ONTAP NAS 드라이버

Trident

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/trident-2410/trident-use/ontap-nas.html on September 26, 2025. Always check docs.netapp.com for the latest.

목차

ONTAP NAS 드라이버 . . . 1
- ONTAP NAS 드라이버 개요 . . . 1
  - ONTAP NAS 드라이버 세부 정보입니다 . . . 1
  - 사용자 권한 . . . 1
- ONTAP NAS 드라이버를 사용하여 백엔드를 구성할 준비를 합니다 . . . 2
  - 요구 사항 . . . 2
  - ONTAP 백엔드를 인증합니다 . . . 2
  - NFS 엑스포트 정책을 관리합니다 . . . 7
  - SMB 볼륨 프로비저닝을 위한 준비 . . . 10
- ONTAP NAS 구성 옵션 및 예 . . . 12
  - 백엔드 구성 옵션 . . . 12
  - 볼륨 프로비저닝을 위한 백엔드 구성 옵션 . . . 15
  - 최소 구성의 예 . . . 18
  - 가상 풀의 백엔드 예 . . . 22
  - 백엔드를 StorageClasses에 매핑합니다 . . . 28
  - 초기 구성 후 업데이트 `dataLIF` . . . 29

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 정보입니다

Trident는 ONTAP 클러스터와 통신할 수 있도록 다음과 같은 NAS 스토리지 드라이버를 제공합니다. 지원되는 액세스 모드는 *ReadWriteOnce*(RWO), *ReadOnlyMany*(ROX), *ReadWriteMany*(rwx), *ReadWriteOncePod*(RWOP)입니다.

드라이버	프로토콜	볼륨 모드	액세스 모드가 지원됩니다	지원되는 파일 시스템
`ontap-nas`	NFS SMB를 참조하십시오	파일 시스템	RWO, ROX, rwx, RWOP	"", `nfs smb`
`ontap-nas-economy`	NFS SMB를 참조하십시오	파일 시스템	RWO, ROX, rwx, RWOP	"", `nfs smb`
`ontap-nas-flexgroup`	NFS SMB를 참조하십시오	파일 시스템	RWO, ROX, rwx, RWOP	"", `nfs smb`

- `ontap-san-economy`영구 볼륨 사용률 수가 보다 높을 것으로 예상되는 경우에만 "지원되는 ONTAP 볼륨 제한"사용합니다.
- `ontap-nas-economy`영구 볼륨 사용 횟수가 다음보다 크고 `ontap-san-economy` 드라이버를 사용할 수 없는 경우에만 "지원되는 ONTAP 볼륨 제한"사용합니다.
- 데이터 보호, 재해 복구 또는 이동성이 필요할 것으로 예상되는 경우에는 사용하지 마십시오 `ontap-nas-economy`.

사용자 권한

Trident는 ONTAP 또는 SVM 관리자로 실행해야 하며, 일반적으로 클러스터 사용자 `vsadmin` 또는 SVM 사용자 또는 같은 역할을 가진 다른 이름의 사용자를 사용할 `admin` 것입니다.

Amazon FSx for NetApp ONTAP 배포의 경우 Trident은 클러스터 사용자 또는 `vsadmin` SVM 사용자를 사용하여 ONTAP 또는 SVM 관리자로 실행하거나 `fsxadmin` 동일한 역할을 가진 다른 이름의 사용자를 실행해야 합니다. `fsxadmin`사용자는 클러스터 관리자를 제한적으로 대체합니다.

> `limitAggregateUsage`매개 변수를 사용하려면 클러스터 관리 권한이 필요합니다. Trident와 함께 Amazon FSx for NetApp ONTAP를 사용할 때 `limitAggregateUsage` 매개 변수는 및 `fsxadmin` 사용자 계정에서 작동하지 `vsadmin` 않습니다. 이 매개 변수를 지정하면 구성 작업이 실패합니다.

Trident 드라이버가 사용할 수 있는 더 제한적인 역할을 ONTAP 내에 만들 수 있지만 권장하지 않습니다. Trident의

대부분의 새로운 릴리즈에서는 추가 API를 호출하므로 업그레이드가 어렵고 오류가 발생하기 쉽습니다.

ONTAP NAS 드라이버를 사용하여 백엔드를 구성할 준비를 합니다

ONTAP NAS 드라이버를 사용하여 ONTAP 백엔드를 구성하기 위한 요구 사항, 인증 옵션 및 엑스포트 정책을 이해합니다.

요구 사항

- 모든 ONTAP 백엔드에 대해 Trident에는 SVM에 할당된 애그리게이트가 하나 이상 필요합니다.
- 둘 이상의 드라이버를 실행하고 둘 중 하나를 가리키는 스토리지 클래스를 생성할 수 있습니다. 예를 들어 드라이버를 사용하는 Gold 클래스와 해당 드라이버를 사용하는 Bronze `ontap-nas-economy` 클래스를 구성할 수 `ontap-nas` 있습니다.
- 모든 Kubernetes 작업자 노드에 적절한 NFS 툴이 설치되어 있어야 합니다. "여기"자세한 내용은 을 참조하십시오.
- Trident는 Windows 노드에서만 실행되는 Pod에 마운트된 SMB 볼륨을 지원합니다. 자세한 내용은 을 SMB 볼륨 프로비저닝을 위한 준비 참조하십시오.

ONTAP 백엔드를 인증합니다

Trident는 ONTAP 백엔드를 인증하는 두 가지 모드를 제공합니다.

