ONTAP NAS 드라이버

Trident

NetApp
July 01, 2026

목차

ONTAP NAS 드라이버

ONTAP NAS 드라이버 개요

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

ONTAP NAS 드라이버 세부 정보

Trident는 ONTAP 클러스터와 통신하기 위해 다음과 같은 NAS 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-nas`	NFS SMB	파일 시스템	RWO, ROX, RWX, RWOP	"", `nfs`, `smb`
`ontap-nas-economy`	NFS SMB	파일 시스템	RWO, ROX, RWX, RWOP	"", `nfs`, `smb`
`ontap-nas-flexgroup`	NFS SMB	파일 시스템	RWO, ROX, RWX, RWOP	"", `nfs`, `smb`

- `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.

ONTAP NAS 드라이버를 사용하여 백엔드를 구성할 준비를 하십시오

ONTAP NAS 드라이버를 사용하여 ONTAP 백엔드를 구성하기 위한 요구 사항, 인증 옵션 및 엑스포트 정책을 이해하십시오. 25.10 릴리스부터 NetApp Trident는 "NetApp AFX 스토리지 시스템"을(를) 지원합니다. NetApp AFX 스토리지 시스템은 스토리지 계층 구현에서 다른 ONTAP 시스템(ASA, AFF, FAS)과 다릅니다. Trident 백엔드 구성에서 시스템이 AFX인지 여부를 지정할 필요가 없습니다. `ontap-nas`을(를) `storageDriverName`(으)로 선택하면 Trident가 AFX 시스템을 자동으로 감지합니다.

AFX 시스템에서는 `ontap-nas` 드라이버(NFS 프로토콜 사용)만 지원되며 SMB 프로토콜은 지원되지 않습니다.

요구 사항

- 모든 ONTAP 백엔드의 경우 Trident를 사용하려면 SVM에 하나 이상의 애그리게이트를 할당해야 합니다.
- 여러 드라이버를 실행하고, 각 드라이버를 가리키는 스토리지 클래스를 생성할 수 있습니다. 예를 들어, `ontap-nas` 드라이버를 사용하는 Gold 클래스와 `ontap-nas-economy` 드라이버를 사용하는 Bronze 클래스를 구성할 수 있습니다.
- 모든 Kubernetes 워커 노드에는 적절한 NFS 도구가 설치되어 있어야 합니다. 자세한 내용은 "여기"을(를) 참조하십시오.
- Trident는 Windows 노드에서 실행되는 Pod에 마운트된 SMB 볼륨만 지원합니다. 자세한 내용은 SMB 볼륨 프로비저닝 준비를 참조하십시오.

ONTAP 백엔드를 인증합니다

Trident는 ONTAP 백엔드를 인증하는 두 가지 모드를 제공합니다.

- 자격 증명 기반: 이 모드는 ONTAP 백엔드에 대한 충분한 권한이 필요합니다. ONTAP 버전과의 최대 호환성을 보장하기 위해 `admin` 또는 `vsadmin`와 같이 미리 정의된 보안 로그인 역할과 연결된 계정을 사용하는 것이 좋습니다.
- 인증서 기반: 이 모드에서는 Trident가 ONTAP 클러스터와 통신하기 위해 백엔드에 인증서가 설치되어 있어야 합니다. 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-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
credentials:
  name: secret-backend-creds
```

JSON

```json
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "credentials": {
        "name": "secret-backend-creds"
    }
}
```

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

인증서 기반 인증 활성화

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=vsadmin"
```

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
```

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

```
security login create -user-or-group-name vsadmin -application ontapi
-authentication-method cert -vserver <vserver-name>
security login create -user-or-group-name vsadmin -application http
-authentication-method cert -vserver <vserver-name>
```

5. 생성된 인증서를 사용하여 인증을 테스트하십시오. <ONTAP Management LIF> 및 <vserver name>를 Management LIF IP 및 SVM 이름으로 바꾸십시오. LIF의 서비스 정책이 `default-data-management`로 설정되어 있는지 확인해야 합니다.

```
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-updated.json
{
"version": 1,
"storageDriverName": "ontap-nas",
"backendName": "NasBackend",
"managementLIF": "1.2.3.4",
"dataLIF": "1.2.3.8",
"svm": "vserver_test",
"clientCertificate": "Faaaakkkkeeee...Vaaalllluuuueeee",
"clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",
"storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident
+------------+----------------+--------------------------------------
+--------+---------+
|    NAME    | STORAGE DRIVER |                 UUID                 |
STATE  | VOLUMES |
+------------+----------------+--------------------------------------
+--------+---------+
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |       9 |
+------------+----------------+--------------------------------------
+--------+---------+
```

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 update backend`을(를) 실행합니다.

```
cat cert-backend-updated.json
```

```
{
"version": 1,
"storageDriverName": "ontap-nas",
"backendName": "NasBackend",
"managementLIF": "1.2.3.4",
"dataLIF": "1.2.3.8",
"svm": "vserver_test",
"username": "vsadmin",
"password": "password",
"storagePrefix": "myPrefix_"
}
```

```
#Update backend with tridentctl
tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident
+------------+----------------+--------------------------------------
+--------+---------+
|    NAME    | STORAGE DRIVER |                 UUID                 |
STATE   | VOLUMES |
+------------+----------------+--------------------------------------
+--------+---------+
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
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"

NFS 엑스포트 정책 관리

Trident는 NFS 엑스포트 정책을 사용하여 프로비저닝하는 볼륨에 대한 액세스를 제어합니다.

Trident는 엑스포트 정책 작업 시 두 가지 옵션을 제공합니다.

