ONTAP NAS-Treiber

Trident

NetApp
January 15, 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 zur Verfügung, um mit dem ONTAP Cluster zu kommunizieren. Unterstützte Zugriffsmodi sind: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

Treiber	Protokoll	Lautstärke modus	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 `ontap-san-economy` nur wenn die Anzahl der dauerhaften Speichernutzungen voraussichtlich höher sein wird als"Unterstützte ONTAP Lautstärkebegrenzungen" .
- Verwenden `ontap-nas-economy` nur wenn die Anzahl der dauerhaften Speichernutzungen voraussichtlich höher sein wird als"Unterstützte ONTAP Lautstärkebegrenzungen" und die `ontap-san-economy` Der Treiber kann nicht verwendet werden.
- Nicht verwenden `ontap-nas-economy` wenn Sie mit einem Bedarf an Datenschutz, Notfallwiederherstellung oder Mobilität rechnen.
- NetApp empfiehlt die Verwendung von Flexvol Autogrow nicht in allen ONTAP -Treibern, außer ontap-san. Als Ausweichlösung unterstützt Trident die Verwendung von Snapshot-Reserven und skaliert Flexvol-Volumes entsprechend.

Benutzerberechtigungen

Trident wird voraussichtlich entweder als ONTAP oder SVM-Administrator ausgeführt, typischerweise unter Verwendung von `admin` Clusterbenutzer oder ein `vsadmin` SVM-Benutzer oder ein Benutzer mit einem anderen Namen, der die gleiche Rolle hat.

Bei Amazon FSx for NetApp ONTAP Bereitstellungen erwartet Trident , dass es entweder als ONTAP oder SVM-Administrator ausgeführt wird und den Cluster nutzt. `fsxadmin` Benutzer oder ein `vsadmin` SVM-Benutzer oder ein Benutzer mit einem anderen Namen, der die gleiche Rolle hat. Der `fsxadmin` Der Benutzer ist ein eingeschränkter Ersatz für den Cluster-Administratorbenutzer.

Wenn Sie die `limitAggregateUsage` Für diesen Parameter sind Cluster-Administratorrechte erforderlich. Bei der Verwendung von Amazon FSx for NetApp ONTAP mit Trident `limitAggregateUsage` Der Parameter funktioniert nicht mit dem `vsadmin` Und `fsxadmin` Benutzerkonten. Die Konfiguration schlägt fehl, wenn Sie diesen Parameter angeben.

Es ist zwar möglich, innerhalb von ONTAP eine restriktivere Rolle zu erstellen, die ein Trident -Treiber verwenden kann, wir empfehlen dies jedoch nicht. Die meisten neuen Versionen von Trident werden zusätzliche APIs aufrufen, die berücksichtigt werden müssen, was Aktualisierungen schwierig und fehleranfällig macht.

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

Machen Sie sich mit den Anforderungen, Authentifizierungsoptionen und Exportrichtlinien für die Konfiguration eines ONTAP Backends mit ONTAP -NAS-Treibern vertraut.

Anforderungen

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

Authentifizieren Sie das ONTAP Backend

Trident bietet zwei Modi zur Authentifizierung eines ONTAP Backends.

- Anmeldeinformationsbasiert: Dieser Modus erfordert ausreichende Berechtigungen für das ONTAP Backend. Es wird empfohlen, ein Konto zu verwenden, das einer vordefinierten Sicherheitsanmelderolle zugeordnet ist, wie zum Beispiel `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. Hierbei müssen in der Backend-Definition Base64-kodierte Werte des Client-Zertifikats, des Schlüssels und des vertrauenswürdigen CA-Zertifikats (falls verwendet, empfohlen) enthalten sein.

Sie können bestehende Backends aktualisieren, um zwischen anmeldeinformationsbasierten und zertifikatsbasierten Methoden zu wechseln. Es wird jedoch jeweils nur eine Authentifizierungsmethode unterstützt. Um zu einer anderen Authentifizierungsmethode zu wechseln, müssen Sie die bestehende Methode aus der Backend-Konfiguration entfernen.

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

Aktivieren Sie die anmeldeinformationsbasierte Authentifizierung

Trident benötigt die Anmeldeinformationen eines SVM-/Cluster-Administrators, um mit dem ONTAP Backend zu kommunizieren. Es wird empfohlen, standardisierte, vordefinierte Rollen zu verwenden, wie zum Beispiel `admin` oder `vsadmin` . Dies gewährleistet die Vorwärtskompatibilität mit zukünftigen ONTAP Versionen, die möglicherweise Feature-APIs zur Verwendung durch zukünftige Trident Versionen bereitstellen. Eine benutzerdefinierte Sicherheitsanmelderolle kann erstellt und mit Trident verwendet werden, dies 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 Anmeldeinformationen im Klartext gespeichert werden. Nach der Erstellung des Backends werden Benutzernamen und 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 für Administratoren zulässige Operation, die vom Kubernetes-/Speicheradministrator durchgeführt werden muss.

