# ONTAP NAS-Treiber

Trident

NetApp
July 01, 2026

# Inhalt

# ONTAP NAS-Treiber

## ONTAP NAS-Treiberübersicht

Erfahren Sie mehr über die Konfiguration eines ONTAP Backends mit ONTAP und Cloud Volumes ONTAP NAS-Treibern.

### ONTAP NAS-Treiberdetails

Trident stellt die folgenden NAS-Speichertreiber für die Kommunikation mit dem ONTAP Cluster bereit. Unterstützte Zugriffsmodi sind: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

| Treiber | Protokoll | volumeMode | Unterstützte Zugriffsmodi | Unterstützte Dateisysteme |
|---|---|---|---|---|
| `ontap-nas` | NFS SMB | Dateisystem | RWO, ROX, RWX, RWOP | "", `nfs`, `smb` |
| `ontap-nas-economy` | NFS SMB | Dateisystem | RWO, ROX, RWX, RWOP | "", `nfs`, `smb` |
| `ontap-nas-flexgroup` | NFS SMB | Dateisystem | RWO, ROX, RWX, RWOP | "", `nfs`, `smb` |

- Verwenden Sie `ontap-san-economy` nur, wenn die Anzahl der persistenten Speichernutzungen voraussichtlich höher ist als "Unterstützte ONTAP Volume-Grenzwerte".
- Verwenden Sie `ontap-nas-economy` nur, wenn die Anzahl der persistenten Speichernutzungen voraussichtlich höher ist als "Unterstützte ONTAP Volume-Grenzwerte" und der `ontap-san-economy` Treiber nicht verwendet werden kann.
- Verwenden Sie `ontap-nas-economy` nicht, wenn Sie einen Bedarf an Datenschutz, Notfallwiederherstellung oder Mobilität erwarten.
- NetApp empfiehlt nicht, Flexvol autogrow in allen ONTAP-Treibern zu verwenden, außer ontap-san. Als Workaround unterstützt Trident die Verwendung von Snapshot-Reserve und skaliert Flexvol-Volumes entsprechend.

### Benutzerberechtigungen

Trident wird entweder als ONTAP- oder SVM-Administrator ausgeführt, typischerweise mit dem `admin` cluster-Benutzer oder einem `vsadmin` SVM-Benutzer oder einem Benutzer mit anderem Namen, der die gleiche Rolle hat.

Für Amazon FSx for NetApp ONTAP-Bereitstellungen wird Trident entweder als ONTAP- oder SVM-Administrator ausgeführt, mit dem cluster `fsxadmin` Benutzer oder einem `vsadmin` SVM-Benutzer oder einem Benutzer mit anderem Namen, der die gleiche Rolle hat. Der `fsxadmin` Benutzer ist ein eingeschränkter Ersatz für den cluster-Admin-Benutzer.

Wenn Sie den `limitAggregateUsage` Parameter verwenden, sind Cluster-Administratorrechte erforderlich. Bei Verwendung von Amazon FSx für NetApp ONTAP mit Trident wird der `limitAggregateUsage` Parameter nicht mit den `vsadmin` und `fsxadmin` Benutzerkonten funktionieren. Der Konfigurationsvorgang schlägt fehl, wenn Sie diesen Parameter angeben.

Zwar ist es möglich, in ONTAP eine restriktivere Rolle zu erstellen, die ein Trident-Treiber verwenden kann, wir raten jedoch davon ab. Die meisten neuen Versionen von Trident rufen zusätzliche APIs auf, die berücksichtigt werden müssten, was Aktualisierungen erschwert und fehleranfällig macht.

# Bereiten Sie die Konfiguration eines Backends mit ONTAP NAS-Treibern vor

Verstehen Sie die Anforderungen, Authentifizierungsoptionen und Exportrichtlinien für die Konfiguration eines ONTAP Backends mit ONTAP NAS-Treibern. Ab der Version 25.10 unterstützt NetApp Trident "NetApp AFX-Speichersystem". NetApp AFX-Speichersysteme unterscheiden sich von anderen ONTAP-Systemen (ASA, AFF und FAS) in der Implementierung ihrer Speicherschicht. In der Trident-Backend-Konfiguration müssen Sie nicht angeben, dass Ihr System AFX ist. Wenn Sie `ontap-nas` als `storageDriverName` auswählen, erkennt Trident die AFX-Systeme automatisch.

Nur der `ontap-nas` Treiber (mit NFS-Protokoll) wird für AFX-Systeme unterstützt; das SMB-Protokoll wird nicht unterstützt.

## Anforderungen

- Für alle ONTAP Backends erfordert Trident, dass mindestens ein Aggregat dem SVM zugewiesen wird.
- Sie können mehr als einen Treiber ausführen und Speicherklassen erstellen, die auf den einen oder den anderen verweisen. Beispielsweise könnten Sie eine Gold-Klasse konfigurieren, die den `ontap-nas` Treiber verwendet, und eine Bronze-Klasse, die den `ontap-nas-economy` verwendet.
- Auf allen Ihren Kubernetes-Worker-Knoten müssen die entsprechenden NFS-Tools installiert sein. Weitere Informationen finden Sie unter "hier,".
- Trident unterstützt SMB-Volumes nur, wenn sie in Pods eingebunden sind, die auf Windows-Knoten ausgeführt werden. Siehe Bereiten Sie die Bereitstellung von SMB-Volumes vor für Details.

## Authentifizieren Sie das ONTAP Backend

Trident bietet zwei Modi zur Authentifizierung eines ONTAP Backend.

- Anmeldeinformationsbasiert: Dieser Modus erfordert ausreichende Berechtigungen für das ONTAP Backend. Es wird empfohlen, ein Konto zu verwenden, das einer vordefinierten Sicherheitsanmelderolle zugeordnet ist, wie `admin` oder `vsadmin` um maximale Kompatibilität mit ONTAP Versionen zu gewährleisten.
- Zertifikatsbasiert: In diesem Modus ist ein auf dem Backend installiertes Zertifikat erforderlich, damit Trident mit einem ONTAP Cluster kommunizieren kann. Hier muss die Backend-Definition Base64-kodierte Werte des Client-Zertifikats, des Schlüssels und, falls verwendet (empfohlen), des vertrauenswürdigen CA-Zertifikats enthalten.

Sie können bestehende Backends aktualisieren, um zwischen anmeldeinformationsbasierten und zertifikatsbasierten Authentifizierungsverfahren zu wechseln. Es wird jedoch jeweils nur ein Authentifizierungsverfahren unterstützt. Um zu einem anderen Authentifizierungsverfahren zu wechseln, müssen Sie das bestehende Verfahren aus der Backend-Konfiguration entfernen.