- Trident는 엑스포트 정책을 동적으로 관리할 수 있습니다. 이 운영 모드에서 스토리지 관리자는 허용 가능한 IP 주소를 나타내는 CIDR 블록 목록을 지정합니다. Trident는 게시 시점에 이러한 범위에 속하는 해당 노드 IP를 엑스포트 정책에 자동으로 추가합니다. 또는 CIDR이 지정되지 않은 경우, 볼륨이 게시될 노드에서 발견된 모든 글로벌 범위 유니캐스트 IP가 엑스포트 정책에 추가됩니다.
- 스토리지 관리자는 엑스포트 정책을 생성하고 규칙을 수동으로 추가할 수 있습니다. Trident는 구성 파일에 다른 엑스포트 정책 이름이 지정되지 않은 경우 기본 엑스포트 정책을 사용합니다.

엑스포트 정책을 동적으로 관리합니다

Trident는 ONTAP 백엔드에 대한 엑스포트 규칙을 동적으로 관리할 수 있는 기능을 제공합니다. 이를 통해 스토리지 관리자는 명시적인 규칙을 수동으로 정의하는 대신 워커 노드 IP에 대해 허용 가능한 주소 공간을 지정할 수 있습니다. 이는 엑스포트 규칙 관리를 크게 간소화하며, 엑스포트 규칙을 수정할 때 더 이상 스토리지 클러스터에서 수동으로 개입할 필요가 없습니다. 또한, 이 기능을 통해 볼륨을 마운트하고 지정된 IP 범위 내에 있는 워커 노드만 스토리지 클러스터에 액세스할 수 있도록 제한하여 세밀하고 자동화된 관리를 지원합니다.

> 동적 엑스포트 규칙을 사용할 때는 네트워크 주소 변환(NAT)을 사용하지 마십시오. NAT를 사용하면 스토리지 컨트롤러가 실제 IP 주소가 아닌 프런트엔드 NAT 주소를 인식하게 되므로 엑스포트 규칙에서 일치하는 항목이 없으면 액세스가 거부됩니다.

예

반드시 사용해야 하는 구성 옵션이 두 가지 있습니다. 다음은 백엔드 정의 예시입니다.

```
---
version: 1
storageDriverName: ontap-nas-economy
backendName: ontap_nas_auto_export
managementLIF: 192.168.0.135
svm: svm1
username: vsadmin
password: password
autoExportCIDRs:
  - 192.168.0.0/24
autoExportPolicy: true
```

> 이 기능을 사용할 때는 SVM의 루트 접합부에 노드 CIDR 블록을 허용하는 엑스포트 규칙(예: 기본 엑스포트 정책)이 포함된 엑스포트 정책이 미리 생성되어 있는지 확인해야 합니다. 항상 NetApp 권장 모범 사례에 따라 Trident 전용 SVM을 사용하십시오.

다음은 위의 예를 사용하여 이 기능이 작동하는 방식에 대한 설명입니다.

- `autoExportPolicy`이(가) `true`(으)로 설정되어 있습니다. 이는 Trident가 `svm1` SVM에 대해 이 백엔드로 프로비저닝된 각 볼륨에 대한 엑스포트 정책을 생성하고 `autoexportCIDRs` 주소 블록을 사용하여 규칙 추가 및 삭제를 처리함을 나타냅니다. 볼륨이 노드에 연결될 때까지 해당 볼륨은 원치 않는 액세스를 방지하기 위해 규칙이 없는 빈 엑스포트 정책을 사용합니다. 볼륨이 노드에 게시되면 Trident는 지정된 CIDR 블록 내의 노드 IP를 포함하는 기본 qtree와 동일한 이름의 엑스포트 정책을 생성합니다. 이러한 IP는 상위 FlexVol 볼륨에서 사용하는 엑스포트 정책에도 추가됩니다.
  - 예를 들면 다음과 같습니다.
    - 백엔드 UUID 403b5326-8482-40db-96d0-d83fb3f4daec
    - `autoExportPolicy` 로 설정 `true`
    - 스토리지 접두사 `trident`
    - PVC UUID a79bcf5f-7b6d-4a40-9876-e2551f159c1c
    - trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c라는 이름의 qtree는 FlexVol에 대한 엑스포트 규칙 `trident-403b5326-8482-40db96d0-d83fb3f4daec`, qtree에 대한 엑스포트 규칙 `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c`, 그리고 SVM에 빈 엑스포트 규칙 `trident_empty`을 생성합니다. FlexVol 엑스포트 규칙의 규칙은 qtree 엑스포트 규칙에 포함된 모든 규칙의 상위 집합입니다. 빈 엑스포트 규칙은 연결되지 않은 볼륨에서 재사용됩니다.
- `autoExportCIDRs`에는 주소 블록 목록이 포함되어 있습니다. 이 필드는 선택 사항이며 기본값은 ["0.0.0.0/0", "::/0"]입니다. 정의되지 않은 경우 Trident는 게시와 함께 작업자 노드에서 발견된 모든 전역 범위 유니캐스트 주소를 추가합니다.

이 예에서는 `192.168.0.0/24` 주소 공간이 제공됩니다. 이는 게시와 함께 이 주소 범위 내에 속하는 Kubernetes 노드 IP가 Trident가 생성하는 엑스포트 정책에 추가됨을 나타냅니다. Trident가 실행 중인 노드를 등록할 때 해당 노드의 IP 주소를 검색하고 `autoExportCIDRs`에 제공된 주소 블록과 비교합니다. 게시 시점에 IP를 필터링한 후 Trident는 게시 대상 노드의 클라이언트 IP에 대한 엑스포트 정책 규칙을 생성합니다.