Zertifikatsbasierte Authentifizierung aktivieren

Neue und bestehende Backends können ein Zertifikat verwenden und mit dem ONTAP Backend kommunizieren. Für die Backend-Definition werden drei Parameter benötigt.

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

Ein typischer Arbeitsablauf umfasst die folgenden Schritte.

Schritte

1. Generieren Sie ein Clientzertifikat und einen Schlüssel. Beim Generieren muss der allgemeine Name (CN) auf den ONTAP Benutzer gesetzt werden, der sich authentifizieren soll.

```
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 könnte bereits vom Speicheradministrator erledigt werden. Ignorieren, falls keine vertrauenswürdige Zertifizierungsstelle 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 die folgenden Funktionen unterstützt: `cert` Authentifizierungsmethode.

```
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-Adresse und den SVM-Namen. Sie müssen sicherstellen, dass die Servicerichtlinie des LIF auf Folgendes eingestellt ist: `default-data-management` .

```
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 ein 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 die Authentifizierungsmethoden oder ändern Sie die Anmeldeinformationen.

Sie können ein bestehendes Backend aktualisieren, um eine andere Authentifizierungsmethode zu verwenden oder um die Anmeldeinformationen zu ändern. Dies funktioniert in beide Richtungen: Backends, die Benutzername/Passwort verwenden, können auf die Verwendung von Zertifikaten umgestellt werden; Backends, die Zertifikate verwenden, können auf Benutzername/Passwort-basiert umgestellt werden. Dazu müssen Sie die bestehende Authentifizierungsmethode entfernen und die neue Authentifizierungsmethode hinzufügen. Verwenden Sie anschließend die aktualisierte Datei backend.json, die die erforderlichen Parameter enthält, um die Ausführung durchzuführen. `tridentctl update backend`.

```
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 Ändern von Passwörtern muss der Speicheradministrator zuerst das Passwort für den Benutzer auf ONTAP aktualisieren. Anschließend erfolgt ein Backend-Update. Bei der Zertifikatsrotation können dem Benutzer mehrere Zertifikate hinzugefügt werden. Anschließend wird das Backend aktualisiert, um das neue Zertifikat zu verwenden. Danach kann das alte Zertifikat aus dem ONTAP Cluster gelöscht werden.

Durch die Aktualisierung des Backends wird der Zugriff auf bereits erstellte Volumes nicht beeinträchtigt, und

auch später hergestellte Volume-Verbindungen werden nicht beeinträchtigt. Ein erfolgreiches Backend-Update zeigt an, dass Trident mit dem ONTAP -Backend kommunizieren und zukünftige Volumenoperationen bewältigen kann.

Erstellen einer benutzerdefinierten ONTAP Rolle für Trident

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

Siehe"Trident -Benutzerrollengenerator" Weitere Informationen zum Erstellen benutzerdefinierter Trident -Rollen finden Sie hier.

