ONTAP SAN-Treiber

Trident

NetApp
January 15, 2026

Inhalt

ONTAP SAN-Treiber

ONTAP SAN-Treiberübersicht

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

ONTAP SAN-Treiberdetails

Trident stellt die folgenden SAN-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-san`	iSCSI SCSI über FC	Block	RWO, ROX, RWX, RWOP	Kein Dateisystem; rohes Blockgerät
`ontap-san`	iSCSI SCSI über FC	Dateisystem	RWO, RWOP ROX und RWX sind im Dateisystem-Volume-Modus nicht verfügbar.	`xfs`, `ext3` , `ext4`
`ontap-san`	NVMe/TCP SieheWeitere Überlegungen zu NVMe/TCP.	Block	RWO, ROX, RWX, RWOP	Kein Dateisystem; rohes Blockgerät
`ontap-san`	NVMe/TCP SieheWeitere Überlegungen zu NVMe/TCP.	Dateisystem	RWO, RWOP ROX und RWX sind im Dateisystem-Volume-Modus nicht verfügbar.	`xfs`, `ext3` , `ext4`
`ontap-san-economy`	iSCSI	Block	RWO, ROX, RWX, RWOP	Kein Dateisystem; rohes Blockgerät

Treiber	Protokoll	Lautstärke modus	Unterstützte Zugriffsmodi	Unterstützte Dateisysteme
`ontap-san-economy`	iSCSI	Dateisystem	RWO, RWOP ROX und RWX sind im Dateisystem-Volume-Modus nicht verfügbar.	`xfs`, `ext3` , `ext4`

- 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.

Weitere Überlegungen zu NVMe/TCP

Trident unterstützt das NVMe-Protokoll (Non-Volatile Memory Express) mithilfe des `ontap-san` Fahrer einschließlich:

- IPv6
- Snapshots und Klone von NVMe-Volumes

- Ändern der Größe eines NVMe-Volumes
- Importieren eines NVMe-Volumes, das außerhalb von Trident erstellt wurde, damit sein Lebenszyklus von Trident verwaltet werden kann.
- NVMe-natives Multipathing
- Geordnetes oder ungeordnetes Herunterfahren der K8s-Knoten (24.06)

Trident unterstützt Folgendes nicht:

- DH-HMAC-CHAP, das nativ von NVMe unterstützt wird
- Gerätemapper (DM) Multipathing
- LUKS-Verschlüsselung

NVMe wird nur mit ONTAP REST APIs unterstützt und nicht mit ONTAPI (ZAPI).

Bereiten Sie die Konfiguration des Backends mit ONTAP SAN-Treibern vor.

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

Anforderungen

Für alle ONTAP Backends verlangt Trident , dass mindestens ein Aggregat dem SVM zugewiesen wird.

"ASA r2-Systeme"Sie unterscheiden sich von anderen ONTAP Systemen (ASA, AFF und FAS) in der Implementierung ihrer Speicherschicht. In ASA r2-Systemen werden Speicherverfügbarkeitszonen anstelle von Aggregaten verwendet. Siehe"Das" Wissensdatenbankartikel zur Zuordnung von Aggregaten zu SVMs in ASA r2-Systemen.

Denken Sie daran, dass Sie auch mehrere Treiber gleichzeitig ausführen und Speicherklassen erstellen können, die auf den einen oder anderen Treiber verweisen. Beispielsweise könnten Sie Folgendes konfigurieren: `san-dev` Klasse, die die `ontap-san` Fahrer und ein `san-default` Klasse, die die `ontap-san-economy` eins.

Auf allen Ihren Kubernetes-Worker-Knoten müssen die entsprechenden iSCSI-Tools installiert sein. Siehe "Bereiten Sie den Worker-Knoten vor." für Details.

Authentifizieren Sie das ONTAP Backend

Trident bietet zwei Modi zur Authentifizierung eines ONTAP Backends.