Wenn Sie versuchen, **sowohl Anmeldeinformationen als auch Zertifikate** anzugeben, schlägt die Backend-Erstellung mit der Fehlermeldung fehl, dass mehr als ein Authentifizierungsverfahren in der Konfigurationsdatei angegeben wurde.

### Aktivieren Sie die anmeldeinformationsbasierte Authentifizierung

Trident benötigt die Anmeldeinformationen eines Administrators mit SVM- oder Cluster-Berechtigungen, um mit dem ONTAP Backend zu kommunizieren. Es wird empfohlen, vordefinierte Standardrollen wie `admin` oder `vsadmin` zu verwenden. Dies gewährleistet die Vorwärtskompatibilität mit zukünftigen ONTAP Versionen, die möglicherweise Feature-APIs für zukünftige Trident Versionen bereitstellen. Eine benutzerdefinierte Sicherheits-Anmelderolle kann erstellt und mit Trident verwendet werden, wird jedoch nicht empfohlen.

Eine beispielhafte Backend-Definition sieht folgendermaßen aus:

**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"
    }
}
```

Beachten Sie, dass die Backend-Definition der einzige Ort ist, an dem die Zugangsdaten im Klartext gespeichert werden. Nach der Backend-Erstellung werden Benutzernamen/Passwörter mit Base64 kodiert und

als Kubernetes-Secrets gespeichert. Die Erstellung/Aktualisierung eines Backends ist der einzige Schritt, der Kenntnisse der Zugangsdaten erfordert. Daher handelt es sich um eine ausschließlich vom Kubernetes-/Speicheradministrator durchzuführende Operation.

### Zertifikatsbasierte Authentifizierung aktivieren

Neue und bestehende Backends können ein Zertifikat verwenden und mit dem ONTAP Backend kommunizieren. In der Backend-Definition sind drei Parameter erforderlich.

- clientCertificate: Base64-kodierter Wert des Client-Zertifikats.
- clientPrivateKey: Base64-kodierter Wert des zugehörigen privaten Schlüssels.
- trustedCACertificate: Base64-kodierter Wert des Zertifikats einer vertrauenswürdigen CA. Wenn eine vertrauenswürdige CA verwendet wird, muss dieser Parameter angegeben werden. Dies kann ignoriert werden, wenn keine vertrauenswürdige CA verwendet wird.

Ein typischer Arbeitsablauf umfasst die folgenden Schritte.

#### Schritte

1. Generieren Sie ein Clientzertifikat und einen Schlüssel. Legen Sie beim Generieren den Common Name (CN) auf den ONTAP Benutzer fest, als den Sie sich authentifizieren möchten.

```
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. Fügen Sie dem ONTAP Cluster ein vertrauenswürdiges CA-Zertifikat hinzu. Dies wurde möglicherweise bereits vom Storage-Administrator erledigt. Ignorieren Sie dies, falls keine vertrauenswürdige CA verwendet wird.

```
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. Installieren Sie das Clientzertifikat und den Schlüssel (aus Schritt 1) auf dem ONTAP Cluster.

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

4. Bestätigen Sie, dass die ONTAP Sicherheitsanmeldungsrolle das `cert` Authentifizierungsverfahren unterstützt.

```
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. Testen Sie die Authentifizierung mit dem generierten Zertifikat. Ersetzen Sie <ONTAP Management LIF> und <vserver name> durch die Management-LIF-IP und den SVM-Namen. Sie müssen sicherstellen, dass die Service-Richtlinie des LIF auf `default-data-management` gesetzt ist.

```
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. Zertifikat, Schlüssel und vertrauenswürdiges CA-Zertifikat mit Base64 kodieren.

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

7. Erstellen Sie das Backend unter Verwendung der im vorherigen Schritt erhaltenen Werte.

```
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 |
+------------+----------------+--------------------------------------
+--------+---------+
```

**Aktualisieren Sie Authentifizierungsverfahren oder rotieren Sie die Anmeldeinformationen**

Sie können ein bestehendes Backend aktualisieren, um ein anderes Authentifizierungsverfahren zu verwenden oder um die Anmeldeinformationen zu rotieren. Dies funktioniert in beide Richtungen: Backends, die Benutzername/Passwort verwenden, können auf Zertifikate umgestellt werden; Backends, die Zertifikate verwenden, können auf Benutzername/Passwort umgestellt werden. Dazu müssen Sie das bestehende Authentifizierungsverfahren entfernen und das neue Authentifizierungsverfahren hinzufügen. Verwenden Sie dann die aktualisierte backend.json-Datei mit den erforderlichen Parametern, um `tridentctl update backend` auszuführen.

