ONTAP SAN 드라이버

Trident

NetApp
July 01, 2026

목차

ONTAP SAN 드라이버

ONTAP SAN 드라이버 개요

ONTAP 및 Cloud Volumes ONTAP SAN 드라이버를 사용하여 ONTAP 백엔드를 구성하는 방법에 대해 알아보십시오.

ONTAP SAN 드라이버 세부 정보

Trident는 ONTAP 클러스터와 통신하기 위해 다음과 같은 SAN 스토리지 드라이버를 제공합니다. 지원되는 액세스 모드는 *ReadWriteOnce*(RWO), *ReadOnlyMany*(ROX), *ReadWriteMany*(RWX), *ReadWriteOncePod*(RWOP)입니다.

드라이버	프로토콜	**volumeMode**	지원되는 액세스 모드	지원되는 파일 시스템
`ontap-san`	FC를 통한 iSCSI SCSI	블록	RWO, ROX, RWX, RWOP	파일 시스템 없음, 원시 블록 디바이스
`ontap-san`	FC를 통한 iSCSI SCSI	파일 시스템	RWO, RWOP ROX 및 RWX는 Filesystem 볼륨 모드에서 사용할 수 없습니다.	`xfs`, `ext3`, `ext4`
`ontap-san`	NVMe/TCP 다음을 참조하십시오. NVMe/TCP에 대한 추가 고려 사항.	블록	RWO, ROX, RWX, RWOP	파일 시스템 없음, 원시 블록 디바이스
`ontap-san`	NVMe/TCP 다음을 참조하십시오. NVMe/TCP에 대한 추가 고려 사항.	파일 시스템	RWO, RWOP ROX 및 RWX는 Filesystem 볼륨 모드에서 사용할 수 없습니다.	`xfs`, `ext3`, `ext4`
`ontap-san-economy`	iSCSI	블록	RWO, ROX, RWX, RWOP	파일 시스템 없음, 원시 블록 디바이스

드라이버	프로토콜	**volumeMode**	지원되는 액세스 모드	지원되는 파일 시스템
`ontap-san-economy`	iSCSI	파일 시스템	RWO, RWOP ROX 및 RWX는 Filesystem 볼륨 모드에서 사용할 수 없습니다.	`xfs`, `ext3`, `ext4`

- `ontap-san-economy`지속적 볼륨 사용 수가 "지원되는 ONTAP 볼륨 제한"보다 높을 것으로 예상되는 경우에만 사용하십시오.
- `ontap-nas-economy`영구 볼륨 사용 수가 "지원되는 ONTAP 볼륨 제한"보다 높을 것으로 예상되고 `ontap-san-economy` 드라이버를 사용할 수 없는 경우에만 사용하십시오.
- 데이터 보호, 재해 복구 또는 이동성이 필요할 것으로 예상되는 경우에는 `ontap-nas-economy`사용하지 마십시오.
- NetApp은 ontap-san을 제외한 모든 ONTAP 드라이버에서 Flexvol 자동 확장을 사용하지 않는 것을 권장합니다. 해결 방법으로 Trident는 스냅샷 예약 기능을 지원하며, 이에 따라 Flexvol 볼륨을 확장합니다.

사용자 권한

Trident는 일반적으로 `admin` 클러스터 사용자 또는 `vsadmin` SVM 사용자, 또는 동일한 역할을 가진 다른 이름의 사용자를 사용하여 ONTAP 또는 SVM 관리자로 실행되어야 합니다. Amazon FSx for NetApp ONTAP 배포의 경우 Trident는 클러스터 `fsxadmin` 사용자 또는 `vsadmin` SVM 사용자, 또는 동일한 역할을 가진 다른 이름의 사용자를 사용하여 ONTAP 또는 SVM 관리자로 실행되어야 합니다. `fsxadmin` 사용자는 클러스터 관리자 사용자를 제한적으로 대체합니다.

`limitAggregateUsage` 매개변수를 사용하는 경우 클러스터 관리자 권한이 필요합니다. Trident와 함께 Amazon FSx for NetApp ONTAP를 사용하는 경우 `limitAggregateUsage` 매개변수는 `vsadmin` 및 `fsxadmin` 사용자 계정에서 작동하지 않습니다. 이 매개변수를 지정하면 구성 작업이 실패합니다.

ONTAP 내에서 Trident 드라이버가 사용할 수 있는 더욱 제한적인 역할을 생성하는 것도 가능하지만 권장하지 않습니다. 대부분의 새로운 Trident 릴리스에서는 추가 API를 호출하므로 이를 고려해야 하기 때문에 업그레이드가 어렵고 오류가 발생하기 쉽습니다.

NVMe/TCP에 대한 추가 고려 사항

Trident는 `ontap-san` 드라이버를 사용하여 다음을 포함한 NVMe(Non-Volatile Memory Express) 프로토콜을 지원합니다.

- IPv6
- NVMe 볼륨의 스냅샷 및 클론
- NVMe 볼륨 크기 조정
- Trident 외부에서 생성된 NVMe 볼륨을 가져와서 Trident에서 수명 주기를 관리할 수 있도록 합니다
- NVMe 네이티브 다중 경로

- K8s 노드의 정상 종료 또는 비정상 종료(24.06)

Trident는 다음을 지원하지 않습니다.

- NVMe에서 기본적으로 지원하는 DH-HMAC-CHAP
- 장치 매퍼(DM) 다중 경로
- LUKS 암호화

NVMe는 ONTAP REST API에서만 지원되며 ONTAPI(ZAPI)에서는 지원되지 않습니다.

ONTAP SAN 드라이버를 사용하여 백엔드를 구성할 준비를 하십시오

ONTAP SAN 드라이버를 사용하여 ONTAP 백엔드를 구성하기 위한 요구 사항 및 인증 옵션을 이해하십시오.

요구 사항

모든 ONTAP 백엔드의 경우 Trident를 사용하려면 SVM에 하나 이상의 애그리게이트를 할당해야 합니다.

"ASA r2 시스템"는 스토리지 계층 구현 방식에서 다른 ONTAP 시스템(ASA, AFF, FAS)과 차이가 있습니다. ASA r2 시스템에서는 애그리게이트 대신 스토리지 가용성 영역을 사용합니다. ASA r2 시스템에서 SVM에 애그리게이트를 할당하는 방법에 대한 "이것" 기술 자료 문서를 참조하십시오.