- 자격 증명 기반: 이 모드에서는 ONTAP 백엔드에 대한 충분한 권한이 필요합니다. ONTAP 버전과의 호환성을 최대화하려면 또는 과 `vsadmin` 같이 미리 정의된 보안 로그인 역할과 연결된 계정을 사용하는 것이 좋습니다 `admin`.
- 인증서 기반: 이 모드에서는 Trident가 ONTAP 클러스터와 통신하기 위해 백엔드에 인증서가 설치되어 있어야 합니다. 이 경우 백엔드 정의에는 클라이언트 인증서, 키 및 사용할 경우 신뢰할 수 있는 CA 인증서의 Base64로 인코딩된 값이 있어야 합니다(권장).

자격 증명 기반 방법과 인증서 기반 방법 간에 이동하기 위해 기존 백엔드를 업데이트할 수 있습니다. 그러나 한 번에 하나의 인증 방법만 지원됩니다. 다른 인증 방법으로 전환하려면 백엔드 구성에서 기존 방법을 제거해야 합니다.

> 자격 증명과 인증서 * 를 모두 제공하려고 하면 구성 파일에 둘 이상의 인증 방법이 제공된다는 오류가 발생하여 백엔드 생성이 실패합니다.

자격 증명 기반 인증을 사용합니다

Trident은 ONTAP 백엔드와 통신하기 위해 SVM 범위/클러스터 범위 관리자에 대한 자격 증명이 필요합니다. 또는 `vsadmin` 과 같은 미리 정의된 표준 역할을 사용하는 것이 좋습니다 `admin`. 따라서 향후 Trident 릴리스에서 사용할 기능 API를 노출할 수 있는 향후 ONTAP 릴리즈와의 호환성이 보장됩니다. 사용자 지정 보안 로그인 역할을 만들어 Trident와 함께 사용할 수 있지만 권장하지는 않습니다.

백엔드 정의의 예는 다음과 같습니다.

YAML

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

JSON을 참조하십시오

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password"
}
```

백엔드 정의는 자격 증명이 일반 텍스트로 저장되는 유일한 위치라는 점에 유의하십시오. 백엔드가 생성된 후 사용자 이름/암호는 Base64로 인코딩되어 Kubernetes 암호로 저장됩니다. 백엔드의 생성/업딩은 자격 증명에 대한 지식이 필요한 유일한 단계입니다. 따라서 Kubernetes/스토리지 관리자가 수행할 수 있는 관리 전용 작업입니다.

인증서 기반 인증을 사용합니다

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

- clientCertificate: Base64로 인코딩된 클라이언트 인증서 값입니다.
- clientPrivateKey: Base64 - 연결된 개인 키의 인코딩된 값입니다.
- TrustedCACertificate: 신뢰할 수 있는 CA 인증서의 Base64 인코딩 값입니다. 신뢰할 수 있는 CA를 사용하는 경우 이 매개 변수를 제공해야 합니다. 신뢰할 수 있는 CA가 사용되지 않으면 이 작업을 무시할 수 있습니다.

일반적인 워크플로에는 다음 단계가 포함됩니다.

단계

1. 클라이언트 인증서 및 키를 생성합니다. 생성 시 CN(일반 이름)을 ONTAP 사용자로 설정하여 인증하십시오.

```
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. 신뢰할 수 있는 CA 인증서를 ONTAP 클러스터에 추가합니다. 이는 스토리지 관리자가 이미 처리한 것일 수 있습니다. 트러스트된 CA가 사용되지 않으면 무시합니다.

```
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 인증 방법을 지원하는지 `cert` 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 테스트합니다. ONTAP 관리 LIF> 및 <SVM 이름>을 관리 LIF IP 및 SVM 이름으로 바꿉니다. LIF의 서비스 정책이 로 설정되어 있는지 확인해야 `default-data-management` 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. Base64로 인증서, 키 및 신뢰할 수 있는 CA 인증서를 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...Vaaallllluuuueeee",
"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 회전합니다

다른 인증 방법을 사용하거나 자격 증명을 회전하도록 기존 백엔드를 업데이트할 수 있습니다. 이렇게 하면 사용자 이름/암호를 사용하는 백엔드를 인증서를 사용하도록 업데이트할 수 있고 인증서를 사용하는 백엔드는 사용자 이름/암호 기반으로 업데이트할 수 있습니다. 이렇게 하려면 기존 인증 방법을 제거하고 새 인증 방법을 추가해야 합니다. 그런 다음 실행할 필수 매개 변수가 포함된 업데이트된 backend.json 파일을 `tridentctl update backend` 사용합니다.

```
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 회전할 때 스토리지 관리자는 먼저 ONTAP에서 사용자의 암호를 업데이트해야 합니다. 그 다음에는 백엔드 업데이트가 있습니다. 인증서를 회전할 때 여러 인증서를 사용자에게 추가할 수 있습니다. 그런 다음 백엔드가 업데이트되어 새 인증서를 사용합니다. 그러면 ONTAP 클러스터에서 이전 인증서를 삭제할 수 있습니다.

백엔드를 업데이트해도 이미 생성된 볼륨에 대한 액세스가 중단되거나 이후에 생성된 볼륨 연결에 영향을 미치지 않습니다. 백엔드 업데이트에 성공하면 Trident가 ONTAP 백엔드와 통신하여 향후 볼륨 작업을 처리할 수 있음을 나타냅니다.

Trident에 대한 사용자 지정 **ONTAP** 역할을 생성합니다

Privileges에서 작업을 수행할 때 ONTAP 관리자 역할을 사용할 필요가 없도록 최소 Trident로 ONTAP 클러스터 역할을 생성할 수 있습니다. Trident 백엔드 구성에 사용자 이름을 포함하면 Trident은 사용자가 생성한 ONTAP 클러스터 역할을 사용하여 작업을 수행합니다.