- Anmeldeinformationsbasiert: Benutzername und Passwort eines ONTAP Benutzers mit den erforderlichen Berechtigungen. Es wird empfohlen, eine vordefinierte Sicherheitsanmelderolle zu verwenden, wie zum Beispiel `admin` oder `vsadmin` um maximale Kompatibilität mit ONTAP Versionen zu gewährleisten.
- Zertifikatsbasiert: Trident kann auch mit einem ONTAP Cluster über ein auf dem Backend installiertes Zertifikat kommunizieren. 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-san
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: password
```

JSON

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

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 oder 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.

Zertifikatbasierte 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=admin"
```

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

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.

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

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

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 backend update .`

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

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

> 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"

Authentifizieren Sie Verbindungen mit bidirektionalem CHAP

Trident kann iSCSI-Sitzungen mit bidirektionalem CHAP authentifizieren. `ontap-san` Und `ontap-san-economy` Fahrer. Dies erfordert die Aktivierung der `useCHAP` Option in Ihrer Backend-Definition. Wenn eingestellt auf `true` Trident konfiguriert die Standard-Initiator-Sicherheit der SVM auf bidirektionales CHAP und legt den Benutzernamen und die Geheimnisse aus der Backend-Datei fest. NetApp empfiehlt die Verwendung von bidirektionalem CHAP zur Authentifizierung von Verbindungen. Siehe die folgende Beispielkonfiguration:

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

Der `useCHAP` Der Parameter ist eine boolesche Option, die nur einmal konfiguriert werden kann. Es ist standardmäßig auf „false“ eingestellt. Sobald Sie den Wert auf „true“ gesetzt haben, können Sie ihn nicht mehr auf „false“ setzen.

Zusätzlich zu `useCHAP=true` , Die `chapInitiatorSecret` , `chapTargetInitiatorSecret` , `chapTargetUsername` , Und `chapUsername` Die Felder müssen in der Backend-Definition enthalten sein. Die Geheimnisse können nach der Erstellung eines Backends durch Ausführen von geändert werden. `tridentctl update` .

So funktioniert es

Durch die Einstellung `useCHAP` Wenn dies der Fall ist, weist der Speicheradministrator Trident an, CHAP auf dem Speicher-Backend zu konfigurieren. Hierzu gehört Folgendes:

- CHAP auf der SVM einrichten:
  - Wenn der Standard-Initiator-Sicherheitstyp der SVM „Keine“ ist (Standardeinstellung) **und** keine LUNs im Volume vorhanden sind, legt Trident den Standard-Sicherheitstyp auf „Keine“ fest. `CHAP` und fahren Sie mit der Konfiguration des CHAP-Initiators sowie des Zielbenutzernamens und der zugehörigen Geheimnisse fort.
  - Wenn die SVM LUNs enthält, wird Trident CHAP auf der SVM nicht aktivieren. Dadurch wird sichergestellt, dass der Zugriff auf LUNs, die bereits auf der SVM vorhanden sind, nicht eingeschränkt wird.

- Konfiguration des CHAP-Initiators und des Zielbenutzernamens sowie der Geheimnisse; diese Optionen müssen in der Backend-Konfiguration angegeben werden (wie oben gezeigt).

Nachdem das Backend erstellt wurde, erstellt Trident ein entsprechendes `tridentbackend` CRD speichert die CHAP-Geheimnisse und Benutzernamen als Kubernetes-Geheimnisse. Alle von Trident auf diesem Backend erstellten PVs werden über CHAP eingebunden und angehängt.

Rotieren Sie Anmeldeinformationen und aktualisieren Sie Backends

Sie können die CHAP-Zugangsdaten aktualisieren, indem Sie die CHAP-Parameter in der `backend.json` Datei. Dies erfordert eine Aktualisierung der CHAP-Geheimnisse und die Verwendung von `tridentctl update` Befehl, um diese Änderungen widerzuspiegeln.

> Beim Aktualisieren der CHAP-Geheimnisse für ein Backend müssen Sie Folgendes verwenden: `tridentctl` um das Backend zu aktualisieren. Aktualisieren Sie die Anmeldeinformationen des Speicherclusters nicht über die ONTAP CLI oder den ONTAP System Manager, da Trident diese Änderungen nicht erkennen kann.