> `autoExportPolicy`및 `autoExportCIDRs`를 생성한 후 백엔드에 대해 업데이트할 수 있습니다. 자동으로 관리되는 백엔드에 대해 새 `CIDR`을 추가하거나 기존 `CIDR`을 삭제할 수 있습니다. 기존 연결이 끊어지지 않도록 `CIDR`을 삭제할 때 주의하십시오. 또한 백엔드에 대해 `autoExportPolicy`를 비활성화하고 수동으로 생성된 엑스포트 정책으로 대체하도록 선택할 수 있습니다. 이렇게 하려면 백엔드 구성에서 `exportPolicy` 매개 변수를 설정해야 합니다.

Trident가 백엔드를 생성하거나 업데이트한 후 `tridentctl` 또는 해당 `tridentbackend` CRD를 사용하여 백엔드를 확인할 수 있습니다.

```
./tridentctl get backends ontap_nas_auto_export -n trident -o yaml
items:
- backendUUID: 403b5326-8482-40db-96d0-d83fb3f4daec
  config:
    aggregate: ""
    autoExportCIDRs:
    - 192.168.0.0/24
    autoExportPolicy: true
    backendName: ontap_nas_auto_export
    chapInitiatorSecret: ""
    chapTargetInitiatorSecret: ""
    chapTargetUsername: ""
    chapUsername: ""
    dataLIF: 192.168.0.135
    debug: false
    debugTraceFlags: null
    defaults:
      encryption: "false"
      exportPolicy: <automatic>
      fileSystemType: ext4
```

노드가 제거되면 Trident는 모든 엑스포트 정책을 확인하여 해당 노드에 해당하는 액세스 규칙을 제거합니다. 관리형 백엔드의 엑스포트 정책에서 이 노드 IP를 제거함으로써 Trident는 클러스터의 새 노드에서 이 IP가 재사용되지 않는 한 무단 마운트를 방지합니다.

기존 백엔드의 경우 `tridentctl update backend`로 백엔드를 업데이트하면 Trident에서 엑스포트 정책을 자동으로 관리합니다. 이렇게 하면 필요할 때 백엔드의 UUID와 qtree 이름을 따서 명명된 두 개의 새 엑스포트 정책이 생성됩니다. 백엔드에 있는 볼륨은 마운트 해제 후 다시 마운트되면 새로 생성된 엑스포트 정책을 사용합니다.

> ⓘ 자동 관리되는 엑스포트 규칙이 있는 백엔드를 삭제하면 동적으로 생성된 엑스포트 규칙도 삭제됩니다. 백엔드를 다시 생성하면 새 백엔드로 간주되어 새 엑스포트 규칙이 생성됩니다.

실행 중인 노드의 IP 주소가 업데이트되면 해당 노드에서 Trident Pod를 재시작해야 합니다. 그러면 Trident는 관리하는 백엔드에 대한 엑스포트 정책을 업데이트하여 이 IP 변경 사항을 반영합니다.

SMB 볼륨 프로비저닝 준비

약간의 추가 준비 작업을 거치면 `ontap-nas` 드라이버를 사용하여 SMB 볼륨을 프로비저닝할 수 있습니다.

> ⚠ ONTAP 온프레미스 클러스터용 `ontap-nas-economy` SMB 볼륨을 생성하려면 SVM에서 NFS 및 SMB/CIFS 프로토콜을 모두 구성해야 합니다. 이러한 프로토콜 중 하나라도 구성하지 않으면 SMB 볼륨 생성이 실패합니다.

> ⓘ `autoExportPolicy`는 SMB 볼륨에서 지원되지 않습니다.

시작하기 전에

SMB 볼륨을 프로비저닝하기 전에 다음 사항을 충족해야 합니다.

- Linux 컨트롤러 노드와 Windows Server 2022를 실행하는 하나 이상의 Windows 워커 노드로 구성된 Kubernetes 클러스터입니다. Trident는 Windows 노드에서 실행되는 Pod에 마운트된 SMB 볼륨만 지원합니다.
- Active Directory 자격 증명이 포함된 Trident 비밀 키가 하나 이상 필요합니다. 비밀 키를 생성하려면 `smbcreds`:

```
kubectl create secret generic smbcreds --from-literal username=user
--from-literal password='password'
```

- Windows 서비스로 구성된 CSI 프록시입니다. `csi-proxy`를 구성하려면 Windows에서 실행되는 Kubernetes 노드에 대한 "GitHub: CSI 프록시" 또는 "GitHub: Windows용 CSI 프록시"를 참조하십시오.

단계

1. 온프레미스 ONTAP의 경우 선택적으로 SMB 공유를 생성하거나 Trident가 대신 생성해 줄 수 있습니다.

   Amazon FSx for ONTAP에는 SMB 공유가 필요합니다.

   SMB 관리자 공유는 "Microsoft Management Console" 공유 폴더 스냅인을 사용하거나 ONTAP CLI를 사용하는 두 가지 방법으로 생성할 수 있습니다. ONTAP CLI를 사용하여 SMB 공유를 생성하려면 다음을 수행합니다.

   a. 필요한 경우 공유에 대한 디렉터리 경로 구조를 생성하십시오.

      `vserver cifs share create` 명령은 공유 생성 시 -path 옵션에 지정된 경로를 확인합니다. 지정된 경로가 존재하지 않으면 명령이 실패합니다.

   b. 지정된 SVM과 연결된 SMB 공유를 생성합니다.

```
vserver cifs share create -vserver vserver_name -share-name
share_name -path path [-share-properties share_properties,...]
[other_attributes] [-comment text]
```

   c. 공유가 생성되었는지 확인합니다.

```
vserver cifs share show -share-name share_name
```

      자세한 내용은 "SMB 공유 생성"를 참조하십시오.