Trident 사용자 지정 역할 생성에 대한 자세한 내용은 을 "Trident 사용자 지정 역할 생성기"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 사용자에 대한 사용 이름 만들기:

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

3. 역할을 사용자에게 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 레벨에서 사용자 지정 역할을 생성하려면 * 클러스터 > 설정 * 을 선택합니다.

      SVM 레벨에서 사용자 지정 역할을 생성하려면 * 스토리지 > 스토리지 VM >> 설정 > 사용자 및 역할 * 을 선택합니다 `required SVM`.

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

자세한 내용은 다음 페이지를 참조하십시오.

- "ONTAP 관리를 위한 사용자 지정 역할" 또는 "사용자 지정 역할을 정의합니다"
- "역할 및 사용자 작업"

NFS 엑스포트 정책을 관리합니다

Trident는 NFS 엑스포트 정책을 사용하여 프로비저닝한 볼륨에 대한 액세스를 제어합니다.

Trident는 내보내기 정책을 사용할 때 두 가지 옵션을 제공합니다.

- Trident는 엑스포트 정책 자체를 동적으로 관리할 수 있습니다. 이 운영 모드에서 스토리지 관리자는 허용되는 IP 주소를 나타내는 CIDR 블록의 목록을 지정합니다. Trident는 이러한 범위에 속하는 적용 가능한 노드 IP를 게시 시 자동으로 내보내기 정책에 추가합니다. 또는 CIDR을 지정하지 않으면 게시되는 볼륨이 있는 노드에서 찾은 모든 글로벌 범위 유니캐스트 IP가 엑스포트 정책에 추가됩니다.
- 스토리지 관리자는 엑스포트 정책을 생성하고 규칙을 수동으로 추가할 수 있습니다. 구성에 다른 엑스포트 정책 이름을 지정하지 않는 한 Trident는 기본 엑스포트 정책을 사용합니다.

엑스포트 정책을 동적으로 관리

Trident는 ONTAP 백엔드에 대한 엑스포트 정책을 동적으로 관리하는 기능을 제공합니다. 따라서 스토리지 관리자는 명시적 규칙을 수동으로 정의하는 대신 작업자 노드 IP에 허용되는 주소 공간을 지정할 수 있습니다. 엑스포트 정책 관리를 크게 간소화하므로, 엑스포트 정책을 수정하면 더 이상 스토리지 클러스터에 대한 수동 작업이 필요하지 않습니다. 또한 이렇게 하면 볼륨을 마운트하고 지정된 범위 내에서 IP를 갖는 작업자 노드만 스토리지 클러스터에 대한 액세스를 제한하여 세분화된 자동 관리를 지원합니다.

> 동적 내보내기 정책을 사용할 때는 NAT(Network Address Translation)를 사용하지 마십시오. NAT를 사용하면 스토리지 컨트롤러는 실제 IP 호스트 주소가 아니라 프런트엔드 NAT 주소를 인식하므로 내보내기 규칙에 일치하는 항목이 없으면 액세스가 거부됩니다.

> Trident 24.10에서는 `ontap-nas` 스토리지 드라이버가 이전 릴리스와 마찬가지로 계속 작동합니다. ONTAP-NAS 드라이버에 대해서는 변경된 사항이 없습니다. Trident 24.10에서는 스토리지 드라이버만 `ontap-nas-economy` 볼륨 기반의 세분화된 액세스 제어를 갖습니다.