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

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

Bestehende Verbindungen bleiben unberührt; sie bleiben aktiv, wenn die Anmeldeinformationen von Trident

auf der SVM aktualisiert werden. Neue Verbindungen verwenden die aktualisierten Zugangsdaten, bestehende Verbindungen bleiben weiterhin aktiv. Durch das Trennen und erneute Verbinden alter PV-Geräte werden diese mit den aktualisierten Zugangsdaten verwendet.

ONTAP SAN-Konfigurationsoptionen und Beispiele

Erfahren Sie, wie Sie ONTAP SAN-Treiber mit Ihrer Trident -Installation erstellen und verwenden. Dieser Abschnitt enthält Beispiele für die Backend-Konfiguration und Details zur Zuordnung von Backends zu StorageClasses.

"ASA r2-Systeme"Sie unterscheiden sich von anderen ONTAP Systemen (ASA, AFF und FAS) in der Implementierung ihrer Speicherschicht. Diese Abweichungen wirken sich wie angegeben auf die Verwendung bestimmter Parameter aus. "Erfahren Sie mehr über die Unterschiede zwischen ASA r2-Systemen und anderen ONTAP Systemen.".

> Nur die `ontap-san` Der Treiber (mit iSCSI- und NVMe/TCP-Protokollen) wird für ASA r2-Systeme unterstützt.

In der Trident Backend-Konfiguration müssen Sie nicht angeben, dass Ihr System ASA r2 ist. Wenn Sie auswählen `ontap-san` als die `storageDriverName` Trident erkennt automatisch das ASA r2- oder das herkömmliche ONTAP System. Einige Backend-Konfigurationsparameter sind für ASA r2-Systeme nicht anwendbar, wie in der folgenden Tabelle vermerkt.

Backend-Konfigurationsoptionen

Die folgenden Tabellen enthalten die Backend-Konfigurationsoptionen:

Parameter	Beschreibung	Standard
`version`		Immer 1
`storageDriverName`	Name des Speichertreibers	`ontap-san`oder `ontap-san-economy`
`backendName`	Benutzerdefinierter Name oder das Speicher-Backend	Fahrername + "_" + dataLIF

Parameter	Beschreibung	Standard
`managementLIF`	IP-Adresse eines Cluster- 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 . Wenn Sie die Anmeldeinformationen „vsadmin“ verwenden, `managementLIF` muss die des SVM sein; bei Verwendung von "Admin"-Anmeldeinformationen, `managementLIF` muss die des Clusters sein.	„10.0.0.1“, „[2001:1234:abcd::fefe]“
`dataLIF`	IP-Adresse des Protokolls LIF. 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]` . **Nicht für iSCSI angeben.** Trident Anwendungen"ONTAP Selective LUN Map" um die iSCSI LIFs zu ermitteln, die zum Aufbau einer Multipath-Sitzung benötigt werden. Es wird eine Warnung generiert, wenn `dataLIF` ist explizit definiert. **Für Metrocluster auslassen.** Siehe dieMetroCluster Beispiel .	Abgeleitet durch die SVM
`svm`	Zu verwendende virtuelle Speichermaschine **Für Metrocluster auslassen.** Siehe dieMetroCluster Beispiel .	Abgeleitet, wenn eine SVM `managementLIF` wird angegeben
`useCHAP`	Verwenden Sie CHAP zur Authentifizierung von iSCSI für ONTAP SAN-Treiber [Boolesch]. Auf einstellen `true` damit Trident bidirektionales CHAP als Standardauthentifizierung für die im Backend angegebene SVM konfiguriert und verwendet. Siehe "Bereiten Sie die Konfiguration des Backends mit ONTAP SAN-Treibern vor." für Details. **Nicht unterstützt für FCP oder NVMe/TCP.**	`false`