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\>
```

Systemmanager verwenden

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 > Einstellungen**.

      (Oder) Um eine benutzerdefinierte Rolle auf SVM-Ebene zu erstellen, wählen Sie **Speicher > Speicher-VMs > `required SVM` > Einstellungen > Benutzer und Rollen**.

   b. Wählen Sie das Pfeilsymbol (→) neben **Benutzer und Rollen** aus.
   c. Wählen Sie unter **Rollen** die Option **+Hinzufügen**.
   d. Definieren Sie die Regeln für die Rolle und klicken Sie auf **Speichern**.
2. **Rolle dem Trident -Benutzer zuordnen**: + Führen Sie die folgenden Schritte auf der Seite **Benutzer und Rollen** aus:
   a. Wählen Sie unter **Benutzer** das Symbol **+** zum Hinzufügen aus.
   b. Wählen Sie den gewünschten Benutzernamen und anschließend eine Rolle im Dropdown-Menü für **Rolle** aus.
   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-Exportrichtlinien, um den Zugriff auf die von ihm bereitgestellten Volumes zu steuern.

Trident bietet zwei Optionen für die Arbeit mit Exportrichtlinien:

- Trident kann die Exportrichtlinie selbst dynamisch verwalten; in diesem Betriebsmodus gibt der Speicheradministrator eine Liste von CIDR-Blöcken an, die zulässige IP-Adressen darstellen. Trident fügt bei der Veröffentlichung automatisch die entsprechenden Knoten-IPs, die in diese Bereiche fallen, zur Exportrichtlinie hinzu. Alternativ werden, wenn keine CIDRs angegeben sind, alle globalen Unicast-IPs, die auf dem Knoten gefunden werden, auf dem das Volume veröffentlicht wird, der Exportrichtlinie hinzugefügt.
- Speicheradministratoren können eine Exportrichtlinie erstellen und Regeln manuell hinzufügen. Trident verwendet die Standardexportrichtlinie, es sei denn, in der Konfiguration ist ein anderer Exportrichtlinienname angegeben.

Exportrichtlinien dynamisch verwalten

Trident bietet die Möglichkeit, Exportrichtlinien für ONTAP Backends dynamisch zu verwalten. Dies gibt dem Speicheradministrator die Möglichkeit, einen zulässigen Adressraum für Worker-Knoten-IPs festzulegen, anstatt explizite Regeln manuell zu definieren. Es vereinfacht die Verwaltung der Exportrichtlinien erheblich; Änderungen an den Exportrichtlinien erfordern keinen manuellen Eingriff mehr in den Speichercluster. Darüber hinaus trägt dies dazu bei, den Zugriff auf den Speichercluster auf Worker-Knoten zu beschränken, die Volumes einbinden und über IPs im angegebenen Bereich verfügen, wodurch eine feingranulare und automatisierte Verwaltung unterstützt wird.

> Verwenden Sie keine Netzwerkadressübersetzung (NAT), wenn Sie dynamische Exportrichtlinien verwenden. Bei Verwendung von NAT sieht der Speicherkontroller die Frontend-NAT-Adresse und nicht die tatsächliche IP-Hostadresse. Daher wird der Zugriff verweigert, 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 für den Root-Junction in Ihrer SVM eine zuvor erstellte Exportrichtlinie mit einer Exportregel existiert, die den CIDR-Block des Knotens zulässt (z. B. die Standardexportrichtlinie). Befolgen Sie stets die von NetApp empfohlenen Best Practices, um eine SVM für Trident zu dedizieren.

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

- `autoExportPolicy`ist eingestellt auf `true`. Dies deutet darauf hin, dass Trident für jedes

mit diesem Backend bereitgestellte Volume eine Exportrichtlinie erstellt. `svm1` SVM und handhaben das Hinzufügen und Löschen von Regeln mithilfe von `autoexportCIDRs` Adressblöcke. Solange ein Volume nicht an einen Knoten angehängt ist, verwendet das Volume eine leere Exportrichtlinie ohne Regeln, um unerwünschten Zugriff auf dieses Volume zu verhindern. Wenn ein Volume auf einem Knoten veröffentlicht wird, erstellt Trident eine Exportrichtlinie mit demselben Namen wie der zugrunde liegende Qtree, der die Knoten-IP innerhalb des angegebenen CIDR-Blocks enthält. Diese IPs werden auch der Exportrichtlinie 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
        - Ein Qtree mit dem Namen trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c erstellt eine Exportrichtlinie für den FlexVol mit dem Namen `trident-403b5326-8482-40db96d0-d83fb3f4daec` , eine Exportrichtlinie für den Qtree namens `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c` und eine leere Exportpolitik namens `trident_empty` auf der SVM. Die Regeln für die FlexVol -Exportrichtlinie bilden eine Obermenge aller in den Qtree-Exportrichtlinien enthaltenen Regeln. Die leere Exportrichtlinie wird von allen Volumes wiederverwendet, die nicht angehängt sind.

- `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 werden.

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

Sie können aktualisieren `autoExportPolicy` Und `autoExportCIDRs` für Backends, nachdem Sie diese erstellt haben. Sie können neue CIDRs für ein automatisch verwaltetes Backend hinzufügen oder bestehende CIDRs löschen. Beim Löschen von CIDRs ist darauf zu achten, dass bestehende Verbindungen nicht unterbrochen werden. Sie können diese Option auch deaktivieren. `autoExportPolicy` für ein Backend und greifen Sie auf eine manuell erstellte Exportrichtlinie zurück. Dies erfordert die Einstellung der `exportPolicy` Parameter in Ihrer Backend-Konfiguration.

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

```
./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 Exportrichtlinien, um die dem Knoten entsprechenden Zugriffsregeln zu entfernen. Durch das Entfernen dieser Knoten-IP aus den Exportrichtlinien der verwalteten Backends verhindert Trident unerwünschte Mounts, es sei denn, diese IP wird von einem neuen Knoten im Cluster wiederverwendet.

Bei bereits bestehenden Backends wird das Backend aktualisiert mit `tridentctl update backend` stellt sicher, dass Trident die Exportrichtlinien automatisch verwaltet. Dadurch werden bei Bedarf zwei neue Exportrichtlinien erstellt, die nach der UUID und dem Qtree-Namen des Backends benannt sind. Auf dem Backend vorhandene Volumes verwenden nach dem Aushängen und erneuten Einhängen die neu erstellten Exportrichtlinien.