```
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 |
+------------+----------------+--------------------------------------
+--------+---------+
```

Beim Rotieren von Passwörtern muss der Speicheradministrator zunächst das Passwort für den Benutzer auf ONTAP aktualisieren. Danach erfolgt ein Backend-Update. Beim Rotieren von Zertifikaten können dem Benutzer mehrere Zertifikate hinzugefügt werden. Das Backend wird dann aktualisiert, um das neue Zertifikat zu verwenden, wonach das alte Zertifikat aus dem ONTAP Cluster gelöscht werden kann.

Die Aktualisierung des Backends beeinträchtigt weder den Zugriff auf bereits erstellte Volumes noch später hergestellte Volume-Verbindungen. Eine erfolgreiche Backend-Aktualisierung zeigt an, dass Trident mit dem ONTAP Backend kommunizieren und zukünftige Volume-Operationen ausführen kann.

### Erstellen einer benutzerdefinierten ONTAP Rolle für Trident

Sie können eine ONTAP-Clusterrolle mit minimalen Berechtigungen erstellen, sodass Sie nicht die ONTAP-Admin-Rolle verwenden müssen, um Vorgänge in Trident durchzuführen. Wenn Sie den Benutzernamen in einer Trident-Backend-Konfiguration angeben, verwendet Trident die von Ihnen erstellte ONTAP-Clusterrolle, um die Vorgänge auszuführen.

Weitere Informationen zum Erstellen benutzerdefinierter Trident-Rollen finden Sie unter "Trident Custom-Role-Generator".

**Verwendung der ONTAP-Befehlszeile**

1. Erstellen Sie eine neue Rolle mit folgendem Befehl:

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

2. Erstellen Sie einen Benutzernamen für den Trident Benutzer:

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

3. Ordnen Sie die Rolle dem Benutzer zu:

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

**Verwenden von System Manager**

Führen Sie die folgenden Schritte im ONTAP System Manager aus:

1. **Erstellen Sie eine benutzerdefinierte Rolle**:
   a. Um eine benutzerdefinierte Rolle auf Clusterebene zu erstellen, wählen Sie **Cluster > Settings**.

      (Oder) Um eine benutzerdefinierte Rolle auf SVM-Ebene zu erstellen, wählen Sie **Storage > Storage VMs > `required SVM`> Settings > Users and Roles**.

   b. Wählen Sie das Pfeilsymbol (→) neben **Users and Roles** aus.
   c. Wählen Sie unter **Rollen +Add** aus.
   d. Definieren Sie die Regeln für die Rolle und klicken Sie auf **Save**.
2. **Rolle dem Trident-Benutzer zuordnen**: + Führen Sie die folgenden Schritte auf der Seite **Benutzer und Rollen** aus:
   a. Wählen Sie das Symbol **+** unter **Benutzer** aus.
   b. Wählen Sie den gewünschten Benutzernamen aus und wählen Sie eine Rolle im Dropdown-Menü für **Rolle**.
   c. Klicken Sie auf **Speichern**.

Weitere Informationen finden Sie auf den folgenden Seiten:

- "Benutzerdefinierte Rollen für die Administration von ONTAP" oder "Benutzerdefinierte Rollen definieren"
- "Mit Rollen und Benutzern arbeiten"

## NFS-Exportrichtlinien verwalten

Trident verwendet NFS-Exportregeln, um den Zugriff auf die Volumes zu steuern, die es bereitstellt.

Trident bietet zwei Optionen für die Arbeit mit Exportrichtlinien:

- Trident kann die Exportregel dynamisch selbst verwalten; in diesem Betriebsmodus gibt der Speicheradministrator eine Liste von CIDR-Blöcken an, die zulässige IP-Adressen repräsentieren. Trident fügt anwendbare Knoten-IPs, die in diese Bereiche fallen, der Exportregel beim Veröffentlichen automatisch hinzu. Alternativ, wenn keine CIDRs angegeben werden, werden alle globalen Unicast-IPs, die auf dem Knoten gefunden werden, auf den das Volume veröffentlicht wird, zur Exportregel hinzugefügt.
- Speicheradministratoren können eine Exportregel erstellen und Regeln manuell hinzufügen. Trident verwendet die Standard-Exportregel, sofern in der Konfiguration kein anderer Name für die Exportregel angegeben ist.

### Exportregeln dynamisch verwalten

Trident bietet die Möglichkeit, Exportregeln für ONTAP-Backends dynamisch zu verwalten. Dadurch erhält der Speicheradministrator die Möglichkeit, einen zulässigen Adressraum für Worker-Knoten-IPs anzugeben, anstatt explizite Regeln manuell zu definieren. Dies vereinfacht die Verwaltung der Exportregel erheblich; Änderungen an der Exportregel erfordern keine manuelle Intervention mehr am Storage-Cluster. Außerdem hilft dies, den Zugriff auf den Storage-Cluster nur auf Worker-Knoten zu beschränken, die Volumes einbinden und deren IPs im angegebenen Bereich liegen, was eine feingranulare und automatisierte Verwaltung unterstützt.

> Verwenden Sie keine Netzwerkadressübersetzung (NAT), wenn Sie dynamische Exportregeln verwenden. Mit NAT sieht der Speicherkontroller die Frontend-NAT-Adresse und nicht die tatsächliche IP-Hostadresse, sodass der Zugriff verweigert wird, wenn in den Exportregeln keine Übereinstimmung gefunden wird.

#### Beispiel

Es gibt zwei Konfigurationsoptionen, die verwendet werden müssen. Hier ist ein Beispiel für eine Backend-Definition:

```
---
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
```

> Bei Verwendung dieser Funktion müssen Sie sicherstellen, dass die Root-Verbindung in Ihrer SVM über eine zuvor erstellte Exportregel verfügt, die den CIDR-Block des Knotens zulässt (wie z. B. die Standard-Exportregel). Befolgen Sie stets die von NetApp empfohlenen Best Practices, um eine SVM für Trident zu dedizieren.

Hier ist eine Erklärung, wie diese Funktion anhand des obigen Beispiels funktioniert:

- `autoExportPolicy` ist auf `true` gesetzt. Dies bedeutet, dass Trident für jedes mit diesem Backend

bereitgestellte Volume für die `svm1` SVM eine Exportregel erstellt und das Hinzufügen sowie Löschen von Regeln mithilfe von `autoexportCIDRs` Adressblöcken verwaltet. Solange ein Volume nicht an einen Knoten angehängt ist, verwendet das Volume eine leere Exportregel ohne Regeln, um unerwünschten Zugriff auf dieses Volume zu verhindern. Wenn ein Volume auf einem Knoten veröffentlicht wird, erstellt Trident eine Exportregel mit demselben Namen wie der zugrunde liegende qtree, der die Knoten-IP innerhalb des angegebenen CIDR-Blocks enthält. Diese IPs werden auch der Exportregel hinzugefügt, die vom übergeordneten FlexVol volume verwendet wird.

  - Beispiel:
    - Backend-UUID 403b5326-8482-40db-96d0-d83fb3f4daec
    - `autoExportPolicy` eingestellt auf `true`
    - Speicherpräfix `trident`
    - PVC UUID a79bcf5f-7b6d-4a40-9876-e2551f159c1c
    - Der Qtree mit dem Namen trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c erstellt eine Exportrichtlinie für das FlexVol mit dem Namen `trident-403b5326-8482-40db96d0-d83fb3f4daec`, eine Exportrichtlinie für den Qtree mit dem Namen `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c` und eine leere Exportrichtlinie mit dem Namen `trident_empty` auf dem SVM. Die Regeln der FlexVol-Exportrichtlinie bilden eine Obermenge aller in den Qtree-Exportrichtlinien enthaltenen Regeln. Die leere Exportrichtlinie wird von allen nicht angehängten Volumes wiederverwendet.

- `autoExportCIDRs` enthält eine Liste von Adressblöcken. Dieses Feld ist optional und hat standardmäßig den Wert ["0.0.0.0/0", "::/0"]. Falls nicht definiert, fügt Trident alle global gültigen Unicast-Adressen hinzu, die auf den Worker-Knoten mit Veröffentlichungen gefunden wurden.

In diesem Beispiel wird der `192.168.0.0/24` Adressraum bereitgestellt. Dies bedeutet, dass Kubernetes-Knoten-IPs, die in diesen Adressbereich fallen und Veröffentlichungen enthalten, der von Trident erstellten Exportregel hinzugefügt werden. Wenn Trident einen Knoten registriert, auf dem es ausgeführt wird, ruft es die IP-Adressen des Knotens ab und prüft sie anhand der in `autoExportCIDRs` bereitgestellten Adressblöcke. Zum Veröffentlichungszeitpunkt erstellt Trident nach dem Filtern der IPs die Exportregel für die Client-IPs des Knotens, auf den veröffentlicht wird.

Sie können `autoExportPolicy` und `autoExportCIDRs` für Backends nach deren Erstellung aktualisieren. Sie können neue CIDRs für ein automatisch verwaltetes Backend hinzufügen oder bestehende CIDRs löschen. Gehen Sie beim Löschen von CIDRs vorsichtig vor, um sicherzustellen, dass bestehende Verbindungen nicht getrennt werden. Sie können auch wählen, `autoExportPolicy` für ein Backend zu deaktivieren und auf eine manuell erstellte Exportrichtlinie zurückzugreifen. Dies erfordert das Setzen des `exportPolicy` Parameters in Ihrer Backend-Konfiguration.

Nachdem Trident ein Backend erstellt oder aktualisiert hat, können Sie das Backend mit `tridentctl` oder der entsprechenden `tridentbackend` CRD überprüfen:

```
./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
```

Wenn ein Knoten entfernt wird, überprüft Trident alle Exportregeln, um die Zugriffsregeln zu entfernen, die dem Knoten entsprechen. Durch das Entfernen dieser Knoten-IP aus den Exportregeln der verwalteten Backends verhindert Trident unerwünschte Einbindungen, es sei denn, diese IP wird von einem neuen Knoten im Cluster wiederverwendet.

Bei bereits vorhandenen Backends stellt die Aktualisierung des Backends mit `tridentctl update backend` sicher, dass Trident die Exportregeln automatisch verwaltet. Dabei werden bei Bedarf zwei neue Exportregeln erstellt, die nach der UUID und dem Qtree-Namen des Backends benannt sind. Volumes, die auf dem Backend vorhanden sind, verwenden nach dem Aushängen und erneuten Einhängen die neu erstellten Exportregeln.

> Das Löschen eines Backends mit automatisch verwalteten Exportregeln löscht die dynamisch erstellte Exportregel. Wenn das Backend neu erstellt wird, wird es als neues Backend behandelt und führt zur Erstellung einer neuen Exportregel.

Wird die IP-Adresse eines aktiven Knotens geändert, muss der Trident Pod auf dem Knoten neu gestartet werden. Trident aktualisiert anschließend die Exportregel für die von ihm verwalteten Backends, um diese IP-Änderung widerzuspiegeln.

## Bereiten Sie die Bereitstellung von SMB-Volumes vor

Mit ein wenig zusätzlicher Vorbereitung können Sie SMB-Volumes mit `ontap-nas` Treibern bereitstellen.

> Sie müssen sowohl das NFS- als auch das SMB/CIFS-Protokoll auf der SVM konfigurieren, um ein `ontap-nas-economy` SMB-Volume für ONTAP On-Premises-Cluster zu erstellen. Wenn eines dieser Protokolle nicht konfiguriert ist, schlägt die Erstellung des SMB-Volumes fehl.

`autoExportPolicy` is not supported for SMB-Volumes.

**Bevor Sie beginnen**

Bevor Sie SMB-Volumes bereitstellen können, müssen Sie Folgendes haben.

- Ein Kubernetes-Cluster mit einem Linux-Controller-Knoten und mindestens einem Windows-Worker-Knoten, auf dem Windows Server 2022 läuft. Trident unterstützt SMB-Volumes nur, wenn sie in Pods eingebunden sind, die auf Windows-Knoten ausgeführt werden.
- Mindestens ein Trident secret, das Ihre Active Directory-Anmeldeinformationen enthält. Um ein secret zu generieren `smbcreds`:

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

- Ein als Windows-Dienst konfigurierter CSI-Proxy. Um einen `csi-proxy` zu konfigurieren, siehe "GitHub: CSI Proxy" oder "GitHub: CSI-Proxy für Windows" für Kubernetes-Knoten, die unter Windows laufen.

**Schritte**

1. Für On-Premises ONTAP können Sie optional eine SMB-Freigabe erstellen oder Trident kann eine für Sie erstellen.

   SMB-Shares sind für Amazon FSx for ONTAP erforderlich.

   Sie können die SMB-Administratorfreigaben auf zwei Arten erstellen: entweder mit dem "Microsoft Management Console" Shared Folders Snap-In oder mit der ONTAP CLI. Um die SMB-Freigaben mit der ONTAP CLI zu erstellen:

   a. Erstellen Sie bei Bedarf die Verzeichnispfadstruktur für die Freigabe.

      Der `vserver cifs share create` Befehl prüft den in der Option -path beim Erstellen der Freigabe angegebenen Pfad. Wenn der angegebene Pfad nicht existiert, schlägt der Befehl fehl.

   b. Erstellen Sie eine SMB-Freigabe, die dem angegebenen SVM zugeordnet ist:

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

   c. Überprüfen Sie, ob die Freigabe erstellt wurde:

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

   Weitere Einzelheiten finden Sie in "Erstellen Sie eine SMB-Freigabe".

2. Bei der Erstellung des Backends müssen Sie Folgendes konfigurieren, um SMB-Volumes anzugeben. Alle FSx for ONTAP Backend-Konfigurationsoptionen finden Sie unter "FSx for ONTAP Konfigurationsoptionen

und Beispiele".

| Parameter | Beschreibung | Beispiel |
|---|---|---|
| `smbShare` | Sie können eines der folgenden angeben: den Namen einer SMB-Freigabe, die mit der Microsoft Management Console oder ONTAP CLI erstellt wurde; einen Namen, damit Trident die SMB-Freigabe erstellen kann; oder Sie können den Parameter leer lassen, um den gemeinsamen Freigabezugriff auf Volumes zu verhindern. Dieser Parameter ist optional für lokale ONTAP. Dieser Parameter ist für Amazon FSx for ONTAP Backends erforderlich und darf nicht leer sein. | `smb-share` |
| `nasType` | **Muss auf `smb` gesetzt werden.** Wenn null, wird standardmäßig `nfs` verwendet. | `smb` |
| `securityStyle` | Sicherheitsstil für neue Volumes. **Muss auf `ntfs` oder `mixed` für SMB-Volumes eingestellt werden.** | `ntfs` or `mixed` für SMB-Volumes |
| `unixPermissions` | Modus für neue Volumes. **Muss für SMB-Volumes leer bleiben.** | "" |

### Sichere SMB-Verbindungen aktivieren

Ab der Version 25.06 unterstützt NetApp Trident die sichere Bereitstellung von SMB-Volumes, die mit `ontap-nas` und `ontap-nas-economy` Backends erstellt wurden. Wenn Secure SMB aktiviert ist, können Sie Active Directory (AD)-Benutzern und -Benutzergruppen mithilfe von Zugriffssteuerungslisten (ACLs) kontrollierten Zugriff auf die SMB-Freigaben gewähren.

#### Wichtige Punkte

- Das Importieren `ontap-nas-economy` von Volumes wird nicht unterstützt.
- Es werden nur schreibgeschützte Klone für `ontap-nas-economy` volumes unterstützt.
- Wenn Secure SMB aktiviert ist, ignoriert Trident die im Backend angegebene SMB-Freigabe.
- Das Aktualisieren der PVC-Annotation, der Speicherklassenannotation und des Backend-Felds aktualisiert nicht die SMB share ACL.
- Die in der Annotation des Klon-PVC angegebene SMB-Share-ACL hat Vorrang vor denen im Quell-PVC.
- Stellen Sie sicher, dass Sie gültige AD-Benutzer angeben, wenn Sie sicheres SMB aktivieren. Ungültige Benutzer werden nicht zur ACL hinzugefügt.
- Wenn Sie dem gleichen AD-Benutzer im Backend, in der Speicherklasse und im PVC unterschiedliche Berechtigungen zuweisen, ist die Berechtigungspriorität: PVC, Speicherklasse und dann Backend.
- Secure SMB wird für `ontap-nas`managed Volume-Importe unterstützt und ist für unmanaged Volume-Importe nicht anwendbar.

#### Schritte

1. Geben Sie adAdminUser in TridentBackendConfig wie im folgenden Beispiel an:

```
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. Fügen Sie die Annotation in die Speicherklasse ein.

   Fügen Sie die `trident.netapp.io/smbShareAdUser` Annotation zur Storage Class hinzu, um sicheres SMB ohne Fehler zu aktivieren. Der für die Annotation `trident.netapp.io/smbShareAdUser` angegebene Benutzerwert sollte derselbe sein wie der im `smbcreds` Secret angegebene Benutzername. Sie können eines der folgenden für `smbShareAdUserPermission` auswählen: `full_control`, `change` oder `read`. Die Standardberechtigung ist `full_control`.

```
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. Erstellen Sie ein PVC.

   Das folgende Beispiel erstellt eine PVC:

```
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-Konfigurationsoptionen und Beispiele

Lernen Sie, wie Sie ONTAP NAS-Treiber mit Ihrer Trident-Installation erstellen und verwenden. Dieser Abschnitt enthält Beispiele für die Backend-Konfiguration und Details zur Zuordnung von Backends zu StorageClasses. Ab der Version 25.10 unterstützt NetApp Trident "NetApp AFX-Speichersysteme". NetApp AFX-Speichersysteme unterscheiden sich von anderen ONTAP-basierten Systemen (ASA, AFF und FAS) in der Implementierung ihrer Speicherschicht.

Nur der `ontap-nas` Treiber (mit NFS-Protokoll) wird für NetApp AFX-Systeme unterstützt; das SMB-Protokoll wird nicht unterstützt.

## Backend-Konfigurationsoptionen

In der Trident-Backend-Konfiguration müssen Sie nicht angeben, dass Ihr System ein NetApp AFX-Speichersystem ist. Wenn Sie `ontap-nas` als `storageDriverName` auswählen, erkennt Trident das AFX-Speichersystem automatisch. Einige Backend-Konfigurationsparameter sind für AFX-Speichersysteme nicht anwendbar.

Die folgende Tabelle zeigt die Backend-Konfigurationsoptionen:

| Parameter | Beschreibung | Standard |
|---|---|---|
| `version` | | Immer 1 |

| Parameter | Beschreibung | Standard |
| --- | --- | --- |
| `storageDriverName` | Name des Speichertreibers<br>Für NetApp AFX-Systeme wird nur `ontap-nas` unterstützt. | `ontap-nas`, `ontap-nas-economy`, oder `ontap-nas-flexgroup` |
| `backendName` | Benutzerdefinierter Name oder das Speicher-Backend | Treibername + "_" + dataLIF |
| `managementLIF` | IP-Adresse eines Clusters oder einer SVM-Management-LIF. Ein vollqualifizierter Domänenname (FQDN) kann angegeben werden. Kann so eingestellt werden, dass IPv6-Adressen verwendet werden, wenn Trident mit dem IPv6-Flag installiert wurde. IPv6-Adressen müssen in eckigen Klammern angegeben werden, wie `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]`. Für einen reibungslosen MetroCluster-Switchover siehe MetroCluster Beispiel. | "10.0.0.1", "[2001:1234:abcd::fefe]" |
| `dataLIF` | IP-Adresse des Protokoll-LIF. NetApp empfiehlt, `dataLIF` anzugeben. Falls nicht angegeben, ruft Trident dataLIFs vom SVM ab. Ein vollqualifizierter Domainname (FQDN) kann für die NFS-Mount-Operationen angegeben werden, wodurch die Erstellung eines Round-Robin-DNS zur Lastverteilung über mehrere dataLIFs ermöglicht wird. Kann nach der Ersteinrichtung geändert werden. Siehe . Kann so eingestellt werden, dass IPv6-Adressen verwendet werden, wenn Trident mit dem IPv6-Flag installiert wurde. IPv6-Adressen müssen in eckigen Klammern angegeben werden, wie `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]`. **Für MetroCluster weglassen.** Siehe MetroCluster Beispiel. | Angegebene Adresse oder abgeleitet von SVM, falls nicht angegeben (nicht empfohlen) |
| `svm` | Zu verwendende virtuelle Speichermaschine **Für MetroCluster auslassen.** Siehe MetroCluster Beispiel. | Wird abgeleitet, wenn eine SVM `managementLIF` angegeben ist |
| `autoExportPolicy` | Automatische Erstellung und Aktualisierung von Exportrichtlinien aktivieren [Boolean]. Mit den Optionen `autoExportPolicy` und `autoExportCIDRs` kann Trident Exportrichtlinien automatisch verwalten. | false |
| `autoExportCIDRs` | Liste der CIDRs, anhand derer die Node-IPs von Kubernetes gefiltert werden, wenn `autoExportPolicy` aktiviert ist. Mit den Optionen `autoExportPolicy` und `autoExportCIDRs` kann Trident Exportrichtlinien automatisch verwalten. | ["0.0.0.0/0", "::/0"]` |
| `labels` | Satz beliebiger JSON-formatierter Bezeichnungen, die auf Volumes angewendet werden sollen | "" |