예

두 가지 구성 옵션을 사용해야 합니다. 다음은 백엔드 정의의 예입니다.

```
---
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 교차점에 노드 CIDR 블록(예: 기본 엑스포트 정책)을 허용하는 엑스포트 규칙과 함께 이전에 생성된 엑스포트 정책이 있는지 확인해야 합니다. Trident 전용 SVM을 사용하려면 항상 NetApp 권장 모범 사례를 따르십시오.

다음은 위의 예를 사용하여 이 기능이 작동하는 방식에 대한 설명입니다.

- `autoExportPolicy` 가 로 설정되어 `true` 있습니다. 이는 Trident이 SVM에 대해 이 백엔드로 프로비저닝된 각 볼륨에 대한 엑스포트 정책을 `svm1` 생성하고 주소 블록을 사용하여 규칙 추가 및 삭제를 `autoexportCIDRs`

처리합니다. 볼륨이 노드에 연결될 때까지 볼륨은 규칙 없이 빈 엑스포트 정책을 사용하여 볼륨에 대한 원치 않는 액세스를 차단합니다. 볼륨이 노드에 게시되면 Trident에서 지정된 CIDR 블록 내에 노드 IP를 포함하는 기본 qtree와 같은 이름의 엑스포트 정책을 생성합니다. 이러한 IP는 상위 FlexVol에서 사용하는 내보내기 정책에도 추가됩니다.

  - 예를 들면 다음과 같습니다.
    - 백엔드 UUID 403b5326-8482-40dB-96d0-d83fb3f4daec
    - `autoExportPolicy` 로 설정합니다 `true`
    - 스토리지 접두사입니다 `trident`
    - PVC UUID a79bcf5f-7b6d-4a40-9876-e2551f159c1c
    - 이름이 Trident_PVC_a79bcf5f_7b6d_4a40_9876_e2551f159c1c인 FlexVol qtree에 대한 엑스포트 정책, 이름이 인 qtree에 대한 `trident-403b5326-8482-40db96d0-d83fb3f4daec` 엑스포트 정책, `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c` SVM에 명명된 빈 엑스포트 정책을 `trident_empty` 생성합니다. FlexVol 엑스포트 정책 규칙은 qtree 엑스포트 정책에 포함된 모든 규칙의 상위 집합이 됩니다. 빈 내보내기 정책은 연결되지 않은 모든 볼륨에서 다시 사용됩니다.

- `autoExportCIDRs` 주소 블록 목록을 포함합니다. 이 필드는 선택 사항이며 기본적으로 ["0.0.0.0/0", ":/0"] 입니다. 정의되지 않은 경우 Trident는 작업자 노드에 있는 모든 전역 범위의 유니캐스트 주소를 게시물과 함께 추가합니다.

이 예에서는 `192.168.0.0/24` 주소 공간이 제공됩니다. 이는 발행물이 있는 이 주소 범위에 속하는 Kubernetes 노드 IP가 Trident에서 생성하는 엑스포트 정책에 추가된다는 것을 나타냅니다. Trident는 실행되는 노드를 등록할 때 노드의 IP 주소를 검색하여 에서 제공하는 주소 블록과 대조하여 확인합니다 `autoExportCIDRs`. 게시 시 IP를 필터링한 후 Trident는 게시 대상 노드의 클라이언트 IP에 대한 내보내기 정책 규칙을 만듭니다.

백엔드를 만든 후 및 `autoExportCIDRs` 백엔드를 업데이트할 수 `autoExportPolicy` 있습니다. 기존 CIDR을 자동으로 관리하거나 삭제하는 백엔드에 새 CIDR을 추가할 수 있습니다. CIDR을 삭제할 때는 기존 연결이 끊어지지 않도록 주의해야 합니다. 백엔드에 대해 비활성화하고 수동으로 생성된 엑스포트 정책으로 폴백할 수도 `autoExportPolicy` 있습니다. 이를 위해서는 백엔드 구성에서 매개 변수를 설정해야 `exportPolicy` 합니다.

Trident에서 백엔드를 생성하거나 업데이트한 후 또는 해당 `tridentbackend` CRD를 사용하여 백엔드를 확인할 수 `tridentctl` 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 노드에 해당하는 액세스 규칙을 제거합니다. Trident는 관리되는 백엔드의 내보내기 정책에서 이 노드 IP를 제거하여 클러스터의 새 노드에서 이 IP를 재사용하지 않는 한 불량 마운트를 방지합니다.

기존 백엔드의 경우 백엔드를 로 업데이트하면 `tridentctl update backend` Trident에서 엑스포트 정책을 자동으로 관리할 수 있습니다. 이렇게 하면 필요한 경우 백엔드의 UUID 및 qtree 이름을 따서 명명된 두 개의 새 엑스포트 정책이 생성됩니다. 백엔드에 있는 볼륨은 마운트 해제했다가 다시 마운트하면 새로 생성된 엑스포트 정책을 사용합니다.

> 자동 관리되는 내보내기 정책이 있는 백엔드를 삭제하면 동적으로 생성된 내보내기 정책이 삭제됩니다. 백엔드가 다시 생성되면 백엔드가 새 백엔드로 처리되어 새 엑스포트 정책이 생성됩니다.

라이브 노드의 IP 주소가 업데이트되면 노드에서 Trident Pod를 다시 시작해야 합니다. 그런 다음 Trident는 이 IP 변경 사항을 반영하도록 관리하는 백엔드에 대한 내보내기 정책을 업데이트합니다.

SMB 볼륨 프로비저닝을 위한 준비

약간의 추가 준비를 통해 드라이버를 사용하여 SMB 볼륨을 프로비저닝할 수 `ontap-nas` 있습니다.