여러 드라이버를 실행할 수도 있고, 특정 드라이버를 가리키는 스토리지 클래스를 생성할 수도 있다는 점을 기억하세요. 예를 들어, `san-dev` 드라이버를 사용하는 `ontap-san` 클래스와 `san-default` 드라이버를 사용하는 `ontap-san-economy` 클래스를 구성할 수 있습니다.

모든 Kubernetes 워커 노드에는 적절한 iSCSI 도구가 설치되어 있어야 합니다. 자세한 내용은 "작업자 노드를 준비합니다"를 참조하십시오.

ONTAP 백엔드를 인증합니다

Trident는 ONTAP 백엔드를 인증하는 두 가지 모드를 제공합니다.

- 자격 증명 기반: 필요한 권한을 가진 ONTAP 사용자의 사용자 이름과 암호입니다. ONTAP 버전과의 최대 호환성을 보장하기 위해 `admin` 또는 `vsadmin`와 같이 미리 정의된 보안 로그인 역할을 사용하는 것이 좋습니다.
- 인증서 기반: Trident는 백엔드에 설치된 인증서를 사용하여 ONTAP 클러스터와 통신할 수도 있습니다. 이 경우 백엔드 정의에는 클라이언트 인증서, 키, 그리고 사용하는 경우(권장) 신뢰할 수 있는 CA 인증서의 Base64 인코딩 값이 포함되어야 합니다.

기존 백엔드를 업데이트하여 자격 증명 기반 방식과 인증서 기반 방식 간에 전환할 수 있습니다. 단, 한 번에 하나의 인증 방법만 지원됩니다. 다른 인증 방법으로 전환하려면 백엔드 구성에서 기존 방법을 제거해야 합니다.

자격 증명과 인증서를 모두 제공하려고 하면 구성 파일에 두 개 이상의 인증 방법이 제공되었다는 오류와 함께 백엔드 생성이 실패합니다.

자격 증명 기반 인증 활성화

Trident는 ONTAP 백엔드와 통신하기 위해 SVM 범위/클러스터 범위 관리자의 자격 증명이 필요합니다. `admin` 또는 `vsadmin`와 같은 표준 사전 정의된 역할을 사용하는 것이 좋습니다. 이렇게 하면 향후 Trident 릴리스에서 사용할 수 있는 기능 API를 노출할 수 있는 향후 ONTAP 릴리스와의 상위 호환성이 보장됩니다. 사용자 지정 보안 로그인 역할을 생성하여 Trident와 함께 사용할 수 있지만 권장하지 않습니다.

백엔드 정의 샘플은 다음과 같습니다.

YAML

```yaml
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: password
```

JSON

```json
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-san",
  "managementLIF": "10.0.0.1",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password"
}
```

백엔드 정의는 자격 증명이 평문으로 저장되는 유일한 위치라는 점을 명심하십시오. 백엔드가 생성된 후 사용자 이름/암호는 Base64로 인코딩되어 Kubernetes 시크릿으로 저장됩니다. 백엔드 생성 또는 업데이트는 자격 증명을 알아야 하는 유일한 단계입니다. 따라서 이는 Kubernetes/스토리지 관리자가 수행하는 관리자 전용 작업입니다.

인증서 기반 인증을 활성화합니다

신규 및 기존 백엔드는 인증서를 사용하여 ONTAP 백엔드와 통신할 수 있습니다. 백엔드 정의에는 세 가지 매개변수가 필요합니다.

- clientCertificate: 클라이언트 인증서의 Base64 인코딩 값입니다.
- clientPrivateKey: 연결된 개인 키의 Base64 인코딩 값입니다.
- trustedCACertificate: 신뢰할 수 있는 CA 인증서의 Base64 인코딩 값입니다. 신뢰할 수 있는 CA를 사용하는 경우 이 매개변수를 반드시 제공해야 합니다. 신뢰할 수 있는 CA를 사용하지 않는 경우에는 이 매개변수를 무시할 수 있습니다.

일반적인 워크플로에는 다음 단계가 포함됩니다.

단계

1. 클라이언트 인증서와 키를 생성합니다. 생성 시 CN(일반 이름)을 인증할 ONTAP 사용자로 설정합니다.

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key
-out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=admin"
```

2. ONTAP 클러스터에 신뢰할 수 있는 CA 인증서를 추가합니다. 스토리지 관리자가 이미 처리했을 수 있습니다. 신뢰할 수 있는 CA를 사용하지 않는 경우 이 단계를 건너뛰십시오.

```
security certificate install -type server -cert-name <trusted-ca-cert-
name> -vserver <vserver-name>
ssl modify -vserver <vserver-name> -server-enabled true -client-enabled
true -common-name <common-name> -serial <SN-from-trusted-CA-cert> -ca
<cert-authority>
```

3. ONTAP 클러스터에 클라이언트 인증서 및 키(1단계)를 설치합니다.

```
security certificate install -type client-ca -cert-name <certificate-
name> -vserver <vserver-name>
security ssl modify -vserver <vserver-name> -client-enabled true
```

> ⓘ 이 명령을 실행하면 ONTAP에서 인증서 입력을 요청합니다. 1단계에서 생성된 `k8senv.pem` 파일의 내용을 붙여넣은 다음 `END`를 입력하여 설치를 완료하십시오.

4. ONTAP 보안 로그인 역할이 `cert` 인증 방법을 지원하는지 확인합니다.

```
security login create -user-or-group-name admin -application ontapi
-authentication-method cert
security login create -user-or-group-name admin -application http
-authentication-method cert
```

5. 생성된 인증서를 사용하여 인증을 테스트하십시오. <ONTAP Management LIF> 및 <vserver name>를 Management LIF IP 및 SVM 이름으로 바꾸십시오.

```
curl -X POST -Lk https://<ONTAP-Management-
LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key
--cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp
xmlns="http://www.netapp.com/filer/admin" version="1.21"
vfiler="<vserver-name>"><vserver-get></vserver-get></netapp>'
```

6. 인증서, 키 및 신뢰할 수 있는 CA 인증서를 Base64로 인코딩합니다.

```
base64 -w 0 k8senv.pem >> cert_base64
base64 -w 0 k8senv.key >> key_base64
base64 -w 0 trustedca.pem >> trustedca_base64
```

7. 이전 단계에서 얻은 값을 사용하여 백엔드를 생성합니다.