2. 백엔드를 생성할 때 SMB 볼륨을 지정하려면 다음을 구성해야 합니다. 모든 FSx for ONTAP 백엔드 구성 옵션에 대한 자세한 내용은 "FSx for ONTAP 구성 옵션 및 예"를 참조하십시오.

매개변수	설명	예
`smbShare`	다음 중 하나를 지정할 수 있습니다. Microsoft Management Console 또는 ONTAP CLI를 사용하여 생성한 SMB 공유의 이름, Trident가 SMB 공유를 생성할 수 있도록 허용하는 이름, 또는 볼륨에 대한 공통 공유 액세스를 방지하려면 매개 변수를 비워 둘 수 있습니다. 이 매개 변수는 온프레미스 ONTAP의 경우 선택 사항입니다. 이 매개 변수는 Amazon FSx for ONTAP 백엔드에 필요하며 비워 둘 수 없습니다.	`smb-share`
`nasType`	* `smb`로 설정해야 합니다.* null인 경우 기본값은 `nfs`입니다.	`smb`
`securityStyle`	새 볼륨에 대한 보안 스타일입니다. **SMB** 볼륨의 경우 **`ntfs`** 또는 **`mixed`**로 설정해야 합니다**.**	`ntfs` 또는 `mixed` SMB 볼륨의 경우
`unixPermissions`	새 볼륨 모드입니다. **SMB** 볼륨의 경우 비워 두어야 합니다**.**	""

보안 **SMB** 활성화

25.06 릴리스부터 NetApp Trident는 `ontap-nas` 및 `ontap-nas-economy` 백엔드를 사용하여 생성된 SMB 볼륨의 보안 프로비저닝을 지원합니다. 보안 SMB가 활성화되면 액세스 제어 목록(ACL)을 사용하여 Active Directory(AD) 사용자 및 사용자 그룹에 SMB 공유에 대한 제어된 액세스를 제공할 수 있습니다.

기억해야 할 사항

- `ontap-nas-economy` 볼륨 가져오기는 지원되지 않습니다.
- `ontap-nas-economy` 볼륨의 경우 읽기 전용 클론만 지원됩니다.
- Secure SMB가 활성화된 경우 Trident는 백엔드에 언급된 SMB 공유를 무시합니다.
- PVC 주석, 스토리지 클래스 주석 및 백엔드 필드를 업데이트해도 SMB 공유 ACL은 업데이트되지 않습니다.
- 클론 PVC의 주석에 지정된 SMB 공유 ACL은 소스 PVC의 ACL보다 우선합니다.
- 보안 SMB를 활성화할 때 유효한 AD 사용자를 제공해야 합니다. 유효하지 않은 사용자는 ACL에 추가되지 않습니다.
- 백엔드, 스토리지 클래스 및 PVC에 동일한 AD 사용자를 지정하고 각기 다른 권한을 부여하는 경우 권한 우선순위는 PVC, 스토리지 클래스, 백엔드 순이 됩니다.
- 보안 SMB는 `ontap-nas` 관리형 볼륨 가져오기에 대해 지원되며, 관리되지 않는 볼륨 가져오기에는 적용되지 않습니다.

단계

1. 다음 예시와 같이 TridentBackendConfig에서 adAdminUser를 지정하십시오:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.193.176.x
  svm: svm0
  useREST: true
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

2. 스토리지 클래스에 주석을 추가합니다.

`trident.netapp.io/smbShareAdUser` 어노테이션을 스토리지 클래스에 추가하여 안전한 SMB를 확실하게 활성화하십시오. 어노테이션 `trident.netapp.io/smbShareAdUser`에 지정된 사용자 값은 `smbcreds` 시크릿에 지정된 사용자 이름과 동일해야 합니다. `smbShareAdUserPermission`에 대해 다음 중 하나를 선택할 수 있습니다: `full_control`, `change` 또는 `read`. 기본 권한은 `full_control`입니다.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADuser
parameters:
  backendType: ontap-nas
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