> 온프레미스에 ONTAP용 SMB 볼륨을 생성하려면 SVM에서 NFS 및 SMB/CIFS 프로토콜을 모두 구성해야 `ontap-nas-economy` 합니다. 이 두 프로토콜 중 하나를 구성하지 않으면 SMB 볼륨 생성에 실패합니다.

> `autoExportPolicy` SMB 볼륨에는 가 지원되지 않습니다.

시작하기 전에

SMB 볼륨을 프로비저닝하려면 먼저 다음 항목이 있어야 합니다.

- Linux 컨트롤러 노드 및 Windows Server 2022를 실행하는 Windows 작업자 노드가 있는 Kubernetes 클러스터 Trident는 Windows 노드에서만 실행되는 Pod에 마운트된 SMB 볼륨을 지원합니다.
- Active Directory 자격 증명이 포함된 Trident 암호가 하나 이상 있습니다. 비밀 생성하기 `smbcreds`:

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

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

단계

1. 온프레미스 ONTAP의 경우 선택적으로 SMB 공유를 생성하거나 Trident에서 공유를 생성할 수 있습니다.

   ONTAP용 Amazon FSx에는 SMB 공유가 필요합니다.

   공유 폴더 스냅인을 사용하거나 ONTAP CLI를 사용하는 두 가지 방법 중 하나로 SMB 관리자 공유를 생성할 수 "Microsoft 관리 콘솔"있습니다. ONTAP CLI를 사용하여 SMB 공유를 생성하려면 다음을 따르십시오.

   a. 필요한 경우 공유에 대한 디렉토리 경로 구조를 생성합니다.

      이 `vserver cifs share create` 명령은 공유를 생성하는 동안 -path 옵션에 지정된 경로를 확인합니다. 지정한 경로가 없으면 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 을 "SMB 공유를 생성합니다"참조하십시오.

2. 백엔드를 생성할 때 SMB 볼륨을 지정하려면 다음을 구성해야 합니다. 모든 FSx for ONTAP 백엔드 구성 옵션은 을 "ONTAP 구성 옵션 및 예제용 FSX"참조하십시오.

매개 변수	설명	예
`smbShare`	Microsoft 관리 콘솔 또는 ONTAP CLI를 사용하여 생성된 SMB 공유의 이름, Trident에서 SMB 공유를 생성할 수 있는 이름, 볼륨에 대한 일반적인 공유 액세스를 방지하기 위해 매개 변수를 비워 둘 수 있습니다. 이 매개 변수는 사내 ONTAP의 경우 선택 사항입니다. 이 매개변수는 ONTAP 백엔드에 대한 아마존 FSx에 필요하며 비워둘 수 없습니다.	`smb-share`
`nasType`	* 를. * 로 설정해야 합니다 `smb` null인 경우 기본값은 로 `nfs`설정됩니다.	`smb`
`securityStyle`	새로운 볼륨에 대한 보안 스타일 **SMB** 볼륨의 경우 또는 **`mixed`** 로 설정해야 **`ntfs`** 합니다.	`ntfs` 또는 `mixed` SMB 볼륨에 대해 설정할 수 있습니다
`unixPermissions`	모드를 선택합니다. SMB 볼륨에 대해서는 * 를 비워 두어야 합니다. *	""

ONTAP NAS 구성 옵션 및 예

Trident 설치 시 ONTAP NAS 드라이버를 생성하고 사용하는 방법에 대해 알아봅니다. 이 섹션에서는 백엔드 구성 예제 및 Backend를 StorageClasses에 매핑하는 방법에 대한 세부 정보를 제공합니다.

백엔드 구성 옵션

백엔드 구성 옵션은 다음 표를 참조하십시오.

매개 변수	설명	기본값
`version`		항상 1
`storageDriverName`	스토리지 드라이버의 이름입니다	"ONTAP-NAS", "ONTAP-NAS-Economy", "ONTAP-NAS-flexgroup", "ONTAP-SAN", "ONTAP-SAN-Economy"
`backendName`	사용자 지정 이름 또는 스토리지 백엔드	드라이버 이름 + "_" + dataLIF
`managementLIF`	클러스터 또는 SVM 관리 LIF의 IP 주소 정규화된 도메인 이름(FQDN)을 지정할 수 있습니다. IPv6 플래그를 사용하여 Trident가 설치된 경우 IPv6 주소를 사용하도록 설정할 수 있습니다. IPv6 주소는 과 같이 대괄호로 정의해야 `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]` 합니다. 원활한 MetroCluster 전환은 를 MetroCluster 예참조하십시오.	“10.0.0.1”, “[2001:1234:ABCD::fee]”

매개 변수	설명	기본값
`dataLIF`	프로토콜 LIF의 IP 주소입니다. 지정하는 것이 좋습니다 `dataLIF`. 제공되지 않는 경우 Trident는 SVM에서 데이터 LIF를 가져옵니다. NFS 마운트 작업에 사용할 FQDN(정규화된 도메인 이름)을 지정하면 여러 데이터 LIF에서 로드 밸런싱을 위해 라운드 로빈 DNS를 생성할 수 있습니다. 초기 설정 후에 변경할 수 있습니다. 을 참조하십시오. IPv6 플래그를 사용하여 Trident가 설치된 경우 IPv6 주소를 사용하도록 설정할 수 있습니다. IPv6 주소는 과 같이 대괄호로 정의해야 `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]` 합니다. * MetroCluster의 경우 생략합니다. * 를 MetroCluster 예참조하십시오.	지정되지 않은 경우 SVM에서 지정 주소 또는 파생(권장하지 않음)