```
cat cert-backend.json
{
"version": 1,
"storageDriverName": "ontap-san",
"backendName": "SanBackend",
"managementLIF": "1.2.3.4",
"svm": "vserver_test",
"clientCertificate": "Faaaakkkkeeee...Vaaalllluuuueeee",
"clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",
"trustedCACertificate": "QNFinfO...SiqOyN",
"storagePrefix": "myPrefix_"
}

tridentctl create backend -f cert-backend.json -n trident
+------------+----------------+--------------------------------------
+--------+---------+
|    NAME    | STORAGE DRIVER |                 UUID                 |
STATE  | VOLUMES |
+------------+----------------+--------------------------------------
+--------+---------+
| SanBackend | ontap-san      | 586b1cd5-8cf8-428d-a76c-2872713612c1 |
online |       0 |
+------------+----------------+--------------------------------------
+--------+---------+
```

인증 방법을 업데이트하거나 자격 증명을 변경하세요

기존 백엔드를 업데이트하여 다른 인증 방법을 사용하거나 자격 증명을 교체할 수 있습니다. 이 기능은 양방향으로 작동합니다. 사용자 이름/암호를 사용하는 백엔드를 인증서를 사용하는 방식으로 업데이트할 수 있고, 인증서를 사용하는 백엔드를 사용자 이름/암호 기반으로 업데이트할 수도 있습니다. 이렇게 하려면 기존 인증 방법을 제거하고 새 인증 방법을 추가해야 합니다. 그런 다음 필요한 매개변수가 포함된 업데이트된 backend.json 파일을 사용하여 `tridentctl backend update`을(를) 실행합니다.

```
cat cert-backend-updated.json
{
"version": 1,
"storageDriverName": "ontap-san",
"backendName": "SanBackend",
"managementLIF": "1.2.3.4",
"svm": "vserver_test",
"username": "vsadmin",
"password": "password",
"storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
tridentctl update backend SanBackend -f cert-backend-updated.json -n
trident
+------------+----------------+--------------------------------------
+--------+---------+
|    NAME    | STORAGE DRIVER |                 UUID                 |
STATE   | VOLUMES |
+------------+----------------+--------------------------------------
+--------+---------+
| SanBackend | ontap-san      | 586b1cd5-8cf8-428d-a76c-2872713612c1 |
online |       9 |
+------------+----------------+--------------------------------------
+--------+---------+
```

암호를 교체할 때는 스토리지 관리자가 먼저 ONTAP에서 사용자의 암호를 업데이트해야 합니다. 그 후 백엔드 업데이트를 진행합니다. 인증서를 교체할 때는 사용자에게 여러 개의 인증서를 추가할 수 있습니다. 백엔드를 업데이트하여 새 인증서를 사용하도록 설정한 후, ONTAP 클러스터에서 이전 인증서를 삭제할 수 있습니다.

백엔드를 업데이트해도 이미 생성된 볼륨에 대한 액세스는 중단되지 않으며, 이후에 생성된 볼륨 연결에도 영향을 미치지 않습니다. 백엔드 업데이트가 성공적으로 완료되면 Trident가 ONTAP 백엔드와 통신하여 향후 볼륨 작업을 처리할 수 있음을 의미합니다.

Trident용 사용자 지정 ONTAP 역할 생성

Trident에서 작업을 수행하기 위해 ONTAP 관리자 역할을 사용할 필요가 없도록 최소 권한으로 ONTAP 클러스터 역할을 생성할 수 있습니다. Trident 백엔드 구성에 사용자 이름을 포함하면 Trident는 생성한 ONTAP 클러스터 역할을 사용하여 작업을 수행합니다.

Trident 사용자 지정 역할 생성에 대한 자세한 내용은 "Trident 사용자 지정 역할 생성기"을 참조하십시오.

ONTAP CLI 사용

1. 다음 명령을 사용하여 새 역할을 생성합니다.

```
security login role create <role_name\> -cmddirname "command" -access all
-vserver <svm_name\>
```

2. Trident 사용자의 사용자 이름을 생성합니다.

```
security login create -username <user_name\> -application ontapi
-authmethod <password\> -role <name_of_role_in_step_1\> -vserver
<svm_name\> -comment "user_description"
```

3. 사용자에게 역할 매핑:

```
security login modify username <user_name\> -vserver <svm_name\> -role
<role_name\> -application ontapi -application console -authmethod
<password\>
```

System Manager 사용

ONTAP System Manager에서 다음 단계를 수행하십시오.

1. 사용자 지정 역할 생성:
   a. 클러스터 수준에서 사용자 지정 역할을 생성하려면 * Cluster > Settings * 를 선택합니다.

      (또는) SVM 수준에서 사용자 지정 역할을 생성하려면 *스토리지 > 스토리지 VM > `required SVM`> 설정 > 사용자 및 역할*을 선택하십시오.

   b. 사용자 및 역할 옆에 있는 화살표 아이콘(→)을 선택합니다.
   c. 역할 에서 **+**추가 를 선택합니다.
   d. 역할에 대한 규칙을 정의하고 *저장*을 클릭합니다.
2. **Trident** 사용자에게 역할 매핑: + 사용자 및 역할 페이지에서 다음 단계를 수행합니다.
   a. 사용자 아래에서 추가 아이콘 *+*를 선택합니다.
   b. 필요한 사용자 이름을 선택하고 역할 드롭다운 메뉴에서 역할을 선택합니다.
   c. *저장*을 클릭합니다.

자세한 내용은 다음 페이지를 참조하십시오.

- "ONTAP 관리를 위한 사용자 지정 역할" 또는 "사용자 지정 역할 정의"
- "역할 및 사용자 작업"

양방향 **CHAP**를 사용하여 연결을 인증합니다

Trident는 `ontap-san` 및 `ontap-san-economy` 드라이버에 대해 양방향 CHAP를 사용하여 iSCSI 세션을 인증할 수 있습니다. 이를 위해서는 백엔드 정의에서 `useCHAP` 옵션을 활성화해야 합니다. `true`로 설정하면 Trident는 SVM의 기본 이니시에이터 보안을 양방향 CHAP로 구성하고 백엔드 파일에서 사용자 이름과 암호를 설정합니다.

NetApp은 연결 인증에 양방향 CHAP를 사용하는 것을 권장합니다. 다음 샘플 구성을 참조하십시오.