Parameter	Beschreibung	Standard
`chapInitiatorSecret`	Geheimnis des CHAP-Initiators. Erforderlich, wenn `useCHAP=true`	""
`labels`	Satz beliebiger JSON-formatierter Bezeichnungen, die auf Datenträger angewendet werden sollen	""
`chapTargetInitiatorSecret`	Geheimnis des CHAP-Zielinitiators. Erforderlich, wenn `useCHAP=true`	""
`chapUsername`	Eingehender Benutzername. Erforderlich, wenn `useCHAP=true`	""
`chapTargetUsername`	Zielbenutzername. Erforderlich, wenn `useCHAP=true`	""
`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 die zertifikatsbasierte Authentifizierung verwendet.	""
`username`	Für die Kommunikation mit dem ONTAP -Cluster ist ein Benutzername erforderlich. Wird für die auf Anmeldeinformationen basierende Authentifizierung verwendet. Informationen zur Active Directory-Authentifizierung finden Sie unter "Authentifizieren Sie Trident bei einem Backend-SVM mithilfe von Active Directory-Anmeldeinformationen".	""
`password`	Für die Kommunikation mit dem ONTAP -Cluster ist ein Passwort erforderlich. Wird für die auf Anmeldeinformationen basierende Authentifizierung verwendet. Informationen zur Active Directory-Authentifizierung finden Sie unter "Authentifizieren Sie Trident bei einem Backend-SVM mithilfe von Active Directory-Anmeldeinformationen".	""
`svm`	Zu verwendende virtuelle Speichermaschine	Abgeleitet, wenn eine SVM `managementLIF` wird angegeben
`storagePrefix`	Präfix, das beim Bereitstellen neuer Volumes in der SVM verwendet wird. Kann später nicht geändert werden. Um diesen Parameter zu aktualisieren, müssen Sie ein neues Backend erstellen.	`trident`

Parameter	Beschreibung	Standard
`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. **Nicht für ASA r2-Systeme angeben**.	""
`limitAggregateUsage`	Die Bereitstellung schlägt fehl, wenn die Auslastung diesen Prozentsatz überschreitet. Wenn Sie ein Amazon FSx for NetApp ONTAP -Backend verwenden, geben Sie dies nicht an. `limitAggregateUsage` . Die bereitgestellten `fsxadmin` Und `vsadmin` enthalten nicht die erforderlichen Berechtigungen, um die aggregierte Nutzung abzurufen und sie mit Trident einzuschränken. **Nicht für ASA r2-Systeme angeben**.	"" (wird nicht standardmäßig erzwungen)
`limitVolumeSize`	Die Bereitstellung schlägt fehl, wenn die angeforderte Volume-Größe diesen Wert überschreitet. Außerdem wird die maximale Größe der von ihm verwalteten Volumes für LUNs beschränkt.	"" (wird nicht standardmäßig erzwungen)
`lunsPerFlexvol`	Die maximale Anzahl an LUNs pro Flexvol muss im Bereich [50, 200] liegen.	`100`
`debugTraceFlags`	Debug-Flags zur Verwendung bei der Fehlersuche. Beispiel: {"api":false, "method":true} Verwenden Sie dies nur, wenn Sie eine Fehlerbehebung durchführen und einen detaillierten Protokollauszug benötigen.	`null`

Parameter	Beschreibung	Standard
`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. `useREST`ist vollständig für NVMe/TCP qualifiziert. NVMe wird nur mit ONTAP REST APIs unterstützt und nicht mit ONTAPI (ZAPI). **Falls angegeben, immer auf setzen `true` für ASA r2-Systeme**.	`true`für ONTAP 9.15.1 oder höher, andernfalls `false`.
`sanType`	Zur Auswahl verwenden `iscsi` für iSCSI, `nvme` für NVMe/TCP oder `fcp` für SCSI über Fibre Channel (FC).	`iscsi`falls leer

Parameter	Beschreibung	Standard
`formatOptions`	Verwenden `formatOptions` um Befehlszeilenargumente für die `mkfs` Befehl, der immer dann angewendet wird, wenn ein Datenträger formatiert wird. Dies ermöglicht es Ihnen, die Lautstärke nach Ihren Wünschen zu formatieren. Stellen Sie sicher, dass Sie die Formatoptionen analog zu den Optionen des Befehls mkfs angeben, jedoch ohne den Gerätepfad. Beispiel: "-E nodiscard" **Unterstützt für `ontap-san` Und `ontap-san-economy` Treiber mit iSCSI-Protokoll. Zusätzlich wird dies für ASA r2-Systeme bei Verwendung der iSCSI- und NVMe/TCP-Protokolle unterstützt.**	
`limitVolumePoolSize`	Maximal anforderbare FlexVol Größe bei Verwendung von LUNs im ontap-san-economy-Backend.	"" (wird nicht standardmäßig erzwungen)
`denyNewVolumePools`	Beschränkt `ontap-san-economy` Backends daran zu hindern, neue FlexVol -Volumes zu erstellen, die ihre LUNs enthalten. Für die Bereitstellung neuer PVs werden ausschließlich bereits vorhandene Flexvols verwendet.	