`svm`	사용할 스토리지 가상 머신 * MetroCluster에는 생략함 * 를 MetroCluster 예참조하십시오.	SVM이 지정된 경우 파생됩니다 `managementLIF`
`autoExportPolicy`	자동 엑스포트 정책 생성 및 업데이트 [Boolean] 활성화 Trident는 및 `autoExportCIDRs` 옵션을 사용하여 `autoExportPolicy` 엑스포트 정책을 자동으로 관리할 수 있습니다.	거짓
`autoExportCIDRs`	이 설정된 경우에 대해 Kubernetes 노드 IP를 필터링하는 CIDR `autoExportPolicy` 목록입니다. Trident는 및 `autoExportCIDRs` 옵션을 사용하여 `autoExportPolicy` 엑스포트 정책을 자동으로 관리할 수 있습니다.	["0.0.0.0/0",":/0"]'
`labels`	볼륨에 적용할 임의의 JSON 형식 레이블 세트입니다	""
`clientCertificate`	Base64 - 클라이언트 인증서의 인코딩된 값입니다. 인증서 기반 인증에 사용됩니다	""
`clientPrivateKey`	Base64 - 클라이언트 개인 키의 인코딩된 값입니다. 인증서 기반 인증에 사용됩니다	""
`trustedCACertificate`	Base64 - 신뢰할 수 있는 CA 인증서의 인코딩된 값입니다. 선택 사항. 인증서 기반 인증에 사용됩니다	""
`username`	클러스터/SVM에 연결할 사용자 이름입니다. 자격 증명 기반 인증에 사용됩니다	
`password`	클러스터/SVM에 연결하는 암호 자격 증명 기반 인증에 사용됩니다	
`storagePrefix`	SVM에서 새 볼륨을 프로비저닝할 때 사용되는 접두사 설정한 후에는 업데이트할 수 없습니다 24자 이상인 ONTAP-nas-Economy와 storagePrefix를 사용할 경우 볼륨 이름에 포함되기는 하지만 qtree에 스토리지 접두사가 포함되지 않습니다.	"트리덴트"

매개 변수	설명	기본값
`aggregate`	프로비저닝을 위한 애그리게이트(선택 사항, SVM에 셋팅해야 하는 경우) 드라이버의 경우 `ontap-nas-flexgroup` 이 옵션은 무시됩니다. 할당되지 않은 경우 사용 가능한 애그리게이트를 사용하여 FlexGroup 볼륨을 프로비저닝할 수 있습니다. SVM에서 Aggregate를 업데이트하면 Trident 컨트롤러를 다시 시작하지 않고도 SVM을 폴링하여 Trident에서 자동으로 업데이트됩니다. 볼륨을 프로비저닝하기 위해 Trident의 특정 애그리게이트를 구성한 경우, 애그리게이트의 이름을 바꾸거나 SVM에서 이동할 경우 SVM 애그리게이트를 폴링하는 동안 백엔드가 Trident에서 오류 상태로 전환됩니다. Aggregate를 SVM에 있는 Aggregate로 변경하거나 완전히 제거하여 백엔드를 다시 온라인 상태로 전환해야 합니다.	""
`limitAggregateUsage`	사용량이 이 비율을 초과하면 프로비저닝이 실패합니다. ONTAP * 용 아마존 FSx에는 * 가 적용되지 않습니다	""(기본적으로 적용되지 않음)
flexgroupAggregateList 를 참조하십시오	프로비저닝을 위한 애그리게이트 목록(선택 사항, SVM에 할당되어야 함) SVM에 할당된 모든 애그리게이트는 FlexGroup 볼륨을 프로비저닝하는 데 사용됩니다. ONTAP-NAS-FlexGroup * 스토리지 드라이버에 대해 지원됩니다. SVM에서 애그리게이트 목록이 업데이트되면 Trident 컨트롤러를 다시 시작하지 않고도 SVM을 폴링하여 Trident에서 목록이 자동으로 업데이트됩니다. 볼륨을 프로비저닝하도록 Trident의 특정 애그리게이트 목록을 구성한 경우, 애그리게이트 목록의 이름을 바꾸거나 SVM에서 이동하면 SVM 애그리게이트를 폴링하는 동안 백엔드가 Trident에서 오류 상태로 전환됩니다. 애그리게이트 목록을 SVM에 있는 목록으로 변경하거나 완전히 제거하여 백엔드를 다시 온라인 상태로 전환해야 합니다.	""
`limitVolumeSize`	요청된 볼륨 크기가 이 값보다 큰 경우 용량 할당에 실패합니다. 또한 qtree에서 관리하는 볼륨의 최대 크기를 제한하고, `qtreesPerFlexvol` 옵션을 통해 FlexVol당 최대 qtree 수를 사용자 지정할 수 있습니다.	""(기본적으로 적용되지 않음)

매개 변수	설명	기본값
`debugTraceFlags`	문제 해결 시 사용할 디버그 플래그입니다. 예제, {"api":false, "method":true} 문제 해결을 진행하고 자세한 로그 덤프가 필요한 경우가 아니면 사용하지 마십시오 `debugTraceFlags`.	null입니다
`nasType`	NFS 또는 SMB 볼륨 생성을 구성합니다. 옵션은 `nfs`, `smb` 또는 null입니다. Null로 설정하면 기본적으로 NFS 볼륨이 설정됩니다.	`nfs`