```
---
version: 1
storageDriverName: ontap-san
backendName: ontap_san_chap
managementLIF: 192.168.0.135
svm: ontap_iscsi_svm
useCHAP: true
username: vsadmin
password: password
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
```

useCHAP 매개변수는 한 번만 구성할 수 있는 부울 옵션입니다. 기본적으로 false로 설정됩니다. true로 설정한 후에는 false로 설정할 수 없습니다.

`useCHAP=true` 외에도 `chapInitiatorSecret`, `chapTargetInitiatorSecret`, `chapTargetUsername` 및 `chapUsername` 필드는 백엔드 정의에 반드시 포함되어야 합니다. 백엔드 생성 후에는 `tridentctl update`를 실행하여 비밀 키를 변경할 수 있습니다.

작동 방식

`useCHAP`을 true로 설정하면 스토리지 관리자가 Trident에 스토리지 백엔드에서 CHAP를 구성하도록 지시합니다. 여기에는 다음 사항이 포함됩니다.

- SVM에서 CHAP 설정:
  - SVM의 기본 이니시에이터 보안 유형이 없음(기본값으로 설정)이고 볼륨에 기존 LUN이 없는 경우, Trident는 기본 보안 유형을 `CHAP`로 설정하고 CHAP 이니시에이터 및 대상 사용자 이름과 암호 구성을 진행합니다.
  - SVM에 LUN이 포함되어 있는 경우 Trident는 SVM에서 CHAP를 활성화하지 않습니다. 이렇게 하면 SVM에 이미 있는 LUN에 대한 액세스가 제한되지 않습니다.
- CHAP 이니시에이터 및 타겟 사용자 이름과 암호를 구성합니다. 이러한 옵션은 백엔드 구성에 지정해야 합니다(위 참조).

백엔드가 생성되면 Trident는 해당 tridentbackend CRD를 생성하고 CHAP 시크릿과 사용자 이름을 Kubernetes 시크릿으로 저장합니다. 이 백엔드에서 Trident가 생성하는 모든 PV는 CHAP를 통해 마운트되고 연결됩니다.

자격 증명을 교체하고 백엔드를 업데이트합니다

`backend.json` 파일의 CHAP 매개변수를 업데이트하여 CHAP 자격 증명을 업데이트할 수 있습니다. 이를 위해서는 CHAP 암호를 업데이트하고 `tridentctl update` 명령을 사용하여 이러한 변경 사항을 반영해야 합니다.

백엔드의 CHAP 암호를 업데이트할 때는 `tridentctl`을 사용하여 백엔드를 업데이트해야 합니다. Trident가 이러한 변경 사항을 인식할 수 없으므로 ONTAP CLI 또는 ONTAP System Manager를 사용하여 스토리지 클러스터의 자격 증명을 업데이트하지 마십시오.

```
cat backend-san.json
{
    "version": 1,
    "storageDriverName": "ontap-san",
    "backendName": "ontap_san_chap",
    "managementLIF": "192.168.0.135",
    "svm": "ontap_iscsi_svm",
    "useCHAP": true,
    "username": "vsadmin",
    "password": "password",
    "chapInitiatorSecret": "cl9qxUpDaTeD",
    "chapTargetInitiatorSecret": "rqxigXgkeUpDaTeD",
    "chapTargetUsername": "iJF4heBRT0TCwxyz",
    "chapUsername": "uh2aNCLSd6cNwxyz",
}