Empfehlungen zur Verwendung von formatOptions

Trident empfiehlt die folgende Option, um den Formatierungsprozess zu beschleunigen:

-E nodiscard:

- Blöcke sollten beim Erstellen des Dateisystems (mkfs) nicht verworfen werden (das anfängliche Verwerfen von Blöcken ist bei Solid-State-Geräten und dünn bereitgestellten Speichern sinnvoll). Dies ersetzt die veraltete Option "-K" und ist auf alle Dateisysteme (xfs, ext3 und ext4) anwendbar.

Authentifizieren Sie Trident bei einem Backend-SVM mithilfe von Active Directory-Anmeldeinformationen

Sie können Trident so konfigurieren, dass es sich mit Active Directory (AD)-Anmeldeinformationen bei einem Back-End-SVM authentifiziert. Bevor ein AD-Konto auf die SVM zugreifen kann, müssen Sie den AD-Domänencontrollerzugriff auf den Cluster oder die SVM konfigurieren. Für die Clusterverwaltung mit einem AD-Konto müssen Sie einen Domänentunnel erstellen. Siehe "Konfigurieren des Active Directory-Domänencontrollerzugriffs in ONTAP" für Details.

Schritte

1. Konfigurieren Sie die DNS-Einstellungen (Domain Name System) für eine Back-End-SVM:

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

2. Führen Sie den folgenden Befehl aus, um ein Computerkonto für die SVM in Active Directory zu erstellen:

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

3. Verwenden Sie diesen Befehl, um einen AD-Benutzer oder eine AD-Gruppe zum Verwalten des Clusters oder SVM zu erstellen

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

4. Legen Sie in der Trident Backend-Konfigurationsdatei Folgendes fest: `username` Und `password` Parameter auf den AD-Benutzer- oder Gruppennamen bzw. das Kennwort.

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`	Speicherplatzzuweisung für LUNs	"true" **Falls angegeben, auf setzen `true` für ASA r2-Systeme**.
`spaceReserve`	Platzreservierungsmodus; "keine" (dünn) oder "Volumen" (dick). **Einstellen auf `none` für ASA r2** -Systeme.	"keiner"
`snapshotPolicy`	Zu verwendende Snapshot-Richtlinie. **Einstellen auf `none` für ASA r2-Systeme**.	"keiner"
`qosPolicy`	Die QoS-Richtliniengruppe soll den erstellten Volumes zugewiesen werden. Wählen Sie pro Speicherpool/Backend entweder qosPolicy oder adaptiveQosPolicy. 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.	""
`adaptiveQosPolicy`	Adaptive QoS-Richtliniengruppe, die den erstellten Volumes zugewiesen werden soll. Wählen Sie pro Speicherpool/Backend entweder qosPolicy oder adaptiveQosPolicy aus.	""
`snapshotReserve`	Prozentsatz des für Snapshots reservierten Speichervolumens. **Nicht für ASA r2-Systeme angeben**.	"0" wenn `snapshotPolicy` ist "keine", ansonsten ""
`splitOnClone`	Beim Erstellen eines Klons diesen von seinem Elternklon trennen	"FALSCH"

Parameter	Beschreibung	Standard
`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" .	"false" **Falls angegeben, auf setzen. `true` für ASA r2-Systeme**.
`luksEncryption`	LUKS-Verschlüsselung aktivieren. Siehe"Verwenden Sie Linux Unified Key Setup (LUKS)." .	**Einstellen auf `false` für ASA r2-Systeme**.
`tieringPolicy`	Tiering-Richtlinie auf "keine" setzen **Für ASA r2-Systeme nicht angeben** .	
`nameTemplate`	Vorlage zum Erstellen benutzerdefinierter Datenträgernamen.	""