| Parameter | Beschreibung | Standard |
| --- | --- | --- |
| `clientCertificate` | Base64-kodierter Wert des Clientzertifikats. Wird für zertifikatbasierte Authentifizierung verwendet | "" |
| `clientPrivateKey` | Base64-kodierter Wert des privaten Client-Schlüssels. Wird für zertifikatbasierte Authentifizierung verwendet | "" |
| `trustedCACertificate` | Base64-kodierter Wert des vertrauenswürdigen CA-Zertifikats. Optional. Wird für zertifikatbasierte Authentifizierung verwendet | "" |
| `username` | Benutzername für die Verbindung zum Cluster/SVM. Wird für die anmeldeinformationsbasierte Authentifizierung verwendet. Für die Active Directory Authentifizierung siehe "Authentifizieren Sie Trident bei einer Backend-SVM mit Active Directory-Anmeldeinformationen". | |
| `password` | Passwort für die Verbindung zum Cluster/SVM. Wird für die anmeldeinformationsbasierte Authentifizierung verwendet. Für die Active Directory Authentifizierung siehe "Authentifizieren Sie Trident bei einer Backend-SVM mit Active Directory-Anmeldeinformationen". | |
| `storagePrefix` | Präfix, das beim Bereitstellen neuer Volumes in der SVM verwendet wird. Kann nach der Festlegung nicht mehr geändert werden.<br><br>Bei Verwendung von ontap-nas-economy und einem storagePrefix, der 24 oder mehr Zeichen umfasst, wird das Speicherpräfix nicht in die Qtrees eingebettet, obwohl es im Volume-Namen enthalten ist. | "Trident" |

| Parameter | Beschreibung | Standard |
| --- | --- | --- |
| `aggregate` | Aggregat für die Bereitstellung (optional; falls festgelegt, muss es der SVM zugewiesen werden). Für den `ontap-nas-flexgroup` Treiber wird diese Option ignoriert. Wenn nicht zugewiesen, kann eines der verfügbaren Aggregate zur Bereitstellung eines FlexGroup Volumes verwendet werden.<br><br>Wird das Aggregat in SVM aktualisiert, wird es in Trident automatisch durch Abfragen von SVM aktualisiert, ohne dass der Trident Controller neu gestartet werden muss. Wenn Sie in Trident ein bestimmtes Aggregat für die Bereitstellung von Volumes konfiguriert haben und dieses Aggregat umbenannt oder aus der SVM verschoben wird, wechselt das Backend in Trident beim Abfragen des SVM-Aggregats in den Fehlerzustand. Sie müssen entweder das Aggregat auf eines ändern, das auf der SVM vorhanden ist, oder es vollständig entfernen, um das Backend wieder online zu bringen.<br><br>**Nicht für AFX storage systems angeben.** | "" |
| `limitAggregateUsage` | Die Bereitstellung schlägt fehl, wenn die Nutzung diesen Prozentsatz überschreitet. **Gilt nicht für Amazon FSx for ONTAP**. **Nicht für AFX storage systems angeben.** | "" (wird nicht standardmäßig erzwungen) |

| Parameter | Beschreibung | Standard |
| --- | --- | --- |
| flexgroupAggregateList | Liste der Aggregate für die Bereitstellung (optional; falls festgelegt, muss sie der SVM zugewiesen werden). Alle Aggregate, die der SVM zugewiesen sind, werden zur Bereitstellung eines FlexGroup-Volumes verwendet. Unterstützt für den **ontap-nas-flexgroup**-Speichertreiber.<br><br>Wird die Aggregatliste in SVM aktualisiert, wird sie in Trident automatisch durch Abfrage von SVM aktualisiert, ohne dass der Trident Controller neu gestartet werden muss. Wenn Sie in Trident eine bestimmte Aggregatliste für die Volume-Bereitstellung konfiguriert haben und diese Aggregatliste umbenannt oder aus SVM verschoben wird, wechselt das Backend in Trident beim Abfragen der SVM-Aggregatliste in den Fehlerzustand. Sie müssen entweder die Aggregatliste auf eine ändern, die in SVM vorhanden ist, oder sie vollständig entfernen, um das Backend wieder online zu bringen. | "" |
| `limitVolumeSize` | Die Bereitstellung schlägt fehl, wenn die angeforderte Volume-Größe diesen Wert überschreitet. | "" (wird nicht standardmäßig erzwungen) |
| `debugTraceFlags` | Debug-Flags zur Verwendung bei der Fehlersuche. Beispiel, {"api":false, "method":true} Verwenden Sie `debugTraceFlags` nicht, es sei denn, Sie führen eine Fehlersuche durch und benötigen eine detaillierte Protokollausgabe. | null |
| `nasType` | Konfigurieren Sie die Erstellung von NFS- oder SMB-Volumes. Optionen sind `nfs`, `smb` oder null. Die Einstellung auf null verwendet standardmäßig NFS-Volumes. **Falls angegeben, immer auf `nfs` für AFX-Speichersysteme setzen.** | `nfs` |
| `nfsMountOptions` | Kommagetrennte Liste von NFS-Mountoptionen. Die Mountoptionen für persistente Kubernetes-Volumes werden normalerweise in Speicherklassen angegeben, aber wenn keine Mountoptionen in einer Speicherklasse angegeben sind, verwendet Trident die Mountoptionen, die in der Konfigurationsdatei des Storage-Backends angegeben sind. Wenn weder in der Speicherklasse noch in der Konfigurationsdatei Mountoptionen angegeben sind, setzt Trident keine Mountoptionen für das zugehörige persistente Volume. | "" |

| Parameter | Beschreibung | Standard |
| --- | --- | --- |
| `qtreesPerFlexvol` | Maximale Qtrees pro FlexVol, muss im Bereich [50, 300] liegen | "200" |
| `smbShare` | Sie können eines der folgenden angeben: den Namen einer SMB-Freigabe, die mit der Microsoft Management Console oder ONTAP CLI erstellt wurde; einen Namen, damit Trident die SMB-Freigabe erstellen kann; oder Sie können den Parameter leer lassen, um den gemeinsamen Freigabezugriff auf Volumes zu verhindern. Dieser Parameter ist optional für lokale ONTAP. Dieser Parameter ist für Amazon FSx for ONTAP Backends erforderlich und darf nicht leer sein. | `smb-share` |
| `useREST` | Boolescher Parameter zur Verwendung von ONTAP REST APIs. `useREST` Wenn auf `true` gesetzt, verwendet Trident ONTAP REST APIs zur Kommunikation mit dem Backend; wenn auf `false` gesetzt, verwendet Trident ONTAPI (ZAPI)-Aufrufe zur Kommunikation mit dem Backend. Diese Funktion erfordert ONTAP 9.11.1 und höher. Zusätzlich muss die verwendete ONTAP-Anmelderolle Zugriff auf die `ontapi` Anwendung haben. Dies wird durch die vordefinierten `vsadmin` und `cluster-admin` Rollen erfüllt. Ab der Trident 24.06-Version und ONTAP 9.15.1 oder höher ist `useREST` standardmäßig auf `true` gesetzt; ändern Sie `useREST` auf `false`, um ONTAPI (ZAPI)-Aufrufe zu verwenden. **Falls angegeben, immer auf `true` für AFX-Speichersysteme setzen.** | `true` für ONTAP 9.15.1 oder höher, andernfalls `false`. |
| `limitVolumePoolSize` | Maximal anforderbare FlexVol-Größe bei Verwendung von Qtrees im ontap-nas-economy Backend. | "" (wird nicht standardmäßig erzwungen) |
| `denyNewVolumePools` | Beschränkt `ontap-nas-economy` Backends darauf, neue FlexVol Volumes zu erstellen, um ihre Qtrees zu enthalten. Nur bereits vorhandene Flexvols werden für die Bereitstellung neuer PVs verwendet. | |
| `adAdminUser` | Active Directory-Administratorbenutzer oder -Benutzergruppe mit vollem Zugriff auf SMB-Freigaben. Verwenden Sie diesen Parameter, um Administratorrechte für die SMB-Freigabe mit vollständiger Kontrolle zu erteilen. | |