./tridentctl update backend ontap_san_chap -f backend-san.json -n trident
+----------------+----------------+--------------------------------------
+--------+---------+
|   NAME         | STORAGE DRIVER |                 UUID                 |
STATE  | VOLUMES |
+----------------+----------------+--------------------------------------
+--------+---------+
| ontap_san_chap | ontap-san      | aa458f3b-ad2d-4378-8a33-1a472ffbeb5c |
online |       7 |
+----------------+----------------+--------------------------------------
+--------+---------+
```

기존 연결은 영향을 받지 않으며, SVM에서 Trident가 자격 증명을 업데이트하면 계속 활성 상태로 유지됩니다. 새 연결은 업데이트된 자격 증명을 사용하고 기존 연결은 계속 활성 상태로 유지됩니다. 기존 PV를 연결 해제했다가 다시 연결하면 업데이트된 자격 증명이 사용됩니다.

ONTAP SAN 구성 옵션 및 예

Trident 설치 환경에서 ONTAP SAN 드라이버를 생성하고 사용하는 방법을 알아보세요. 이

섹션에서는 백엔드 구성 예제와 백엔드를 StorageClasses에 매핑하는 방법에 대한 세부 정보를 제공합니다. "ASA r2 시스템"는 스토리지 계층 구현 방식에서 다른 ONTAP 시스템(ASA, AFF, FAS)과 차이가 있습니다. 이러한 차이점은 표기된 특정 매개변수의 사용에 영향을 미칩니다. "ASA r2 시스템과 다른 ONTAP 시스템 간의 차이점에 대해 자세히 알아보십시오". Trident 백엔드 구성에서 시스템이 ASA r2임을 지정할 필요가 없습니다. `ontap-san`을 `storageDriverName`로 선택하면 Trident가 ASA r2 또는 기타 ONTAP 시스템을 자동으로 감지합니다. 아래 표에 나와 있는 것처럼 일부 백엔드 구성 매개 변수는 ASA r2 시스템에 적용되지 않습니다.

ontap-san 드라이버(iSCSI, NVMe/TCP 및 FC 프로토콜 포함)만 ASA r2 시스템에서 지원됩니다.

백엔드 **configuration** 옵션

백엔드 구성 옵션은 다음 표를 참조하십시오.

매개변수	설명	기본값
version		항상 1
storageDriverName	스토리지 드라이버의 이름	ontap-san 또는 ontap-san-economy
backendName	사용자 지정 이름 또는 스토리지 백엔드	드라이버 이름 + "_" + dataLIF
managementLIF	클러스터 또는 SVM 관리 LIF의 IP 주소입니다. 정규화된 도메인 이름(FQDN)을 지정할 수 있습니다. Trident를 IPv6 플래그를 사용하여 설치한 경우 IPv6 주소를 사용하도록 설정할 수 있습니다. IPv6 주소는 `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]`와 같이 대괄호로 정의해야 합니다. 원활한 MetroCluster 전환을 위해서는 MetroCluster 예시을 참조하십시오. "vsadmin" 자격 증명을 사용하는 경우 `managementLIF`은 SVM의 자격 증명이어야 하며, "admin" 자격 증명을 사용하는 경우 `managementLIF`는 클러스터의 자격 증명이어야 합니다.	"10.0.0.1", "[2001:1234:abcd::fefe]"

매개변수	설명	기본값
`dataLIF`	프로토콜 LIF의 IP 주소입니다. Trident를 IPv6 플래그를 사용하여 설치한 경우 IPv6 주소를 사용하도록 설정할 수 있습니다. IPv6 주소는 `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]`와 같이 대괄호로 정의해야 합니다. **iSCSI**의 경우 지정하지 마십시오. Trident는 "ONTAP 선택적 LUN 매핑"를 사용하여 다중 경로 세션을 설정하는 데 필요한 iSCSI LIF를 검색합니다. `dataLIF`가 명시적으로 정의된 경우 경고가 생성됩니다. **MetroCluster**의 경우 생략합니다. MetroCluster 예시를 참조하십시오.	SVM에 의해 도출됨
`svm`	사용할 스토리지 가상 머신 **MetroCluster**의 경우 생략 MetroCluster 예시를 참조하십시오.	SVM `managementLIF`이 지정된 경우 파생됩니다
`useCHAP`	ONTAP SAN 드라이버용 iSCSI 인증에 CHAP를 사용합니다[부울 매개 변수]. 백엔드에 제공된 SVM에 대해 양방향 CHAP를 기본 인증으로 구성하고 사용하려면 Trident에 대해 `true`로 설정하십시오. 자세한 내용은 "ONTAP SAN 드라이버를 사용하여 백엔드를 구성할 준비를 하십시오"를 참조하십시오. **FCP** 또는 **NVMe/TCP**에서는 지원되지 않습니다.	`false`
`chapInitiatorSecret`	CHAP 이니시에이터 암호입니다. 다음의 경우 필수 사항입니다 `useCHAP=true`	""
`labels`	볼륨에 적용할 임의의 JSON 형식 레이블 세트	""
`chapTargetInitiatorSecret`	CHAP 대상 개시자 비밀 키. 다음의 경우 필수 사항입니다 `useCHAP=true`	""
`chapUsername`	인바운드 사용자 이름. 다음의 경우 필수 사항입니다 `useCHAP=true`	""
`chapTargetUsername`	대상 사용자 이름. 다음의 경우 필수 사항입니다 `useCHAP=true`	""
`clientCertificate`	클라이언트 인증서의 Base64 인코딩 값입니다. 인증서 기반 인증에 사용됩니다	""
`clientPrivateKey`	클라이언트 개인 키를 Base64로 인코딩한 값입니다. 인증서 기반 인증에 사용됩니다	""
`trustedCACertificate`	신뢰할 수 있는 CA 인증서의 Base64 인코딩 값입니다. 선택 사항입니다. 인증서 기반 인증에 사용됩니다.	""
`username`	ONTAP 클러스터와 통신하는 데 필요한 사용자 이름입니다. 자격 증명 기반 인증에 사용됩니다. Active Directory 인증은 "Active Directory 자격 증명을 사용하여 Trident를 백엔드 SVM에 인증합니다"을(를) 참조하십시오.	""
