXi 호스트에서 NVMe over Fabrics(NVMe-oF)를 활성화하세요.
    - b. SCSI 구역화를 완료합니다.
    - c. ESXi 호스트와 ONTAP 시스템이 물리적 및 논리적 계층에서 연결되어 있는지 확인하세요.

FC 프로토콜에 대한 ONTAP SVM을 구성하려면 다음을 참조하세요. ["FC에 대한 SVM 구성"](#).

VMware vSphere 8.0에서 NVMe/FC 프로토콜을 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요. ["ONTAP 사용한 ESXi 8.x에 대한 NVMe-oF 호스트 구성"](#).

VMware vSphere 7.0에서 NVMe/FC를 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요. ["ONTAP NVMe/FC 호스트 구성 가이드"](#) 그리고 ["TR-4684"](#).

#### 단계

1. vSphere 클라이언트에 로그인합니다.
2. 호스트 시스템, 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 \* NetApp ONTAP 도구\* > \*데이터 저장소 만들기\*를 선택합니다.
3. VMFS 데이터 저장소 유형을 선택하세요.
4. 이름 및 프로토콜 창에 데이터 저장소 이름, 크기 및 프로토콜 정보를 입력합니다. 기존 VMFS 데이터 저장소 클러스터에 새 데이터 저장소를 추가하려면 고급 옵션에서 데이터 저장소 클러스터 선택기를 선택합니다.
5. 저장소 창에서 저장소 VM을 선택합니다. 필요에 따라 고급 옵션 섹션에 \*사용자 지정 개시자 그룹 이름\*을 제공합니다. 데이터 저장소에 대해 기존 igroup을 선택하거나 사용자 정의 이름으로 새 igroup을 만들 수 있습니다.

NVMe/FC 또는 NVMe/TCP 프로토콜을 선택하면 새로운 네임스페이스 하위 시스템이 생성되어 네임스페이스 매핑에 사용됩니다. 네임스페이스 하위 시스템은 데이터 저장소 이름을 포함하는 자동 생성된 이름을 사용하여 생성됩니다. 저장소 창의 고급 옵션에 있는 사용자 지정 네임스페이스 하위 시스템 이름 필드에서 네임스페이스 하위 시스템의 이름을 바꿀 수 있습니다.

6. 저장소 속성 창에서:

- a. 드롭다운 옵션에서 \*집계\*를 선택합니다.



ASA r2 스토리지 시스템의 경우, ASA r2 스토리지가 분산 스토리지이므로 집계 옵션이 표시되지 않습니다. ASA r2 스토리지 시스템 유형으로 SVM을 선택하면 스토리지 속성 페이지에 QoS 활성화 옵션이 표시됩니다.

- b. 선택한 프로토콜에 따라 씬 유형의 공간 예비를 갖춘 저장 장치(LUN/네임스페이스)가 생성됩니다.



ONTAP 9.16.1부터 ASA r2 스토리지 시스템은 클러스터당 최대 12개의 노드를 지원합니다.

- c. 이기종 클러스터인 12개 노드 SVM이 있는 ASA r2 스토리지 시스템에 대해 \*성능 서비스 수준\*을 선택합니다. 선택한 SVM이 동종 클러스터이거나 SVM 사용자를 사용하는 경우 이 옵션을 사용할 수 없습니다.

'모든'은 기본 성능 서비스 수준(PSL) 값입니다. 이 설정은 ONTAP 균형 배치 알고리즘을 사용하여 저장 장치를 생성합니다. 하지만 필요에 따라 성능이나 익스트림 옵션을 선택할 수 있습니다.

- d. 필요에 따라 기존 볼륨 사용, **QoS** 활성화 옵션을 선택하고 세부 정보를 제공합니다.



ASA r2 스토리지 유형에서는 볼륨 생성 또는 선택이 스토리지 유닛 생성 (LUN/네임스페이스)에 적용되지 않습니다. 따라서 이러한 옵션은 표시되지 않습니다.



기존 볼륨을 사용하여 NVMe/FC 또는 NVMe/TCP 프로토콜을 사용하는 VMFS 데이터 저장소를 만들 수 없습니다. 새 볼륨을 만들어야 합니다.

7. 요약 창에서 데이터 저장소 세부 정보를 검토하고 \*마침\*을 선택합니다.



보호된 클러스터에 데이터 저장소를 생성하면 "데이터 저장소가 보호된 클러스터에 마운트되고 있습니다."라는 읽기 전용 메시지가 표시됩니다.

결과

VMFS 데이터 저장소가 생성되어 모든 호스트에 마운트됩니다.



## 저작권 정보

Copyright © 2025 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.