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

Wenn die IP-Adresse eines aktiven Knotens aktualisiert wird, müssen Sie den Trident Pod auf dem Knoten neu starten. Trident wird anschließend die Exportrichtlinie für die von ihm verwalteten Backends aktualisieren, um diese IP-Änderung widerzuspiegeln.

Bereiten Sie die Bereitstellung von SMB-Volumes vor

Mit ein wenig zusätzlicher Vorbereitung können Sie SMB-Volumes bereitstellen mithilfe von `ontap-nas` Fahrer.

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

`autoExportPolicy`wird für SMB-Volumes nicht unterstützt.

Bevor Sie beginnen

Bevor Sie SMB-Volumes bereitstellen können, benötigen Sie Folgendes.

- Ein Kubernetes-Cluster mit einem Linux-Controller-Knoten und mindestens einem Windows-Worker-Knoten, auf dem Windows Server 2022 ausgeführt wird. Trident unterstützt SMB-Volumes nur, wenn sie in Pods eingebunden sind, die auf Windows-Knoten laufen.
- Mindestens ein Trident Geheimnis, das Ihre Active Directory-Anmeldeinformationen enthält. Um Geheimnisse 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 zu konfigurieren `csi-proxy` , siehe"GitHub: CSI-Proxy" oder"GitHub: CSI-Proxy für Windows" für Kubernetes-Knoten, die unter Windows laufen.

Schritte

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

   Für Amazon FSx for ONTAP werden SMB-Freigaben benötigt.

   Sie können die SMB-Administratorfreigaben auf zwei Arten erstellen, entweder mithilfe von"Microsoft Management Console" Über das Snap-In „Freigegebene Ordner“ oder über die ONTAP -Befehlszeilenschnittstelle. So erstellen Sie die SMB-Freigaben mithilfe der ONTAP -Befehlszeilenschnittstelle:

   a. Erstellen Sie gegebenenfalls die Verzeichnispfadstruktur für die Freigabe.

      Der `vserver cifs share create` Der Befehl überprüft den Pfad, der bei der Erstellung der Freigabe in der Option -path angegeben wurde. 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
      ```

      Siehe"Erstellen einer SMB-Freigabe" Für alle Details.

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

Parameter	Beschreibung	Beispiel
`smbShare`	Sie können eine der folgenden Optionen angeben: den Namen einer SMB-Freigabe, die mit der Microsoft Management Console oder der ONTAP CLI erstellt wurde; einen Namen, unter dem Trident die SMB-Freigabe erstellen kann; oder Sie können den Parameter leer lassen, um den Zugriff auf Volumes durch die gemeinsame Freigabe zu verhindern. Dieser Parameter ist für On-Premises ONTAP optional. Dieser Parameter ist für Amazon FSx for ONTAP -Backends erforderlich und darf nicht leer sein.	`smb-share`
`nasType`	**Muss eingestellt werden auf `smb` .** Wenn null, wird standardmäßig der Wert verwendet. `nfs` .	`smb`
`securityStyle`	Sicherheitsstil für neue Bände. **Muss eingestellt sein auf `ntfs` oder `mixed` für SMB-Volumes.**	`ntfs`oder `mixed` für SMB-Volumes
`unixPermissions`	Modus für neue Volumes. **Muss bei SMB-Volumes leer bleiben.**	""

Sichere SMB-Verbindungen aktivieren

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

Wichtige Punkte

- Importieren `ontap-nas-economy` Volumen werden nicht unterstützt.
- Es werden nur schreibgeschützte Klone unterstützt für `ontap-nas-economy` Bände.
- 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-Freigabe-ACL.
- Die in der Annotation des Klon-PVC angegebene SMB-Freigabe-ACL hat Vorrang vor denjenigen im Quell-PVC.
- Stellen Sie sicher, dass Sie gültige AD-Benutzer angeben, während Sie Secure SMB aktivieren. Ungültige Benutzer werden nicht zur Zugriffskontrollliste (ACL) hinzugefügt.
- Wenn Sie dem gleichen AD-Benutzer im Backend, in der Speicherklasse und im PVC unterschiedliche Berechtigungen zuweisen, ergibt sich folgende Berechtigungspriorität: PVC, Speicherklasse und dann Backend.
- Secure SMB wird unterstützt für `ontap-nas` Gilt für verwaltete Volume-Importe und nicht für nicht verwaltete Volume-Importe.

Schritte

1. Geben Sie adAdminUser in TridentBackendConfig wie im folgenden Beispiel gezeigt 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 der Speicherklasse hinzu.