`password`	ONTAP 클러스터와 통신하는 데 필요한 암호입니다. 자격 증명 기반 인증에 사용됩니다. Active Directory 인증은 "Active Directory 자격 증명을 사용하여 Trident를 백엔드 SVM에 인증합니다"을(를) 참조하십시오.	""

매개변수	설명	기본값
`svm`	사용할 스토리지 가상 머신	SVM `managementLIF`이 지정된 경우 파생됩니다
`storagePrefix`	SVM에서 새 볼륨을 프로비저닝할 때 사용되는 접두사입니다. 나중에 수정할 수 없습니다. 이 매개 변수를 업데이트하려면 새 백엔드를 생성해야 합니다.	`trident`
`aggregate`	프로비저닝용 애그리게이트(선택 사항, 설정된 경우 SVM에 할당해야 함). `ontap-nas-flexgroup` 드라이버의 경우 이 옵션은 무시됩니다. 할당하지 않으면 사용 가능한 애그리게이트 중 하나를 사용하여 FlexGroup 볼륨을 프로비저닝할 수 있습니다. SVM에서 애그리게이트가 업데이트되면 Trident 컨트롤러를 재시작하지 않고도 SVM을 폴링하여 Trident에 자동으로 업데이트됩니다. Trident에서 볼륨을 프로비저닝하도록 특정 애그리게이트를 구성한 경우, 해당 애그리게이트의 이름이 변경되거나 SVM에서 이동되면 SVM 애그리게이트를 폴링하는 동안 Trident에서 백엔드가 실패 상태로 전환됩니다. 백엔드를 다시 온라인 상태로 전환하려면 SVM에 있는 애그리게이트로 변경하거나 해당 애그리게이트를 완전히 제거해야 합니다. **ASA r2** 시스템의 경우 지정하지 마십시오.	""
`limitAggregateUsage`	사용량이 이 비율을 초과하면 프로비저닝이 실패합니다. Amazon FSx for NetApp ONTAP 백엔드를 사용하는 경우 `limitAggregateUsage`을(를) 지정하지 마십시오. 제공된 `fsxadmin` 및 `vsadmin`에는 Trident를 사용하여 애그리게이트 사용량을 검색하고 제한하는 데 필요한 권한이 포함되어 있지 않습니다. **ASA r2** 시스템의 경우 지정하지 마십시오.	"" (기본적으로 적용되지 않음)
`limitVolumeSize`	요청된 볼륨 크기가 이 값을 초과하면 프로비저닝이 실패합니다. 또한 LUN에 대해 관리하는 볼륨의 최대 크기를 제한합니다.	"" (기본적으로 적용되지 않음)
`lunsPerFlexvol`	FlexVol당 최대 LUN 수는 [50, 200] 범위 내에 있어야 합니다.	`100`
`debugTraceFlags`	문제 해결 시 사용할 디버그 플래그입니다. 예: {"api":false, "method":true} 문제 해결 중이거나 자세한 로그 덤프가 필요한 경우가 아니면 사용하지 마십시오.	`null`

매개변수	설명	기본값
useREST	ONTAP REST API를 사용하기 위한 부울 매개 변수입니다. `useREST`로 설정하면 `true` Trident는 ONTAP REST API를 사용하여 백엔드와 통신하고, `false`로 설정하면 Trident는 ONTAPI(ZAPI) 호출을 사용하여 백엔드와 통신합니다. 이 기능을 사용하려면 ONTAP 9.11.1 이상이 필요합니다. 또한 사용되는 ONTAP 로그인 역할은 `ontapi` 애플리케이션에 대한 액세스 권한이 있어야 합니다. 이는 사전 정의된 `vsadmin` 및 `cluster-admin` 역할로 충족됩니다. Trident 24.06 릴리스 및 ONTAP 9.15.1 이상부터 `useREST`는 기본적으로 `true`로 설정되며, ONTAPI(ZAPI) 호출을 사용하려면 `useREST`를 `false`로 변경하십시오. `useREST`는 NVMe/TCP에 대한 모든 자격을 갖추고 있습니다. NVMe는 ONTAP REST API에서만 지원되며 ONTAPI(ZAPI)에서는 지원되지 않습니다. 지정된 경우 **ASA r2** 시스템의 경우 항상 **`true`**로 설정하십시오.	ONTAP 9.15.1 이상의 경우 true, 그렇지 않은 경우 false.
sanType	iSCSI의 경우 iscsi, NVMe/TCP의 경우 nvme 또는 Fibre Channel(FC)을 통한 SCSI의 경우 `fcp`를 선택하는 데 사용합니다.	iscsi 공백인 경우

매개변수	설명	기본값
formatOptions	`formatOptions`를 사용하여 `mkfs` 명령에 대한 명령줄 인수를 지정할 수 있으며, 이는 볼륨을 포맷할 때마다 적용됩니다. 이를 통해 원하는 대로 볼륨을 포맷할 수 있습니다. 장치 경로를 제외하고 mkfs 명령 옵션과 유사하게 formatOptions를 지정해야 합니다. 예: "-E nodiscard" • ontap-san 및 ontap-san-economy 드라이버에서 iSCSI 프로토콜과 함께 지원됩니다.* 또한 **iSCSI** 및 **NVMe/TCP** 프로토콜을 사용하는 **ASA r2** 시스템에서도 지원됩니다.	
limitVolumePoolSize	ontap-san-economy 백엔드에서 LUN을 사용할 때 요청할 수 있는 최대 FlexVol 크기입니다.	"" (기본적으로 적용되지 않음)
denyNewVolumePools	ontap-san-economy 백엔드에서 LUN을 포함할 새 FlexVol 볼륨 생성을 제한합니다. 기존 Flexvol만 새 PV 프로비저닝에 사용됩니다.	

formatOptions 사용 권장 사항

Trident는 포맷 프로세스를 신속하게 진행하기 위해 다음 옵션을 권장합니다.

- **-E nodiscard (ext3, ext4):** mkfs 실행 시 블록을 버리지 않도록 합니다(초기 블록 버리기는 솔리드 스테이트 장치 및 스파스/씬 프로비저닝 스토리지에서 유용합니다). 이 옵션은 더 이상 사용되지 않는 "-K" 옵션을 대체하며 ext3, ext4 파일 시스템에 적용됩니다.
- **-K (xfs):** mkfs 실행 시 블록을 버리려고 시도하지 않습니다. 이 옵션은 xfs 파일 시스템에 적용됩니다.

Active Directory 자격 증명을 사용하여 **Trident**를 백엔드 **SVM**에 인증합니다

Active Directory(AD) 자격 증명을 사용하여 백엔드 SVM에 인증하도록 Trident를 구성할 수 있습니다. AD 계정이 SVM에 액세스하려면 먼저 클러스터 또는 SVM에 대한 AD 도메인 컨트롤러 액세스를 구성해야 합니다. AD 계정을 사용하여 클러스터를 관리하려면 도메인 터널을 생성해야 합니다. 자세한 내용은 "ONTAP에서 Active Directory 도메인 컨트롤러 액세스 구성"를 참조하십시오.

단계

1. 백엔드 SVM에 대한 DNS(Domain Name System) 설정을 구성합니다.