1. PVC를 생성합니다.

다음 예제는 PVC를 생성합니다.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc4
  namespace: trident
  annotations:
    trident.netapp.io/snapshotDirectory: "true"
    trident.netapp.io/smbShareAccessControl: |
      read:
        - tridentADtest
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-smb-sc
```

ONTAP NAS 구성 옵션 및 예

Trident 설치 환경에서 ONTAP NAS 드라이버를 생성하고 사용하는 방법을 알아보세요. 이 섹션에서는 백엔드 구성 예제와 백엔드를 StorageClasses에 매핑하는 방법에 대한 세부 정보를 제공합니다. 25.10 릴리스부터 NetApp Trident는 "NetApp AFX 스토리지 시스템"을(를) 지원합니다. NetApp AFX 스토리지 시스템은 스토리지 계층 구현에서 다른 ONTAP 기반 시스템(ASA, AFF, FAS)과 다릅니다.

ⓘ `ontap-nas` 드라이버(NFS 프로토콜 사용)만 NetApp AFX 시스템에서 지원되며 SMB 프로토콜은 지원되지 않습니다.

백엔드 **configuration** 옵션

Trident 백엔드 구성에서 시스템이 NetApp AFX 스토리지 시스템임을 지정할 필요가 없습니다. `ontap-nas`을(를) `storageDriverName`(으)로 선택하면 Trident가 AFX 스토리지 시스템을 자동으로 감지합니다. 일부 백엔드 구성 매개변수는 AFX 스토리지 시스템에는 적용되지 않습니다.

다음 표는 백엔드 구성 옵션을 보여줍니다.

매개변수	설명	기본값
`version`		항상 1

매개변수	설명	기본값
`storageDriverName`	스토리지 드라이버의 이름 NetApp AFX 시스템의 경우 `ontap-nas`만 지원됩니다.	`ontap-nas`, `ontap-nas-economy` 또는 `ontap-nas-flexgroup`
`backendName`	사용자 지정 이름 또는 스토리지 백엔드	드라이버 이름 + "_" + dataLIF
`managementLIF`	클러스터 또는 SVM 관리 LIF의 IP 주소입니다. 정규화된 도메인 이름(FQDN)도 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.	"10.0.0.1", "[2001:1234:abcd::fefe]"
`dataLIF`	프로토콜 LIF의 IP 주소입니다. NetApp에서는 `dataLIF`을 지정하는 것을 권장합니다. 지정하지 않으면 Trident는 SVM에서 dataLIF를 가져옵니다. NFS 마운트 작업에 사용할 정규화된 도메인 이름(FQDN)을 지정하여 여러 dataLIF에 걸쳐 로드 밸런싱을 수행하는 라운드 로빈 DNS를 구성할 수 있습니다. 초기 설정 후 변경할 수 있습니다. 다음을 참조하십시오. . 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. **MetroCluster**의 경우 생략합니다. MetroCluster 예시를 참조하십시오.	지정된 주소 또는 지정되지 않은 경우 SVM에서 파생(권장하지 않음)
`svm`	사용할 스토리지 가상 머신 **MetroCluster**의 경우 생략 MetroCluster 예시를 참조하십시오.	SVM `managementLIF`이 지정된 경우 파생됩니다
`autoExportPolicy`	자동 엑스포트 정책 생성 및 업데이트를 활성화합니다[Boolean]. `autoExportPolicy` 및 `autoExportCIDRs` 옵션을 사용하면 Trident가 내보내기 정책을 자동으로 관리할 수 있습니다.	거짓
`autoExportCIDRs`	`autoExportPolicy`이 활성화된 경우 Kubernetes 노드 IP를 필터링하는 데 사용할 CIDR 목록입니다. `autoExportPolicy` 및 `autoExportCIDRs` 옵션을 사용하면 Trident가 내보내기 정책을 자동으로 관리할 수 있습니다.	["0.0.0.0/0", "::/0"]`
`labels`	볼륨에 적용할 임의의 JSON 형식 레이블 세트	""
`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	""

매개변수	설명	기본값
`username`	클러스터/SVM에 연결하는 데 사용할 사용자 이름입니다. 자격 증명 기반 인증에 사용됩니다. Active Directory 인증에 대한 자세한 내용은 "Active Directory 자격 증명을 사용하여 Trident를 백엔드 SVM에 인증합니다"을(를) 참조하십시오.	
`password`	클러스터/SVM에 연결하는 데 사용되는 암호입니다. 자격 증명 기반 인증에 사용됩니다. Active Directory 인증에 대한 자세한 내용은 "Active Directory 자격 증명을 사용하여 Trident를 백엔드 SVM에 인증합니다"을(를) 참조하십시오.	
`storagePrefix`	SVM에서 새 볼륨을 프로비저닝할 때 사용되는 접두사입니다. 설정 후에는 업데이트할 수 없습니다 ontap-nas-economy를 사용하고 storagePrefix가 24자 이상인 경우, qtree에는 스토리지 접두사가 포함되지 않지만 볼륨 이름에는 포함됩니다.	"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. **AFX** 스토리지 시스템에는 지정하지 마십시오.	""
`limitAggregateUsage`	사용량이 이 비율을 초과하면 프로비저닝이 실패합니다. **Amazon FSx for ONTAP**에는 적용되지 않습니다. **AFX** 스토리지 시스템에는 지정하지 마십시오.	"" (기본적으로 적용되지 않음)

매개변수	설명	기본값
flexgroupAggregateList	프로비저닝을 위한 애그리게이트 목록(선택 사항, 설정된 경우 SVM에 할당되어야 함). SVM에 할당된 모든 애그리게이트는 FlexGroup 볼륨을 프로비저닝하는 데 사용됩니다. **ontap-nas-flexgroup** 스토리지 드라이버에서 지원됩니다. ⓘ SVM에서 애그리게이트 목록이 업데이트되면 Trident Controller를 재시작하지 않고도 SVM을 폴링하여 Trident의 목록이 자동으로 업데이트됩니다. Trident에서 볼륨을 프로비저닝하도록 특정 애그리게이트 목록을 구성한 경우, 해당 애그리게이트 목록의 이름이 변경되거나 SVM에서 이동되면 SVM 애그리게이트를 폴링하는 동안 Trident의 백엔드 상태가 실패로 전환됩니다. 백엔드를 다시 온라인 상태로 전환하려면 애그리게이트 목록을 SVM에 있는 다른 목록으로 변경하거나 완전히 제거해야 합니다.	""
`limitVolumeSize`	요청된 볼륨 크기가 이 값을 초과하면 프로비저닝이 실패합니다.	"" (기본적으로 적용되지 않음)
`debugTraceFlags`	문제 해결 시 사용할 디버그 플래그입니다. 예, {"api":false, "method":true} 문제 해결 중이거나 자세한 로그 덤프가 필요한 경우가 아니면 `debugTraceFlags` 사용하지 마십시오.	null
`nasType`	NFS 또는 SMB 볼륨 생성을 구성합니다. 옵션은 `nfs`, `smb` 또는 null입니다. null로 설정하면 기본적으로 NFS 볼륨이 사용됩니다. **AFX** 스토리지 시스템의 경우 지정된 경우 항상 `**nfs**`로 설정하십시오.	`nfs`
`nfsMountOptions`	쉼표로 구분된 NFS 마운트 옵션 목록입니다. Kubernetes 영구 볼륨의 마운트 옵션은 일반적으로 스토리지 클래스에 지정되지만, 스토리지 클래스에 마운트 옵션이 지정되지 않은 경우 Trident는 스토리지 백엔드의 구성 파일에 지정된 마운트 옵션을 사용합니다. 스토리지 클래스 또는 구성 파일에 마운트 옵션이 지정되지 않은 경우 Trident는 연결된 영구 볼륨에 마운트 옵션을 설정하지 않습니다.	""
`qtreesPerFlexvol`	FlexVol당 최대 Qtree 수는 [50, 300] 범위 내에 있어야 합니다	"200"
`smbShare`	다음 중 하나를 지정할 수 있습니다. Microsoft Management Console 또는 ONTAP CLI를 사용하여 생성한 SMB 공유의 이름, Trident가 SMB 공유를 생성할 수 있도록 허용하는 이름, 또는 볼륨에 대한 공통 공유 액세스를 방지하려면 매개 변수를 비워 둘 수 있습니다. 이 매개 변수는 온프레미스 ONTAP의 경우 선택 사항입니다. 이 매개 변수는 Amazon FSx for ONTAP 백엔드에 필요하며 비워 둘 수 없습니다.	`smb-share`

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. **AFX** 스토리지 시스템의 경우 지정된 경우 항상 **`true`**로 설정하십시오.	ONTAP 9.15.1 이상의 경우 true, 그렇지 않은 경우 false.
limitVolumePoolSize	ontap-nas-economy 백엔드에서 Qtree를 사용할 때 요청할 수 있는 최대 FlexVol 크기입니다.	"" (기본적으로 적용되지 않음)
denyNewVolumePools	`ontap-nas-economy`백엔드가 Qtree를 포함할 새 FlexVol 볼륨을 생성하지 못하도록 제한합니다. 기존 Flexvol만 새 PV 프로비저닝에 사용됩니다.	
adAdminUser	SMB 공유에 대한 전체 액세스 권한이 있는 Active Directory 관리자 사용자 또는 사용자 그룹입니다. 이 매개 변수를 사용하여 SMB 공유에 대한 전체 제어 권한이 있는 관리자 권한을 제공합니다.	

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	Qtree에 대한 공간 할당	"true"
spaceReserve	공간 예약 모드, "none"(씬) 또는 "volume"(씩)	"없음"
snapshotPolicy	사용할 스냅샷 정책	"없음"
qosPolicy	생성된 볼륨에 할당할 QoS 정책 그룹입니다. 스토리지 풀/백엔드당 qosPolicy 또는 adaptiveQosPolicy 중 하나를 선택하십시오	""
adaptiveQosPolicy	생성된 볼륨에 할당할 적응형 QoS 정책 그룹입니다. 스토리지 풀/백엔드별로 qosPolicy 또는 adaptiveQosPolicy 중 하나를 선택하십시오. ontap-nas-economy에서는 지원되지 않습니다.	""
snapshotReserve	스냅샷용으로 예약된 볼륨의 비율	`snapshotPolicy`이(가) "none"이면 "0", 그렇지 않으면 ""
splitOnClone	생성 시 상위 항목에서 클론 분할	"false"

매개변수	설명	기본값
`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"
`tieringPolicy`	계층화 정책에서 "none"을 사용합니다.	
`unixPermissions`	새 볼륨용 모드	NFS 볼륨의 경우 "777", SMB 볼륨의 경우 비어 있음(해당 없음)
`snapshotDir`	`.snapshot` 디렉터리에 대한 액세스를 제어합니다	`true`, `false` (명시적으로 설정).
`exportPolicy`	사용할 엑스포트 정책	"default"
`securityStyle`	새 볼륨에 대한 보안 스타일입니다. NFS는 `mixed` 및 `unix` 보안 스타일을 지원합니다. SMB는 `mixed` 및 `ntfs` 보안 스타일을 지원합니다.	NFS 기본값은 `unix`입니다. SMB 기본값은 `ntfs`입니다.
`nameTemplate`	사용자 지정 볼륨 이름을 생성하기 위한 템플릿입니다.	""

Trident에서 QoS 정책 그룹을 사용하려면 ONTAP 9.8 이상이 필요합니다. 공유하지 않는 QoS 정책 그룹을 사용하고 각 구성 요소에 개별적으로 정책 그룹을 적용해야 합니다. 공유 QoS 정책 그룹은 모든 워크로드의 총 처리량에 대한 상한선을 적용합니다.

볼륨 프로비저닝 예

다음은 기본값이 정의된 예입니다.