   Füge die `trident.netapp.io/smbShareAdUser` Annotation der Speicherklasse, um sicheres SMB ohne Ausfall zu ermöglichen. Der für die Annotation angegebene Benutzerwert `trident.netapp.io/smbShareAdUser` sollte mit dem im `smbcreds` Geheimnis. Sie können eine der folgenden Optionen auswählen: `smbShareAdUserPermission` : `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 erzeugt 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.

Backend-Konfigurationsoptionen

Die folgenden Tabellen enthalten die Backend-Konfigurationsoptionen:

Parameter	Beschreibung	Standard
`version`		Immer 1
`storageDriverName`	Name des Speichertreibers	`ontap-nas`, `ontap-nas-economy` , oder `ontap-nas-flexgroup`
`backendName`	Benutzerdefinierter Name oder das Speicher-Backend	Fahrername + "_" + dataLIF
`managementLIF`	IP-Adresse eines Clusters oder SVM-Management-LIF. Es kann ein vollqualifizierter Domänenname (FQDN) 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 definiert werden, z. B. `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]` . Für einen nahtlosen MetroCluster Wechsel sieheMetroCluster Beispiel .	„10.0.0.1“, „[2001:1234:abcd::fefe]“

Parameter	Beschreibung	Standard
`dataLIF`	IP-Adresse des Protokolls LIF. NetApp empfiehlt die Angabe `dataLIF` . Falls keine Daten angegeben werden, ruft Trident die dataLIFs vom SVM ab. Sie können einen vollqualifizierten Domänennamen (FQDN) angeben, der für die NFS-Mount-Operationen verwendet werden soll. Dadurch können Sie ein Round-Robin-DNS erstellen, um die Last auf mehrere DataLIFs zu verteilen. 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 definiert werden, z. B. `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]` . **Für Metrocluster auslassen.** Siehe dieMetroCluster Beispiel .	Angegebene Adresse oder abgeleitet von SVM, falls nicht angegeben (nicht empfohlen).
`svm`	Zu verwendende virtuelle Speichermaschine **Für Metrocluster auslassen.** Siehe dieMetroCluster Beispiel .	Abgeleitet, wenn eine SVM `managementLIF` wird angegeben
`autoExportPolicy`	Automatische Erstellung und Aktualisierung von Exportrichtlinien aktivieren [Boolesch]. Verwenden des `autoExportPolicy` Und `autoExportCIDRs` Optionen: Trident kann Exportrichtlinien automatisch verwalten.	FALSCH
`autoExportCIDRs`	Liste der CIDRs, anhand derer die Kubernetes-Knoten-IPs gefiltert werden sollen, wenn `autoExportPolicy` ist aktiviert. Verwenden des `autoExportPolicy` Und `autoExportCIDRs` Optionen: Trident kann Exportrichtlinien automatisch verwalten.	["0.0.0.0/0", "::/0"]`
`labels`	Satz beliebiger JSON-formatierter Bezeichnungen, die auf Datenträger angewendet werden sollen	""
`clientCertificate`	Base64-kodierter Wert des Clientzertifikats. Wird für zertifikatsbasierte Authentifizierung verwendet	""
`clientPrivateKey`	Base64-kodierter Wert des privaten Client-Schlüssels. Wird für zertifikatsbasierte Authentifizierung verwendet	""
`trustedCACertificate`	Base64-kodierter Wert des vertrauenswürdigen CA-Zertifikats. Optional. Wird für zertifikatsbasierte Authentifizierung verwendet	""
`username`	Benutzername für die Verbindung mit dem Cluster/SVM. Wird für die Authentifizierung auf Basis von Anmeldeinformationen verwendet. Informationen zur Active Directory-Authentifizierung finden Sie unter "Authentifizieren Sie Trident bei einem Backend-SVM mithilfe von Active Directory-Anmeldeinformationen".	

Parameter	Beschreibung	Standard
`password`	Kennwort für die Verbindung mit dem Cluster/SVM. Wird für die Authentifizierung auf Basis von Anmeldeinformationen verwendet. Informationen zur Active Directory-Authentifizierung finden Sie unter "Authentifizieren Sie Trident bei einem Backend-SVM mithilfe von Active Directory-Anmeldeinformationen".	
`storagePrefix`	Präfix, das beim Bereitstellen neuer Volumes in der SVM verwendet wird. Kann nach der Konfiguration nicht mehr aktualisiert werden. Bei Verwendung von ontap-nas-economy und einem storagePrefix mit 24 oder mehr Zeichen wird das storagePrefix nicht in die Qtrees eingebettet, sondern nur im Volume-Namen.	"Dreizack"
`aggregate`	Aggregat für die Bereitstellung (optional; falls festgelegt, muss es der SVM zugewiesen werden). Für die `ontap-nas-flexgroup` Treiber, diese Option wird ignoriert. Falls kein Aggregat zugewiesen ist, kann jedes der verfügbaren Aggregate zur Bereitstellung eines FlexGroup Volumes verwendet werden. Wenn das Aggregat in SVM aktualisiert wird, wird es in Trident automatisch durch Abfrage von SVM aktualisiert, ohne dass der Trident Controller neu gestartet werden muss. Wenn Sie in Trident ein bestimmtes Aggregat zur Bereitstellung von Volumes konfiguriert haben und dieses Aggregat umbenannt oder aus der SVM verschoben wird, wechselt das Backend in Trident in den Fehlerzustand, während es das SVM-Aggregat abfragt. Sie müssen entweder das Aggregat in ein auf der SVM vorhandenes ändern oder es vollständig entfernen, um das Backend wieder online zu bringen.	""
`limitAggregateUsage`	Die Bereitstellung schlägt fehl, wenn die Auslastung diesen Prozentsatz überschreitet. **Gilt nicht für Amazon FSx für ONTAP**.	"" (wird nicht standardmäßig erzwungen)