## Backend-Konfigurationsoptionen für die Bereitstellung von Volumes

Sie können die Standardbereitstellung mithilfe dieser Optionen im `defaults` Abschnitt der Konfiguration steuern. Ein Beispiel finden Sie in den unten stehenden Konfigurationsbeispielen.

| Parameter | Beschreibung | Standard |
|---|---|---|
| `spaceAllocation` | Speicherplatzzuweisung für Qtrees | "true" |
| `spaceReserve` | Platzreservierungsmodus; "none" (dünn) oder "volume" (dick) | "none" |
| `snapshotPolicy` | Zu verwendende Snapshot-Richtlinie | "none" |
| `qosPolicy` | QoS-Richtliniengruppe, die für erstellte Volumes zugewiesen werden soll. Wählen Sie eine der qosPolicy oder adaptiveQosPolicy pro Speicherpool/Backend aus. | "" |
| `adaptiveQosPolicy` | Adaptive QoS-Richtliniengruppe zur Zuweisung für erstellte Volumes. Wählen Sie eine von qosPolicy oder adaptiveQosPolicy pro Storage-Pool/Backend. Wird von ontap-nas-economy nicht unterstützt. | "" |
| `snapshotReserve` | Prozentsatz des für Snapshots reservierten Volumens | "0", falls `snapshotPolicy`"none", andernfalls "" |
| `splitOnClone` | Trennen Sie einen Klon bei seiner Erstellung von seinem übergeordneten Objekt | "false" |
| `encryption` | Aktivieren Sie NetApp Volume Encryption (NVE) auf dem neuen Volume; Standard ist `false`. NVE muss auf dem Cluster lizenziert und aktiviert sein, um diese Option zu verwenden. Wenn NAE im Backend aktiviert ist, wird jedes in Trident bereitgestellte Volume NAE-aktiviert. Weitere Informationen finden Sie unter: "Wie Trident mit NVE und NAE zusammenarbeitet". | "false" |
| `tieringPolicy` | Tiering-Richtlinie auf "none" setzen | |
| `unixPermissions` | Modus für neue Volumes | "777" für NFS-Volumes; leer (nicht zutreffend) für SMB-Volumes |
| `snapshotDir` | Steuert den Zugriff auf das `.snapshot` Verzeichnis | `true`, `false` (explizit festlegen). |
| `exportPolicy` | Zu verwendende Exportrichtlinie | "default" |
| `securityStyle` | Sicherheitsstil für neue Volumes. NFS unterstützt `mixed` und `unix` Sicherheitsstile. SMB unterstützt `mixed` und `ntfs` Sicherheitsstile. | NFS-Standard ist `unix`. SMB-Standard ist `ntfs`. |
| `nameTemplate` | Vorlage zum Erstellen benutzerdefinierter Volume-Namen. | "" |

Die Verwendung von QoS-Richtliniengruppen mit Trident erfordert ONTAP 9.8 oder höher. Sie sollten eine nicht gemeinsam genutzte QoS-Richtliniengruppe verwenden und sicherstellen, dass die Richtliniengruppe auf jede Komponente einzeln angewendet wird. Eine gemeinsam genutzte QoS-Richtliniengruppe erzwingt die Obergrenze für den Gesamtdurchsatz aller Workloads.

#### Beispiele für die Volume-Bereitstellung

Hier ist ein Beispiel mit definierten Standardwerten:

```
---
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"
```

Für `ontap-nas` und `ontap-nas-flexgroups` verwendet Trident nun eine neue Berechnung, um sicherzustellen, dass die FlexVol mit dem snapshotReserve-Prozentsatz und dem PVC korrekt dimensioniert ist. Wenn der Benutzer einen PVC anfordert, erstellt Trident das ursprüngliche FlexVol mit mehr Speicherplatz mithilfe der neuen Berechnung. Diese Berechnung stellt sicher, dass der Benutzer den beschreibbaren Speicherplatz erhält, den er im PVC angefordert hat, und nicht weniger als angefordert. Vor v21.07, wenn der Benutzer einen PVC anfordert (zum Beispiel 5 GiB) und der snapshotReserve auf 50 Prozent gesetzt ist, erhält er nur 2,5 GiB beschreibbaren Speicherplatz. Dies liegt daran, dass das, was der Benutzer anfordert, das gesamte Volume ist und `snapshotReserve` ein Prozentsatz davon ist. Mit Trident 21.07 ist das, was der Benutzer anfordert, der beschreibbare Speicherplatz, und Trident definiert die `snapshotReserve` Zahl als Prozentsatz des gesamten Volumens. Dies gilt nicht für `ontap-nas-economy`. Siehe das folgende Beispiel, um zu sehen, wie dies funktioniert:

Die Berechnung erfolgt wie folgt:

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

Für snapshotReserve = 50 %, und eine PVC-Anforderung = 5 GiB, beträgt die Gesamtgröße des Volumes

5/0,5 = 10 GiB und die verfügbare Größe 5 GiB, was der vom Benutzer in der PVC-Anforderung angeforderten Größe entspricht. Der `volume show`-Befehl sollte Ergebnisse ähnlich diesem Beispiel anzeigen:


Vorhandene Backends aus früheren Installationen werden beim Upgrade von Trident Volumes wie oben beschrieben bereitstellen. Für Volumes, die Sie vor dem Upgrade erstellt haben, sollten Sie deren Größe anpassen, damit die Änderung wirksam wird. Beispielsweise führte ein 2-GiB-PVC mit `snapshotReserve=50` zuvor zu einem Volume, das 1 GiB beschreibbaren Speicherplatz bereitstellt. Durch die Größenänderung des Volumes auf beispielsweise 3 GiB erhält die Anwendung 3 GiB beschreibbaren Speicherplatz auf einem 6-GiB-Volume.