```
---
version: 1
storageDriverName: ontap-nas
backendName: customBackendName
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
labels:
  k8scluster: dev1
  backend: dev1-nasbackend
svm: trident_svm
username: cluster-admin
password: <password>
limitAggregateUsage: 80%
limitVolumeSize: 50Gi
nfsMountOptions: nfsvers=4
debugTraceFlags:
  api: false
  method: true
defaults:
  spaceReserve: volume
  qosPolicy: premium
  exportPolicy: myk8scluster
  snapshotPolicy: default
  snapshotReserve: "10"
```

`ontap-nas` 및 `ontap-nas-flexgroups`의 경우, Trident는 이제 FlexVol이 snapshotReserve 비율과 PVC에 맞게 올바르게 크기가 지정되도록 새로운 계산 방식을 사용합니다. 사용자가 PVC를 요청하면, Trident는 새로운 계산을 사용하여 더 많은 공간을 가진 원래 FlexVol을 생성합니다. 이 계산은 사용자가 PVC에서 요청한 만큼의 쓰기 가능한 공간을 받을 수 있도록 하며, 요청한 것보다 적은 공간을 제공하지 않습니다. v21.07 이전에는 사용자가 PVC(예: 5GiB)를 요청하고 snapshotReserve를 50퍼센트로 설정하면, 쓰기 가능한 공간은 2.5GiB만 제공되었습니다. 이는 사용자가 요청한 것이 전체 볼륨이고 `snapshotReserve`가 그 전체의 비율이기 때문입니다. Trident 21.07부터는 사용자가 요청하는 것이 쓰기 가능한 공간이며, Trident는 `snapshotReserve` 숫자를 전체 볼륨의 비율로 정의합니다. 이 내용은 `ontap-nas-economy`에는 적용되지 않습니다. 다음 예제를 통해 이 동작 방식을 확인할 수 있습니다:

계산 방법은 다음과 같습니다.