Parameter	Beschreibung	Standard
flexgroupAggregateList	Liste der Aggregate für die Bereitstellung (optional; falls festgelegt, muss sie der SVM zugewiesen werden). Alle dem SVM zugewiesenen Aggregate werden zur Bereitstellung eines FlexGroup Volumes verwendet. Unterstützt für den Speichertreiber **ontap-nas-flexgroup**. Wenn die Aggregatliste in SVM aktualisiert wird, wird die Liste 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 Bereitstellung von Volumes konfiguriert haben und diese Aggregatliste umbenannt oder aus SVM verschoben wird, wechselt das Backend in Trident beim Abfragen des SVM-Aggregats in den Fehlerzustand. Sie müssen entweder die Aggregatliste durch eine auf der SVM vorhandene Liste ersetzen oder sie vollständig entfernen, um das Backend wieder online zu bringen.	""
`limitVolumeSize`	Die Bereitstellung schlägt fehl, wenn die angeforderte Volume-Größe diesen Wert überschreitet. Beschränkt außerdem die maximale Größe der von ihm verwalteten Volumina für Qtrees, und die `qtreesPerFlexvol` Diese Option ermöglicht die Anpassung der maximalen Anzahl von Qtrees pro FlexVol volume.	"" (wird nicht standardmäßig erzwungen)
`debugTraceFlags`	Debug-Flags zur Verwendung bei der Fehlersuche. Beispiel: {"api":false, "method":true} Nicht verwenden `debugTraceFlags` Es sei denn, Sie befinden sich in der Fehlersuche und benötigen einen detaillierten Protokollauszug.	null
`nasType`	Konfiguration der Erstellung von NFS- oder SMB-Volumes. Optionen sind `nfs` , `smb` oder null. Bei der Einstellung „null“ werden standardmäßig NFS-Volumes verwendet.	`nfs`

Parameter	Beschreibung	Standard
`nfsMountOptions`	Durch Kommas getrennte Liste der NFS-Mount-Optionen. Die Mount-Optionen für Kubernetes-persistente Volumes werden normalerweise in Speicherklassen angegeben. Wenn jedoch in einer Speicherklasse keine Mount-Optionen angegeben sind, greift Trident auf die in der Konfigurationsdatei des Speicher-Backends angegebenen Mount-Optionen zurück. Wenn in der Speicherklasse oder der Konfigurationsdatei keine Mount-Optionen angegeben sind, setzt Trident keine Mount-Optionen auf einem zugehörigen persistenten Volume.	""
`qtreesPerFlexvol`	Die maximale Anzahl an Qtrees pro FlexVol muss im Bereich [50, 300] liegen.	"200"
`smbShare`	Sie können eine der folgenden Optionen angeben: den Namen einer SMB-Freigabe, die mit der Microsoft Management Console oder der ONTAP CLI erstellt wurde; einen Namen, unter dem Trident die SMB-Freigabe erstellen kann; oder Sie können den Parameter leer lassen, um den Zugriff auf Volumes durch die gemeinsame Freigabe zu verhindern. Dieser Parameter ist für On-Premises ONTAP optional. 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 eingestellt auf `true` Trident verwendet ONTAP REST-APIs zur Kommunikation mit dem Backend; wenn eingestellt auf `false` Trident verwendet ONTAPI (ZAPI)-Aufrufe zur Kommunikation mit dem Backend. Diese Funktion erfordert ONTAP 9.11.1 und höher. Darüber hinaus muss die verwendete ONTAP Anmelderolle Zugriff auf die `ontapi` Anwendung. Dies wird durch die vordefinierte Bedingung erfüllt. `vsadmin` Und `cluster-admin` Rollen. Ab der Trident Version 24.06 und ONTAP 9.15.1 oder höher, `useREST` ist eingestellt auf `true` Standardmäßig; ändern `useREST` Zu `false` ONTAPI (ZAPI)-Aufrufe verwenden.	`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 daran zu hindern, neue FlexVol -Volumes zu erstellen, die ihre Qtrees enthalten. Für die Bereitstellung neuer PVs werden ausschließlich bereits vorhandene Flexvols verwendet.	