## Minimale Konfigurationsbeispiele

Die folgenden Beispiele zeigen Basiskonfigurationen, bei denen die meisten Parameter auf Standardwerte eingestellt sind. Dies ist die einfachste Methode, ein Backend zu definieren.

> Wenn Sie Amazon FSx auf NetApp ONTAP mit Trident verwenden, wird empfohlen, für LIFs DNS-Namen anstelle von IP-Adressen anzugeben.

**ONTAP NAS economy Beispiel**

```
---
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-Beispiel

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

#### MetroCluster Beispiel

Sie können das Backend so konfigurieren, dass Sie die Backend-Definition nach einem Switchover und Switchback während "SVM-Replikation und -Wiederherstellung" nicht manuell aktualisieren müssen.

Für einen nahtlosen Switchover und Switchback geben Sie die SVM mit `managementLIF` an und lassen Sie die `dataLIF` und `svm` Parameter weg. Beispiel:

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

#### Beispiel für SMB-Volumes

```
---
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
```

#### Beispiel für zertifikatsbasierte Authentifizierung

Dies ist ein minimales Beispiel für eine Backend-Konfiguration. `clientCertificate`, `clientPrivateKey` und `trustedCACertificate` (optional, falls eine vertrauenswürdige Zertifizierungsstelle verwendet wird) werden in `backend.json` befüllt und nehmen die Base64-kodierten Werte des Clientzertifikats, des privaten Schlüssels und des Zertifikats der vertrauenswürdigen Zertifizierungsstelle an.

```
---
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_
```

#### Beispiel für eine automatische Exportrichtlinie

Dieses Beispiel zeigt Ihnen, wie Sie Trident anweisen können, dynamische Exportrichtlinien zu verwenden, um die Exportrichtlinie automatisch zu erstellen und zu verwalten. Dies funktioniert gleichermaßen für die `ontap-nas-economy` und `ontap-nas-flexgroup` Treiber.

```
---
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
```

#### Beispiel für IPv6 addresses

Dieses Beispiel zeigt `managementLIF` die Verwendung einer IPv6-Adresse.

```
---
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
```

#### Amazon FSx für ONTAP mit SMB-Volumes Beispiel

Der `smbShare` Parameter ist für FSx for ONTAP mit SMB-Volumes erforderlich.

```
---
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_
```

**Beispiel für die Backend-Konfiguration mit nameTemplate**

```
---
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}}"
```

## Beispiele für Backends mit virtuellen Pools

In den unten gezeigten Beispiel-Backend-Definitionsdateien sind für alle Speicherpools spezifische Standardwerte festgelegt, wie `spaceReserve` bei none, `spaceAllocation` bei false und `encryption` bei false. Die virtuellen Pools werden im Speicherabschnitt definiert.

Trident legt Bereitstellungsbezeichnungen im Feld „Kommentare“ fest. Kommentare werden auf FlexVol für `ontap-nas` oder auf FlexGroup für `ontap-nas-flexgroup` festgelegt. Trident kopiert alle auf einem virtuellen Pool vorhandenen Bezeichnungen bei der Bereitstellung auf das Speichervolume. Zur Vereinfachung können Speicheradministratoren Bezeichnungen pro virtuellem Pool definieren und Volumes nach Bezeichnung gruppieren.

In diesen Beispielen legen einige Speicherpools ihre eigenen `spaceReserve`, `spaceAllocation`, und `encryption` Werte fest, und einige Pools überschreiben die Standardwerte.

**ONTAP NAS-Beispiel**

```
---
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 Beispiel**

```
---
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 economy Beispiel**

```
---
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"
```

## Backends zu StorageClasses zuordnen

Die folgenden StorageClass-Definitionen beziehen sich auf Beispiele für Backends mit virtuellen Pools. Mithilfe des `parameters.selector`-Feldes gibt jede StorageClass an, welche virtuellen Pools zum Hosten eines Volumes verwendet werden können. Das Volume weist die im gewählten virtuellen Pool definierten Aspekte auf.

- Die `protection-gold` StorageClass wird dem ersten und zweiten virtuellen Pool im `ontap-nas-flexgroup` Backend zugeordnet. Diese sind die einzigen Pools, die Schutz auf Goldniveau bieten.

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

- Die `protection-not-gold` StorageClass wird dem dritten und vierten virtuellen Pool im `ontap-nas-flexgroup` Backend zugeordnet. Dies sind die einzigen Pools, die ein anderes Schutzniveau als Gold bieten.

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

- Die `app-mysqldb` StorageClass wird dem vierten virtuellen Pool im `ontap-nas` Backend zugeordnet. Dies ist der einzige Pool, der eine Speicherpoolkonfiguration für mysqldb Typ App bietet.

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

- Der `protection-silver-creditpoints-20k` StorageClass wird dem dritten virtuellen Pool im `ontap-nas-flexgroup` Backend zugeordnet. Dies ist der einzige Pool, der Schutz auf Silber-Niveau und 20000 Kreditpunkte bietet.

```
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"
```

- Die `creditpoints-5k` StorageClass wird dem dritten virtuellen Pool im `ontap-nas` Backend und dem zweiten virtuellen Pool im `ontap-nas-economy` Backend zugeordnet. Dies sind die einzigen Poolangebote mit 5000 Kreditpunkten.

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

Trident entscheidet, welcher virtuelle Pool ausgewählt wird und stellt sicher, dass die Speicheranforderung erfüllt wird.

## Aktualisieren `dataLIF` nach der Erstkonfiguration

Sie können die dataLIF nach der Erstkonfiguration ändern, indem Sie den folgenden Befehl ausführen, um die neue Backend-JSON-Datei mit der aktualisierten dataLIF bereitzustellen.

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

Wenn PVCs an einem oder mehreren Pods angeschlossen sind, müssen Sie alle entsprechenden Pods herunterfahren und anschließend wieder hochfahren, damit die neue dataLIF wirksam wird.

## Beispiele für sicheres SMB

### Backend-Konfiguration mit dem ontap-nas-Treiber

```
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
```

### Backend-Konfiguration mit ontap-nas-economy-Treiber

```
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
```

**Backend-Konfiguration mit Speicherpool**

```
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
```

**Speicherklassenbeispiel mit dem ontap-nas-Treiber**

```
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
```

Stellen Sie sicher, dass Sie `annotations` hinzufügen, um Secure SMB zu aktivieren. Secure SMB funktioniert ohne die Annotationen nicht, unabhängig von den im Backend oder PVC festgelegten Konfigurationen.

**Speicherklassenbeispiel mit ontap-nas-economy-Treiber**

```
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
```

**PVC-Beispiel mit einem einzelnen AD-Benutzer**

```
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
```

**PVC-Beispiel mit mehreren AD-Benutzern**

```
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
```