`nfsMountOptions`	쉼표로 구분된 NFS 마운트 옵션 목록입니다. Kubernetes 영구 볼륨의 마운트 옵션은 일반적으로 스토리지 클래스에 지정되어 있지만, 스토리지 클래스에 마운트 옵션이 지정되지 않은 경우 Trident는 스토리지 백엔드의 구성 파일에 지정된 마운트 옵션을 사용하도록 폴백합니다. 스토리지 클래스 또는 구성 파일에 마운트 옵션이 지정되지 않은 경우 Trident는 연결된 영구 볼륨에 마운트 옵션을 설정하지 않습니다.	""
`qtreesPerFlexvol`	FlexVol당 최대 qtree, 범위 [50, 300]에 있어야 함	"200"
`smbShare`	Microsoft 관리 콘솔 또는 ONTAP CLI를 사용하여 생성된 SMB 공유의 이름, Trident에서 SMB 공유를 생성할 수 있는 이름, 볼륨에 대한 일반적인 공유 액세스를 방지하기 위해 매개 변수를 비워 둘 수 있습니다. 이 매개 변수는 사내 ONTAP의 경우 선택 사항입니다. 이 매개변수는 ONTAP 백엔드에 대한 아마존 FSx에 필요하며 비워둘 수 없습니다.	`smb-share`
`useREST`	ONTAP REST API를 사용하는 부울 매개 변수입니다. `useREST` 로 설정된 `true` 경우 Trident는 ONTAP REST API를 사용하여 백엔드와 통신하고, 로 설정된 경우 `false` Trident는 ONTAP ZAPI 호출을 사용하여 백엔드와 통신합니다. 이 기능을 사용하려면 ONTAP 9.11.1 이상이 필요합니다. 또한 사용되는 ONTAP 로그인 역할에는 애플리케이션에 대한 액세스 권한이 있어야 `ontap` 합니다. 이는 미리 정의된 역할과 역할에 의해 충족됩니다. `vsadmin` `cluster-admin` Trident 24.06 릴리스 및 ONTAP 9.15.1 이상부터 는 `useREST` 기본적으로 로 설정되어 `true` 있으며 ONTAP ZAPI 호출을 사용하도록 로 `false` 변경합니다. `useREST`	`true` ONTAP 9.15.1 이상, 그렇지 않은 경우 `false`.
`limitVolumePoolSize`	ONTAP-NAS-이코노미 백엔드에서 Qtree를 사용할 때 가장 필요한 최대 FlexVol 크기입니다.	""(기본적으로 적용되지 않음)
`denyNewVolumePools`	못하도록백 엔드가 새 FlexVol 볼륨을 생성하지 포함하도록 `ontap-nas-economy` 해당 qtree를 제한합니다. 기존 FlexVol만 새 PVS 프로비저닝에 사용됩니다.	

볼륨 프로비저닝을 위한 백엔드 구성 옵션

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

매개 변수	설명	기본값
`spaceAllocation`	Qtree에 공간 할당	"참"
`spaceReserve`	공간 예약 모드, "없음"(씬) 또는 "볼륨"(일반)	"없음"
`snapshotPolicy`	사용할 스냅샷 정책입니다	"없음"
`qosPolicy`	생성된 볼륨에 할당할 QoS 정책 그룹입니다. 스토리지 풀/백엔드에서 qosPolicy 또는 adapativeQosPolicy 중 하나를 선택합니다	""
`adaptiveQosPolicy`	생성된 볼륨에 할당할 적응형 QoS 정책 그룹입니다. 스토리지 풀/백엔드에서 qosPolicy 또는 adapativeQosPolicy 중 하나를 선택합니다. ONTAP에서 지원되지 않음 - NAS - 이코노미	""
`snapshotReserve`	스냅숏용으로 예약된 볼륨의 백분율입니다	"없음"인 경우 "0", 그렇지 않은 경우 `snapshotPolicy`"
`splitOnClone`	생성 시 상위 클론에서 클론을 분할합니다	"거짓"
`encryption`	새 볼륨에서 NetApp 볼륨 암호화(NVE)를 활성화하고, 기본값은 로 설정합니다. `false` 이 옵션을 사용하려면 NVE 라이센스가 클러스터에서 활성화되어 있어야 합니다. 백엔드에서 NAE가 활성화된 경우 Trident에서 프로비저닝된 모든 볼륨은 NAE가 사용됩니다. 자세한 내용은 다음을 "Trident가 NVE 및 NAE와 작동하는 방법 "참조하십시오.	"거짓"
`tieringPolicy`	"없음"을 사용하는 계층화 정책	ONTAP 9.5 SVM-DR 이전 구성의 경우 "스냅샷 전용
`unixPermissions`	모드를 선택합니다	NFS 볼륨의 경우 "777", SMB 볼륨의 경우 비어 있음(해당 없음
`snapshotDir`	디렉터리에 액세스를 제어합니다 `.snapshot`	NFSv3의 경우 NFSv4의 경우 "true"입니다
`exportPolicy`	사용할 엑스포트 정책	"기본값"
`securityStyle`	새로운 볼륨에 대한 보안 스타일 NFS는 `mixed` 및 `unix` 보안 형식을 지원합니다. SMB 지원 `mixed` 및 `ntfs` 보안 스타일	NFS 기본값은 `unix`입니다. `SMB` 기본값은 `ntfs` 입니다.
`nameTemplate`	사용자 지정 볼륨 이름을 생성하는 템플릿입니다.	""

> Trident에서 QoS 정책 그룹을 사용하려면 ONTAP 9 .8 이상이 필요합니다. 비공유 QoS 정책 그룹을 사용하고 정책 그룹이 각 구성 요소에 개별적으로 적용되도록 해야 합니다. 공유 QoS 정책 그룹은 모든 워크로드의 총 처리량에 대한 제한을 적용합니다.

볼륨 프로비저닝의 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'
```