Parameter	Beschreibung	Standard
`adAdminUser`	Active Directory-Administratorbenutzer oder Benutzergruppe mit vollem Zugriff auf SMB-Freigaben. Verwenden Sie diesen Parameter, um Administratorrechte für die SMB-Freigabe mit voller Kontrolle zu erteilen.	

Backend-Konfigurationsoptionen für die Bereitstellung von Volumes

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

Parameter	Beschreibung	Standard
`spaceAllocation`	Speicherplatzbelegung für Qtrees	"WAHR"
`spaceReserve`	Platzreservierungsmodus; "keine" (dünn) oder "Volumen" (dick)	"keiner"
`snapshotPolicy`	Zu verwendende Snapshot-Richtlinie	"keiner"
`qosPolicy`	Die QoS-Richtliniengruppe soll den erstellten Volumes zugewiesen werden. Wählen Sie pro Speicherpool/Backend entweder qosPolicy oder adaptiveQosPolicy aus.	""
`adaptiveQosPolicy`	Adaptive QoS-Richtliniengruppe, die den erstellten Volumes zugewiesen werden soll. Wählen Sie pro Speicherpool/Backend entweder qosPolicy oder adaptiveQosPolicy. Wird von ontap-nas-economy nicht unterstützt.	""
`snapshotReserve`	Prozentsatz des für Snapshots reservierten Speichervolumens	"0" wenn `snapshotPolicy` ist "keine", ansonsten ""
`splitOnClone`	Beim Erstellen eines Klons diesen von seinem Elternklon trennen	"FALSCH"
`encryption`	Aktivieren Sie die NetApp Volumeverschlüsselung (NVE) auf dem neuen Volume; Standardwert ist `false` . Um diese Option nutzen zu können, muss NVE auf dem Cluster lizenziert und aktiviert sein. Wenn NAE im Backend aktiviert ist, wird jedes in Trident bereitgestellte Volume NAE-fähig sein. Weitere Informationen finden Sie unter:"Wie Trident mit NVE und NAE zusammenarbeitet" .	"FALSCH"
`tieringPolicy`	Stufenrichtlinie: "keine" verwenden	
`unixPermissions`	Modus für neue Volumes	„777“ für NFS-Volumes; leer (nicht zutreffend) für SMB-Volumes
`snapshotDir`	Steuert den Zugriff auf die `.snapshot` Verzeichnis	"true" für NFSv4, "false" für NFSv3

Parameter	Beschreibung	Standard
`exportPolicy`	Exportrichtlinie zu verwenden	"Standard"
`securityStyle`	Sicherheitsstil für neue Bände. NFS unterstützt `mixed` Und `unix` Sicherheitsstile. SMB-Unterstützung `mixed` Und `ntfs` Sicherheitsstile.	NFS-Standard ist `unix` . SMB-Standard ist `ntfs` .
`nameTemplate`	Vorlage zum Erstellen benutzerdefinierter Datenträgernamen.	""

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 jeden einzelnen Bestandteil angewendet wird. Eine gemeinsam genutzte QoS-Richtliniengruppe setzt die Obergrenze für den Gesamtdurchsatz aller Workloads durch.

Beispiele für die Volumenbereitstellung

Hier ist ein Beispiel mit vordefinierten 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` Trident verwendet nun eine neue Berechnung, um sicherzustellen, dass FlexVol mit dem SnapshotReserve-Prozentsatz und PVC korrekt dimensioniert wird.

Wenn der Benutzer ein PVC anfordert, erstellt Trident das ursprüngliche FlexVol mit mehr Speicherplatz mithilfe der neuen Berechnung. Diese Berechnung stellt sicher, dass der Benutzer den im PVC angeforderten beschreibbaren Speicherplatz erhält und nicht weniger. Vor Version 21.07 erhielt der Benutzer, wenn er ein PVC (z. B. 5 GiB) mit einem SnapshotReserve von 50 Prozent anforderte, nur 2,5 GiB beschreibbaren Speicherplatz. Dies liegt daran, dass der Benutzer das gesamte Volumen angefordert hat. `snapshotReserve` ist ein Prozentsatz davon. Mit Trident 21.07 fordert der Benutzer den beschreibbaren Speicherplatz an, und Trident definiert diesen. `snapshotReserve` Zahl als Prozentsatz des Gesamtvolumens. Dies gilt nicht für `ontap-nas-economy` . Wie das funktioniert, sehen Sie im folgenden Beispiel:

Die Berechnung erfolgt wie folgt:

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

Bei SnapshotReserve = 50 % und PVC-Anforderung = 5 GiB beträgt die Gesamtgröße des Volumes 5/.5 = 10 GiB und die verfügbare Größe beträgt 5 GiB, was der vom Benutzer in der PVC-Anforderung angeforderten Größe entspricht. Der `volume show` Der Befehl sollte ähnliche Ergebnisse wie in diesem Beispiel liefern:

```
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.
```

Vorhandene Backends aus früheren Installationen stellen beim Upgrade von Trident Volumes wie oben beschrieben bereit. Für Volumes, die Sie vor dem Upgrade erstellt haben, sollten Sie die Größe der Volumes anpassen, damit die Änderung berücksichtigt wird. Zum Beispiel ein 2 GiB PVC mit `snapshotReserve=50` Das vorherige Ergebnis war ein Volumen mit 1 GiB beschreibbarem Speicherplatz. Wenn Sie die Größe des Volumes beispielsweise auf 3 GiB ändern, stehen der Anwendung 3 GiB beschreibbarer Speicherplatz auf einem 6-GiB-Volume zur Verfügung.

Beispiele für minimale Konfigurationen

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

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

ONTAP NAS Wirtschaftsbeispiel

```
---
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 eine manuelle Aktualisierung der Backend-Definition nach einem Switchover und Switchback vermieden wird."SVM-Replikation und -Wiederherstellung" .

Für einen nahtlosen Übergang und Rückwechsel geben Sie die SVM wie folgt an: `managementLIF` und lassen Sie die `dataLIF` Und `svm` Parameter. 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` und nehmen Sie die Base64-kodierten Werte des Clientzertifikats, des privaten Schlüssels bzw. des vertrauenswürdigen CA-Zertifikats.

```
---
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 genauso für die `ontap-nas-economy` Und `ontap-nas-flexgroup` Fahrer.

```
---
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-Adressen

Dieses Beispiel zeigt `managementLIF` unter 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` Dieser 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_
```

Backend-Konfigurationsbeispiel 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 spezifische Standardwerte für alle Speicherpools festgelegt, wie zum Beispiel: `spaceReserve` bei keiner, `spaceAllocation` bei falsch und `encryption` bei falsch. Die virtuellen Pools werden im Speicherbereich definiert.

Trident legt Bereitstellungsbezeichnungen im Feld „Kommentare“ fest. Kommentare sind auf FlexVol für

`ontap-nas` oder FlexGroup für `ontap-nas-flexgroup` . Trident kopiert bei der Bereitstellung alle im virtuellen Pool vorhandenen Labels auf das Speichervolume. Zur Vereinfachung können Speicheradministratoren Bezeichnungen pro virtuellem Pool definieren und Volumes nach Bezeichnung gruppieren.

In diesen Beispielen legen einige der Speicherpools ihre eigenen Einstellungen fest. `spaceReserve` , `spaceAllocation` , Und `encryption` Werte, 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 Wirtschaftsbeispiel

```
---
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 StorageClasses zuordnen

Die folgenden StorageClass-Definitionen beziehen sich auf Beispiele für Backends mit virtuellen Pools . Verwenden des `parameters.selector` Im Feld „StorageClass“ wird für jede StorageClass angegeben, welche virtuellen Pools zum Hosten eines Volumes verwendet werden können. Das Volumen wird die im gewählten virtuellen Pool definierten Aspekte aufweisen.

- Der `protection-gold` Die StorageClass wird dem ersten und zweiten virtuellen Pool zugeordnet. `ontap-nas-flexgroup` Backend. Dies sind die einzigen Pools, die einen 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"
```

- Der `protection-not-gold` Die StorageClass wird dem dritten und vierten virtuellen Pool zugeordnet. `ontap-nas-flexgroup` Backend. 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"
```

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

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

- Die `protection-silver-creditpoints-20k` Die StorageClass wird dem dritten virtuellen Pool zugeordnet. `ontap-nas-flexgroup` Backend. 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"
```

- Der `creditpoints-5k` Die StorageClass wird dem dritten virtuellen Pool zugeordnet. `ontap-nas` Backend und der zweite virtuelle Pool im `ontap-nas-economy` Backend. 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 Speicheranforderungen erfüllt werden.

Aktualisieren `dataLIF` nach der ersten Konfiguration

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-Regelung wirksam wird.

Beispiele für sichere KMU

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 dem 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 hinzufügen `annotations` um sichere KMU zu ermöglichen. Secure SMB funktioniert nicht ohne die Annotationen, unabhängig von den im Backend oder PVC festgelegten Konfigurationen.

Speicherklassenbeispiel mit dem Treiber ontap-nas-economy

```
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
```