```
Total volume size = <PVC requested size> / (1 - (<snapshotReserve
percentage> / 100))
```

snapshotReserve = 50%이고 PVC 요청 = 5GiB인 경우, 전체 볼륨 크기는 5/.5 = 10GiB이고 사용 가능한 크기는

5GiB로, 사용자가 PVC 요청에서 요청한 크기입니다. `volume show` 명령은 다음 예와 유사한 결과를 표시해야 합니다.

이전 설치의 기존 백엔드는 Trident를 업그레이드할 때 위에서 설명한 대로 볼륨을 프로비저닝합니다. 업그레이드 전에 생성한 볼륨의 경우 변경 사항이 적용되도록 크기를 조정해야 합니다. 예를 들어, `snapshotReserve=50`이전에 2GiB PVC로 설정된 볼륨은 1GiB의 쓰기 공간을 제공합니다. 예를 들어 볼륨 크기를 3GiB로 조정하면 애플리케이션은 6GiB 볼륨에서 3GiB의 쓰기 공간을 사용할 수 있습니다.

최소 구성 예

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

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

ONTAP NAS 이코노미 예

```
---
version: 1
storageDriverName: ontap-nas-economy
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

ONTAP NAS FlexGroup 예

```
---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
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 SVM을 지정하고 `dataLIF` 및 `svm` 매개 변수를 생략하십시오. 예를 들면 다음과 같습니다.

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

SMB 볼륨 예

```
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
nasType: smb
securityStyle: ntfs
unixPermissions: ""
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

인증서 기반 인증 예

이는 최소한의 백엔드 구성 예시입니다. `clientCertificate`, `clientPrivateKey` 및 `trustedCACertificate`(신뢰할 수 있는 CA를 사용하는 경우 선택 사항)는 `backend.json`에 입력되며 클라이언트 인증서, 개인 키 및 신뢰할 수 있는 CA 인증서의 base64 인코딩된 값을 각각 사용합니다.

```
---
version: 1
backendName: DefaultNASBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.15
svm: nfs_svm
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
storagePrefix: myPrefix_
```

자동 엑스포트 정책 예

이 예제는 Trident가 동적 내보내기 정책을 사용하여 내보내기 정책을 자동으로 생성하고 관리하도록 지시하는 방법을 보여줍니다. 이는 `ontap-nas-economy` 및 `ontap-nas-flexgroup` 드라이버에 대해 동일하게 작동합니다.

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
labels:
  k8scluster: test-cluster-east-1a
  backend: test1-nasbackend
autoExportPolicy: true
autoExportCIDRs:
- 10.0.0.0/24
username: admin
password: password
nfsMountOptions: nfsvers=4
```

IPv6 주소 예

이 예시는 IPv6 주소를 사용하는 `managementLIF` 방법을 보여줍니다.

```
---
version: 1
storageDriverName: ontap-nas
backendName: nas_ipv6_backend
managementLIF: "[5c5d:5edf:8f:7657:bef8:109b:1b41:d491]"
labels:
  k8scluster: test-cluster-east-1a
  backend: test1-ontap-ipv6
svm: nas_ipv6_svm
username: vsadmin
password: password
```

SMB 볼륨을 사용하는 **Amazon FSx for ONTAP** 예

`smbShare` 매개 변수는 SMB 볼륨을 사용하는 FSx for ONTAP에 필요합니다.

```
---
version: 1
backendName: SMBBackend
storageDriverName: ontap-nas
managementLIF: example.mgmt.fqdn.aws.com
nasType: smb
dataLIF: 10.0.0.15
svm: nfs_svm
smbShare: smb-share
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
storagePrefix: myPrefix_
```

nameTemplate을 사용한 백엔드 구성 예