및 `ontap-nas-flexgroups` 의 경우 `ontap-nas` Trident는 이제 새로운 계산을 사용하여 FlexVol의 크기가 snapshotReserve 비율 및 PVC로 올바르게 지정되도록 합니다. 사용자가 PVC를 요청하면 Trident는 새 계산을 사용하여 더 많은 공간을 가진 원래 FlexVol를 생성합니다. 이 계산을 통해 사용자는 PVC에서 요청한 쓰기 가능 공간을 확보할 수 있으며 요청된 공간보다 적은 공간을 확보할 수 있습니다. v21.07 이전에는 사용자가 스냅샷 보존 공간을 50%로 하여 PVC(예: 5GiB)를 요청할 때 쓰기 가능한 공간은 2.5GiB에 불과합니다. 이는 사용자가 요청한 볼륨이 전체 볼륨에 해당하고 그 비율이기 `snapshotReserve` 때문입니다. Trident 21.07에서 사용자가 요청하는 것은 쓰기 가능 공간이며 Trident는 이 `snapshotReserve` 수를 전체 볼륨의 백분율로 정의합니다. 에는 적용되지 `ontap-nas-economy` 않습니다. 이 작동 방식을 보려면 다음 예를 참조하십시오.

계산은 다음과 같습니다.

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

snapshotReserve = 50%, PVC request = 5GiB의 경우, 총 볼륨 크기는 2/.5 = 10GiB이고 사용 가능한 크기는 5GiB입니다. 이는 사용자가 PVC 요청에서 요청한 것입니다. 이 `volume show` 명령은 다음 예제와 유사한 결과를 표시해야 합니다.

```
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
                  _pvc_89f1c156_3801_4de4_9f9d_034d54c395f4
                                   online     RW         10GB     5.00GB    0%
                  _pvc_e8372153_9ad9_474a_951a_08ae15e1c0ba
                                   online     RW          1GB    511.8MB    0%
2 entries were displayed.
```

이전 설치의 기존 백엔드는 Trident를 업그레이드할 때 위에서 설명한 대로 볼륨을 프로비저닝합니다. 업그레이드하기 전에 생성한 볼륨의 경우 변경 사항을 관찰하기 위해 볼륨의 크기를 조정해야 합니다. 예를 들어, 이전 버전의 2GiB PVC는 `snapshotReserve=50` 1GiB의 쓰기 가능 공간을 제공하는 볼륨을 생성했습니다. 예를 들어, 볼륨을 3GiB로 조정하면 애플리케이션에 6GiB 볼륨의 쓰기 가능 공간이 3GiB로 표시됩니다.

최소 구성의 예

다음 예에서는 대부분의 매개 변수를 기본값으로 두는 기본 구성을 보여 줍니다. 이는 백엔드를 정의하는 가장 쉬운 방법입니다.

> Trident가 있는 NetApp ONTAP에서 Amazon FSx를 사용하는 경우 IP 주소 대신 LIF에 대한 DNS 이름을 지정하는 것이 좋습니다.

ONTAP NAS 경제성의 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 예

전환 및 전환 중에 백엔드 정의를 수동으로 업데이트할 필요가 없도록 백엔드를 구성할 수 "SVM 복제 및 복구 "있습니다.

원활한 스위치오버 및 스위치백의 경우 및 `svm` 매개 변수를 사용하여 SVM을 지정하고 `managementLIF` 생략합니다. `dataLIF` 예를 들면 다음과 같습니다.

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

SMB 볼륨의 예입니다

```
---
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 인증의 예

이것은 최소 백엔드 구성 예입니다. `clientCertificate`, `clientPrivateKey` 및 `trustedCACertificate` (신뢰할 수 있는 CA를 사용하는 경우 선택 사항)가 에 채워지고 `backend.json` 클라이언트 인증서, 개인 키 및 신뢰할 수 있는 CA 인증서의 base64로 인코딩된 값을 가져옵니다.

```
---
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 정책의 예

이 예에서는 Trident에서 동적 엑스포트 정책을 사용하여 엑스포트 정책을 자동으로 생성 및 관리하도록 하는 방법을 보여 줍니다. 및 `ontap-nas-flexgroup` 드라이버에도 동일하게 `ontap-nas-economy` 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 예에서는 IPv6 주소 사용을 보여 `managementLIF` 줍니다.

```
---
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 **ONTAP**용 **Amazon FSx**의 예

`smbShare`SMB 볼륨을 사용하는 FSx for ONTAP에 매개 변수가 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_
```

nameTemplate이 포함된 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}}_{{.volume.R
equestName}}"
},
"labels": {"cluster": "ClusterA", "PVC":
"{{.volume.Namespace}}_{{.volume.RequestName}}"}
```

가상 풀의 백엔드 예

아래 표시된 샘플 백엔드 정의 파일에서 모든 스토리지 풀에 대해 특정 기본값이 설정되어 있습니다(예: `spaceReserve` 없음, `spaceAllocation` 거짓, 거짓 `encryption`). 가상 풀은 스토리지 섹션에 정의됩니다.

Trident는 "Comments" 필드에 프로비저닝 레이블을 설정합니다. 설명은 의 FlexVol `ontap-nas` 또는 의 FlexGroup에 `ontap-nas-flexgroup` 설정됩니다. Trident는 프로비저닝 시 가상 풀에 있는 모든 레이블을 스토리지 볼륨에 복제합니다. 편의를 위해 스토리지 관리자는 가상 풀 및 그룹 볼륨별로 레이블을 레이블별로 정의할 수 있습니다.

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

ONTAP NAS의 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 FlexGroup의 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 경제성의 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 을 가상 풀의 백엔드 예참조하십시오. 각 StorageClass 는 필드를 사용하여 `parameters.selector` 볼륨을 호스팅하는 데 사용할 수 있는 가상 풀을 호출합니다. 선택한 가상 풀에 볼륨이 정의되어 있습니다.

- `protection-gold`StorageClass는 백엔드의 첫 번째 및 두 번째 가상 풀에 매핑됩니다. `ontap-nas-flexgroup` 골드 레벨 보호 기능을 제공하는 유일한 풀입니다.

```
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 백엔드의 세 번째 및 네 번째 가상 풀에 매핑됩니다. `ontap-nas-flexgroup` 금 이외의 보호 수준을 제공하는 유일한 풀입니다.

```
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 백엔드의 네 번째 가상 풀에 매핑됩니다. `ontap-nas` mysqldb 유형 앱에 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 백엔드의 세 번째 가상 풀에 매핑됩니다. `ontap-nas-flexgroup` 실버 레벨 보호 및 20,000포인트 적립을 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 백엔드의 세 번째 가상 풀과 백엔드의 두 번째 `ontap-nas-economy` 가상 풀에 매핑됩니다. `ontap-nas` 5000 크레딧 포인트를 보유한 유일한 풀 서비스입니다.

```
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 선택되었는지 결정하고 스토리지 요구 사항이 충족되는지 확인합니다.

초기 구성 후 업데이트 `dataLIF`

다음 명령을 실행하여 초기 구성 후에 데이터 LIF를 변경할 수 있으며, 업데이트된 데이터 LIF가 포함된 새 백엔드 JSON 파일을 제공할 수 있습니다.

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

PVC가 하나 이상의 포드에 연결된 경우 해당 포드를 모두 내린 다음 다시 불러와서 새 데이터 LIF가 적용되도록 해야 합니다.

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 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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