```
vserver services dns create -vserver <svm_name> -dns-servers
<dns_server_ip1>,<dns_server_ip2>
```

2. Active Directory에서 SVM용 컴퓨터 계정을 생성하려면 다음 명령을 실행하십시오.

```
vserver active-directory create -vserver DataSVM -account-name ADSERVER1
-domain demo.netapp.com
```

3. 이 명령을 사용하여 클러스터 또는 SVM을 관리할 AD 사용자 또는 그룹을 생성합니다

```
security login create -vserver <svm_name> -user-or-group-name
<ad_user_or_group> -application <application> -authentication-method domain
-role vsadmin
```

4. Trident 백엔드 구성 파일에서 `username` 및 `password` 매개 변수를 각각 AD 사용자 또는 그룹 이름과 암호로 설정하십시오.

볼륨 프로비저닝을 위한 백엔드 구성 옵션

구성의 `defaults` 섹션에서 이러한 옵션을 사용하여 기본 프로비저닝을 제어할 수 있습니다. 예를 들어, 아래 구성 예를 참조하십시오.

매개변수	설명	기본값
`spaceAllocation`	LUN의 공간 할당	"true" 지정된 경우 **ASA r2** 시스템의 경우 `**true**`로 설정하십시오.
`spaceReserve`	공간 예약 모드: "none"(씬) 또는 "volume"(씩). **ASA r2** 시스템의 경우 `none`로 설정합니다.	"없음"
`snapshotPolicy`	사용할 스냅샷 정책입니다. **ASA r2** 시스템의 경우 `**none**`로 설정하세요.	"없음"
`qosPolicy`	생성된 볼륨에 할당할 QoS 정책 그룹입니다. 스토리지 풀/백엔드별로 qosPolicy 또는 adaptiveQosPolicy 중 하나를 선택하십시오. Trident에서 QoS 정책 그룹을 사용하려면 ONTAP 9.8 이상이 필요합니다. 공유되지 않는 QoS 정책 그룹을 사용하고 정책 그룹이 각 구성 요소에 개별적으로 적용되도록 해야 합니다. 공유 QoS 정책 그룹은 모든 워크로드의 총 처리량에 대한 상한선을 적용합니다.	""
`adaptiveQosPolicy`	생성된 볼륨에 할당할 적응형 QoS 정책 그룹입니다. 스토리지 풀/백엔드당 qosPolicy 또는 adaptiveQosPolicy 중 하나를 선택하십시오	""
`snapshotReserve`	스냅샷에 할당할 볼륨 비율입니다. **ASA r2** 시스템의 경우 지정하지 마십시오.	`snapshotPolicy`이(가) "none"이면 "0", 그렇지 않으면 ""
`splitOnClone`	생성 시 상위 항목에서 클론 분할	"false"
`encryption`	새 볼륨에서 NetApp Volume Encryption(NVE)을 활성화합니다. 기본값은 `false`입니다. 이 옵션을 사용하려면 클러스터에서 NVE 라이센스가 있고 활성화되어 있어야 합니다. 백엔드에서 NAE가 활성화된 경우 Trident에서 프로비저닝된 모든 볼륨은 NAE가 활성화됩니다. 자세한 내용은 다음을 참조하십시오. "Trident가 NVE 및 NAE와 작동하는 방식"	"false" 지정된 경우 **ASA r2** 시스템의 경우 `**true**`로 설정하십시오.
`luksEncryption`	LUKS 암호화를 활성화합니다. 다음을 참조하십시오. "Linux Unified Key Setup(LUKS) 사용".	"" **ASA r2** 시스템의 경우 `**false**`로 설정하세요.
`tieringPolicy`	계층화 정책에서 "none"을 사용합니다. **ASA r2** 시스템의 경우 지정하지 마십시오.	

매개변수	설명	기본값
nameTemplate	사용자 지정 볼륨 이름을 생성하기 위한 템플릿입니다.	""

볼륨 프로비저닝 예

다음은 기본값이 정의된 예입니다.

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: trident_svm
username: admin
password: <password>
labels:
  k8scluster: dev2
  backend: dev2-sanbackend
storagePrefix: alternate-trident
debugTraceFlags:
  api: false
  method: true
defaults:
  spaceReserve: volume
  qosPolicy: standard
  spaceAllocation: 'false'
  snapshotPolicy: default
  snapshotReserve: '10'
```

ontap-san 드라이버를 사용하여 생성된 모든 볼륨에 대해 Trident는 LUN 메타데이터를 수용하기 위해 FlexVol에 10%의 추가 용량을 더합니다. LUN은 사용자가 PVC에서 요청한 정확한 크기로 프로비저닝됩니다. Trident는 FlexVol에 10%를 추가합니다(ONTAP에서 사용 가능한 크기로 표시됨). 이제 사용자는 요청한 만큼의 사용 가능한 용량을 확보할 수 있습니다. 또한 이 변경 사항은 사용 가능한 공간이 완전히 활용되지 않는 한 LUN이 읽기 전용이 되는 것을 방지합니다. 이는 ontap-san-economy에는 적용되지 않습니다.

`snapshotReserve`을(를) 정의하는 백엔드의 경우 Trident는 다음과 같이 볼륨 크기를 계산합니다.

```
Total volume size = [(PVC requested size) / (1 - (snapshotReserve
percentage) / 100)] * 1.1
```

1.1은 Trident가 LUN 메타데이터를 수용하기 위해 FlexVol에 추가하는 10%입니다. snapshotReserve = 5%이고 PVC 요청 = 5GiB인 경우 전체 볼륨 크기는 5.79GiB이고 사용 가능한 크기는 5.5GiB입니다. volume show 명령은

다음 예와 유사한 결과를 표시해야 합니다.

현재로서는 크기 조정만이 기존 볼륨에 대한 새 계산을 사용하는 유일한 방법입니다.

최소 구성 예

다음 예시들은 대부분의 매개변수를 기본값으로 유지하는 기본 구성을 보여줍니다. 이것이 백엔드를 정의하는 가장 쉬운 방법입니다.

> Amazon FSx for NetApp ONTAP에서 Trident를 사용하는 경우 NetApp에서는 LIF에 IP 주소 대신 DNS 이름을 지정하는 것이 좋습니다.

ONTAP SAN 예

이는 `ontap-san` 드라이버를 사용한 기본 구성입니다.

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
labels:
  k8scluster: test-cluster-1
  backend: testcluster1-sanbackend
username: vsadmin
password: <password>
```

MetroCluster 예시

"SVM 복제 및 복구" 중에 스위치오버 및 스위치백 후 백엔드 정의를 수동으로 업데이트하지 않아도 되도록 백엔드를 구성할 수 있습니다.

원활한 전환 및 복귀를 위해 `managementLIF`을 사용하여 `SVM`을 지정하고 `svm` 매개변수를 생략하십시오. 예를 들면 다음과 같습니다.

```
version: 1
storageDriverName: ontap-san
managementLIF: 192.168.1.66
username: vsadmin
password: password
```

ONTAP SAN 이코노미 예

```
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
username: vsadmin
password: <password>
```

인증서 기반 인증 예

이 기본 구성 예에서 `clientCertificate`, `clientPrivateKey` 및 `trustedCACertificate`(신뢰할 수 있는 CA를 사용하는 경우 선택 사항)는 `backend.json`에 채워지며 각각 클라이언트 인증서, 개인 키 및 신뢰할 수 있는 CA 인증서의 base64로 인코딩된 값을 사용합니다.

```
---
version: 1
storageDriverName: ontap-san
backendName: DefaultSANBackend
managementLIF: 10.0.0.1
svm: svm_iscsi
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
```

양방향 **CHAP** 예

이 예제들은 `useCHAP`로 설정된 `true` 백엔드를 생성합니다.

ONTAP SAN CHAP 예

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
labels:
  k8scluster: test-cluster-1
  backend: testcluster1-sanbackend
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
username: vsadmin
password: <password>
```

ONTAP SAN 경제 **CHAP** 예

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
username: vsadmin
password: <password>
```

NVMe/TCP 예

ONTAP 백엔드에 NVMe가 구성된 SVM이 있어야 합니다. NVMe/TCP를 위한 기본 백엔드 구성입니다.

```
---
version: 1
backendName: NVMeBackend
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_nvme
username: vsadmin
password: password
sanType: nvme
useREST: true
```

FC(FCP)를 통한 SCSI 예

ONTAP 백엔드에 FC가 구성된 SVM이 있어야 합니다. 다음은 FC를 위한 기본 백엔드 구성입니다.