```
---
version: 1
storageDriverName: ontap-nas
backendName: ontap-nas-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}}"
```

가상 풀이 있는 백엔드의 예

아래에 표시된 샘플 백엔드 정의 파일에서는 모든 스토리지 풀에 대해 `spaceReserve`없음, `spaceAllocation`false, `encryption`false와 같은 특정 기본값이 설정되어 있습니다. 가상 풀은 스토리지 섹션에서 정의됩니다.

Trident는 "설명" 필드에 프로비저닝 레이블을 설정합니다. 설명은 FlexVol의 경우 `ontap-nas` 또는 FlexGroup의 경우 `ontap-nas-flexgroup`에 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 NAS 예

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
svm: svm_nfs
username: admin
password: <password>
nfsMountOptions: nfsvers=4
defaults:
  spaceReserve: none
  encryption: "false"
  qosPolicy: standard
labels:
  store: nas_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
  - labels:
      app: msoffice
      cost: "100"
    zone: us_east_1a
    defaults:
      spaceReserve: volume
      encryption: "true"
      unixPermissions: "0755"
      adaptiveQosPolicy: adaptive-premium
  - labels:
      app: slack
      cost: "75"
    zone: us_east_1b
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0755"
  - labels:
      department: legal
      creditpoints: "5000"
    zone: us_east_1b
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0755"
  - labels:
```

```
      app: wordpress
      cost: "50"
    zone: us_east_1c
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0775"
  - labels:
      app: mysqldb
      cost: "25"
    zone: us_east_1d
    defaults:
      spaceReserve: volume
      encryption: "false"
      unixPermissions: "0775"
```

ONTAP NAS FlexGroup 예

```
---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: <password>
defaults:
  spaceReserve: none
  encryption: "false"
labels:
  store: flexgroup_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
  - labels:
      protection: gold
      creditpoints: "50000"
    zone: us_east_1a
    defaults:
      spaceReserve: volume
      encryption: "true"
      unixPermissions: "0755"
  - labels:
      protection: gold
      creditpoints: "30000"
    zone: us_east_1b
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0755"
  - labels:
      protection: silver
      creditpoints: "20000"
    zone: us_east_1c
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0775"
  - labels:
      protection: bronze
      creditpoints: "10000"
    zone: us_east_1d
```

```
    defaults:
      spaceReserve: volume
      encryption: "false"
      unixPermissions: "0775"
```

ONTAP NAS 이코노미 예

```
---
version: 1
storageDriverName: ontap-nas-economy
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: <password>
defaults:
  spaceReserve: none
  encryption: "false"
labels:
  store: nas_economy_store
region: us_east_1
storage:
  - labels:
      department: finance
      creditpoints: "6000"
    zone: us_east_1a
    defaults:
      spaceReserve: volume
      encryption: "true"
      unixPermissions: "0755"
  - labels:
      protection: bronze
      creditpoints: "5000"
    zone: us_east_1b
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0755"
  - labels:
      department: engineering
      creditpoints: "3000"
    zone: us_east_1c
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0775"
  - labels:
      department: humanresource
      creditpoints: "2000"
    zone: us_east_1d
    defaults:
```

```
      spaceReserve: volume
      encryption: "false"
      unixPermissions: "0775"
```

백엔드를 StorageClasses에 매핑합니다

다음 StorageClass 정의는 가상 풀이 있는 백엔드의 예를 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-nas-flexgroup` 백엔드의 첫 번째 및 두 번째 가상 풀에 매핑됩니다. 이 두 풀만 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-nas-flexgroup` 백엔드의 세 번째 및 네 번째 가상 풀에 매핑됩니다. 이 두 풀만이 골드 등급 이외의 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-nas` 백엔드의 네 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-nas-flexgroup` 백엔드의 세 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-nas` 백엔드의 세 번째 가상 풀과 `ontap-nas-economy` 백엔드의 두 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"
```

Trident는 어떤 가상 풀이 선택될지 결정하고 스토리지 요구사항이 충족되도록 보장합니다.

초기 구성 후 업데이트 `dataLIF`

초기 구성 후 다음 명령을 실행하여 업데이트된 dataLIF가 포함된 새 백엔드 JSON 파일을 제공함으로써 dataLIF를 변경할 수 있습니다.

```
tridentctl update backend <backend-name> -f <path-to-backend-json-file-
with-updated-dataLIF>
```

PVC가 하나 이상의 Pod에 연결된 경우, 새 dataLIF가 적용되려면 해당 Pod를 모두 종료한 다음 다시 시작해야 합니다.

보안 SMB 예

ontap-nas 드라이버를 사용한 백엔드 구성

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  svm: svm2
  nasType: smb
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

ontap-nas-economy 드라이버를 사용한 백엔드 구성

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas-economy
  managementLIF: 10.0.0.1
  svm: svm2
  nasType: smb
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

스토리지 풀을 사용한 백엔드 구성

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  svm: svm0
  useREST: false
  storage:
  - labels:
      app: msoffice
    defaults:
      adAdminUser: tridentADuser
  nasType: smb
  credentials:
    name: backend-tbc-ontap-invest-secret
```

ontap-nas 드라이버를 사용한 스토리지 클래스 예제

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADtest
parameters:
  backendType: ontap-nas
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

`annotations`을(를) 추가하여 보안 SMB를 활성화해야 합니다. 백엔드 또는 PVC에 설정된 구성과 관계없이 어노테이션이 없으면 보안 SMB가 작동하지 않습니다.

ontap-nas-economy 드라이버를 사용한 스토리지 클래스 예

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADuser3
parameters:
  backendType: ontap-nas-economy
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

단일 **AD** 사용자를 사용한 **PVC** 예

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc4
  namespace: trident
  annotations:
    trident.netapp.io/smbShareAccessControl: |
      change:
        - tridentADtest
      read:
        - tridentADuser
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-smb-sc
```

여러 **AD** 사용자를 포함하는 **PVC** 예

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-test-pvc
  annotations:
    trident.netapp.io/smbShareAccessControl: |
      full_control:
        - tridentTestuser
        - tridentuser
        - tridentTestuser1
        - tridentuser1
      change:
        - tridentADuser
        - tridentADuser1
        - tridentADuser4
        - tridentTestuser2
      read:
        - tridentTestuser2
        - tridentTestuser3
        - tridentADuser2
        - tridentADuser3
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
```