Beispiele für die Volumenbereitstellung

Hier ist ein Beispiel mit vordefinierten Standardwerten:

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

Für alle mit der `ontap-san` Der Trident -Treiber erweitert die FlexVol -Kapazität um zusätzliche 10 Prozent, um die LUN-Metadaten aufzunehmen. Die LUN wird mit der exakten Größe bereitgestellt, die der Benutzer im PVC anfordert. Trident erhöht den FlexVol um 10 Prozent (wird in ONTAP als verfügbare Größe angezeigt). Die Nutzer erhalten nun die von ihnen angeforderte nutzbare Speicherkapazität. Diese Änderung verhindert auch, dass LUNs schreibgeschützt werden, es sei denn, der verfügbare Speicherplatz wird vollständig genutzt. Dies gilt nicht für ontap-san-economy.

Für Backends, die definieren `snapshotReserve` Trident berechnet die Größe von Volumina wie folgt:

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

Die 1.1 sind die zusätzlichen 10 Prozent, die Trident zum FlexVol hinzufügt, um die LUN-Metadaten unterzubringen. Für `snapshotReserve` = 5% und PVC-Anforderung = 5 GiB, die Gesamtvolumengröße beträgt 5,79 GiB und die verfügbare Größe beträgt 5,5 GiB. Der `volume show` Der Befehl sollte ähnliche Ergebnisse wie in diesem Beispiel liefern:

Aktuell ist die Größenänderung die einzige Möglichkeit, die neue Berechnung für ein bestehendes Volumen zu nutzen.

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, empfiehlt NetApp, für LIFs DNS-Namen anstelle von IP-Adressen anzugeben.

ONTAP SAN-Beispiel

Dies ist eine Basiskonfiguration unter Verwendung der `ontap-san` Treiber.

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

MetroCluster 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 `svm` Parameter. Beispiel:

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

ONTAP SAN Wirtschaftsbeispiel

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

Beispiel für zertifikatsbasierte Authentifizierung

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

Beispiele für bidirektionale CHAP-Programme

Diese Beispiele erstellen ein Backend mit `useCHAP` eingestellt auf `true` .

ONTAP SAN CHAP Beispiel

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

ONTAP SAN Wirtschaft CHAP Beispiel

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

NVMe/TCP-Beispiel

Sie benötigen eine SVM, die mit NVMe auf Ihrem ONTAP Backend konfiguriert ist. Dies ist eine grundlegende Backend-Konfiguration für NVMe/TCP.

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

SCSI über FC (FCP) Beispiel

Sie benötigen eine SVM, die mit FC auf Ihrem ONTAP Backend konfiguriert ist. Dies ist eine grundlegende Backend-Konfiguration für FC.

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

Backend-Konfigurationsbeispiel mit nameTemplate

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

Beispiel für formatOptions für den ontap-san-economy-Treiber

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

Beispiele für Backends mit virtuellen Pools

In diesen 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 werden auf dem FlexVol volume festgelegt. Trident kopiert bei der Bereitstellung alle auf einem 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 SAN-Beispiel

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

ONTAP SAN Wirtschaftsbeispiel

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

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

NVMe/TCP-Beispiel

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

Backends StorageClasses zuordnen

Die folgenden StorageClass-Definitionen beziehen sich auf dieBeispiele 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 virtuellen Pool im `ontap-san` Backend. Dies ist der einzige Pool, der Schutz auf Goldniveau bietet.

```
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 zweiten und dritten virtuellen Pool zugeordnet. `ontap-san` 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 dritten virtuellen Pool zugeordnet. `ontap-san-economy` 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"
```

- Der `protection-silver-creditpoints-20k` Die StorageClass wird dem zweiten virtuellen Pool zugeordnet. `ontap-san` 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-san` Backend und der vierte virtuelle Pool im `ontap-san-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"
```

- Der `my-test-app-sc` Die StorageClass wird der folgenden zugeordnet: `testAPP` virtueller Pool im `ontap-san` Fahrer mit `sanType: nvme` . Dies ist das einzige Poolangebot `testApp` .

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

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