```
---
version: 1
backendName: fcp-backend
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_fc
username: vsadmin
password: password
sanType: fcp
useREST: true
```

nameTemplate을 사용한 백엔드 구성 예

```
---
version: 1
storageDriverName: ontap-san
backendName: ontap-san-backend
managementLIF: <ip address>
svm: svm0
username: <admin>
password: <password>
defaults:
  nameTemplate:
"{{.volume.Name}}_{{.labels.cluster}}_{{.volume.Namespace}}_{{.vo\
    lume.RequestName}}"
labels:
  cluster: ClusterA
  PVC: "{{.volume.Namespace}}_{{.volume.RequestName}}"
```

formatOptions 예시(**ontap-san-economy** 드라이버용)

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: ""
svm: svm1
username: ""
password: "!"
storagePrefix: whelk_
debugTraceFlags:
  method: true
  api: true
defaults:
  formatOptions: -E nodiscard
```

가상 풀이 있는 백엔드의 예

이 샘플 백엔드 정의 파일에서는 모든 스토리지 풀에 대해 특정 기본값(예: `spaceReserve`없음, `spaceAllocation`false, `encryption`false)이 설정되어 있습니다. 가상 풀은 스토리지 섹션에서 정의됩니다.

Trident는 "설명" 필드에 프로비저닝 레이블을 설정합니다. 설명은 FlexVol 볼륨에 설정됩니다. Trident는 프로비저닝 시 가상 풀에 있는 모든 레이블을 스토리지 볼륨으로 복사합니다. 편의를 위해 스토리지 관리자는 가상 풀별로 레이블을 정의하고 레이블별로 볼륨을 그룹화할 수 있습니다.

이 예시에서 일부 스토리지 풀은 자체 `spaceReserve`, `spaceAllocation` 및 `encryption` 값을 설정하고, 일부 풀은 기본값을 재정의합니다.

ONTAP SAN 예

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
username: vsadmin
password: <password>
defaults:
  spaceAllocation: "false"
  encryption: "false"
  qosPolicy: standard
labels:
  store: san_store
  kubernetes-cluster: prod-cluster-1
region: us_east_1
storage:
  - labels:
      protection: gold
      creditpoints: "40000"
    zone: us_east_1a
    defaults:
      spaceAllocation: "true"
      encryption: "true"
      adaptiveQosPolicy: adaptive-extreme
  - labels:
      protection: silver
      creditpoints: "20000"
    zone: us_east_1b
    defaults:
      spaceAllocation: "false"
      encryption: "true"
      qosPolicy: premium
  - labels:
      protection: bronze
      creditpoints: "5000"
    zone: us_east_1c
    defaults:
      spaceAllocation: "true"
      encryption: "false"
```

ONTAP SAN 이코노미 예

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
username: vsadmin
password: <password>
defaults:
  spaceAllocation: "false"
  encryption: "false"
labels:
  store: san_economy_store
region: us_east_1
storage:
  - labels:
      app: oracledb
      cost: "30"
    zone: us_east_1a
    defaults:
      spaceAllocation: "true"
      encryption: "true"
  - labels:
      app: postgresdb
      cost: "20"
    zone: us_east_1b
    defaults:
      spaceAllocation: "false"
      encryption: "true"
  - labels:
      app: mysqldb
      cost: "10"
    zone: us_east_1c
    defaults:
      spaceAllocation: "true"
      encryption: "false"
  - labels:
      department: legal
      creditpoints: "5000"
```

```
    zone: us_east_1c
    defaults:
      spaceAllocation: "true"
      encryption: "false"
```

NVMe/TCP 예

```
---
version: 1
storageDriverName: ontap-san
sanType: nvme
managementLIF: 10.0.0.1
svm: nvme_svm
username: vsadmin
password: <password>
useREST: true
defaults:
  spaceAllocation: "false"
  encryption: "true"
storage:
  - labels:
      app: testApp
      cost: "20"
    defaults:
      spaceAllocation: "false"
      encryption: "false"
```

백엔드를 **StorageClasses**에 매핑합니다

다음 StorageClass 정의는 가상 풀이 있는 백엔드의 예을 참조합니다. `parameters.selector` 필드를 사용하여 각 StorageClass는 볼륨을 호스팅하는 데 사용할 수 있는 가상 풀을 지정합니다. 볼륨은 선택된 가상 풀에 정의된 속성을 갖게 됩니다.

- `protection-gold` StorageClass는 `ontap-san` 백엔드의 첫 번째 가상 풀에 매핑됩니다. 이 풀만이 골드 레벨 보호를 제공합니다.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection=gold"
  fsType: "ext4"
```

- `protection-not-gold` StorageClass는 `ontap-san` 백엔드의 두 번째 및 세 번째 가상 풀에 매핑됩니다. 이 두 풀만이 골드 수준 외에 다른 보호 수준을 제공합니다.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-not-gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection!=gold"
  fsType: "ext4"
```

- `app-mysqldb` StorageClass는 `ontap-san-economy` 백엔드의 세 번째 가상 풀에 매핑됩니다. 이 풀은 mysqldb 유형 애플리케이션에 대한 스토리지 풀 구성을 제공하는 유일한 풀입니다.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb
provisioner: csi.trident.netapp.io
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"
```

- `protection-silver-creditpoints-20k` StorageClass는 `ontap-san` 백엔드의 두 번째 가상 풀에 매핑됩니다. 이 풀은 실버 등급 보호와 20000 크레딧 포인트를 제공하는 유일한 풀입니다.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-silver-creditpoints-20k
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection=silver; creditpoints=20000"
  fsType: "ext4"
```

- `creditpoints-5k` StorageClass는 `ontap-san` 백엔드의 세 번째 가상 풀과 `ontap-san-economy` 백엔드의 네 번째 가상 풀에 매핑됩니다. 5000 크레딧 포인트를 제공하는 풀은 이 두 가지뿐입니다.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: creditpoints-5k
provisioner: csi.trident.netapp.io
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"
```

- `my-test-app-sc` StorageClass는 `testAPP` 드라이버의 `ontap-san` 가상 풀에 `sanType: nvme`로 매핑됩니다. 이것이 `testApp`을(를) 제공하는 유일한 풀입니다.

```
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: my-test-app-sc
provisioner: csi.trident.netapp.io
parameters:
  selector: "app=testApp"
  fsType: "ext4"
```

Trident는 어떤 가상 풀이 선택될지 결정하고 스토리지 요구사항이 충족되도록 보장합니다.