



Replizieren Sie Volumes mit SnapMirror

Astra Trident

NetApp

January 14, 2026

Inhalt

Replizieren Sie Volumes mit SnapMirror	1
Replikationsvoraussetzungen	1
Erstellen Sie eine gespiegelte PVC	1
Volume-Replikationsstatus	4
Fördern Sie die sekundäre PVC während eines ungeplanten Failover	5
Fördern Sie die sekundäre PVC während eines geplanten Failover	5
Stellen Sie nach einem Failover eine gespiegelte Beziehung wieder her	5
Zusätzliche Vorgänge	6
Replizieren der primären PVC auf eine neue sekundäre PVC	6
Ändern der Größe einer gespiegelten, primären oder sekundären PVC	6
Entfernen Sie die Replikation aus einer PVC	6
Löschen einer PVC (die zuvor gespiegelt wurde)	6
Löschen eines TMR	6
Aktualisieren Sie Spiegelbeziehungen, wenn ONTAP online ist	7
Aktualisieren Sie Spiegelbeziehungen, wenn ONTAP offline ist	7
Astra Control Provisioner Aktivieren	7

Replizieren Sie Volumes mit SnapMirror

Mit Astra Control Provisioner können Sie Spiegelungsbeziehungen zwischen einem Quell-Volume auf einem Cluster und dem Ziel-Volume auf dem Peering-Cluster erstellen, um Daten für die Disaster Recovery zu replizieren. Sie können eine benutzerdefinierte Ressourcendefinition (CRD, Named Custom Resource Definition) verwenden, um die folgenden Vorgänge auszuführen:

- Erstellen von Spiegelbeziehungen zwischen Volumes (VES)
- Entfernen Sie Spiegelungsbeziehungen zwischen Volumes
- Brechen Sie die Spiegelbeziehungen auf
- Bewerben des sekundären Volumes bei Ausfällen (Failover)
- Verlustfreie Transition von Applikationen von Cluster zu Cluster (während geplanter Failover oder Migrationen)

Replikationsvoraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie beginnen:

ONTAP Cluster

- **Astra Control Provisioner:** Astra Control Provisioner Version 23.10 oder höher muss sowohl auf den Quell- als auch auf den Ziel-Kubernetes-Clustern vorhanden sein, die ONTAP als Backend verwenden.
- **Lizenzen:** Asynchrone Lizenzen von ONTAP SnapMirror, die das Datensicherungspaket verwenden, müssen sowohl auf den Quell- als auch auf den Ziel-ONTAP-Clustern aktiviert sein. Weitere Informationen finden Sie unter ["Übersicht über die SnapMirror Lizenzierung in ONTAP"](#).

Peering

- **Cluster und SVM:** Die ONTAP Speicher-Back-Ends müssen aktiviert werden. Weitere Informationen finden Sie unter ["Übersicht über Cluster- und SVM-Peering"](#).



Vergewissern Sie sich, dass die in der Replizierungsbeziehung zwischen zwei ONTAP-Clustern verwendeten SVM-Namen eindeutig sind.

- **Astra Control Provisioner und SVM:** Die Peering von Remote-SVMs müssen für die Astra Control Bereitstellung im Ziel-Cluster verfügbar sein.

Unterstützte Treiber

- Die Volume-Replizierung wird von `ontap-nas` und `ontap-san` Treibern unterstützt.

Erstellen Sie eine gespiegelte PVC

Führen Sie die folgenden Schritte aus, und verwenden Sie die CRD-Beispiele, um eine Spiegelungsbeziehung zwischen primären und sekundären Volumes zu erstellen.

Schritte

1. Führen Sie auf dem primären Kubernetes-Cluster die folgenden Schritte aus:
 - a. Erstellen Sie ein StorageClass-Objekt mit dem `trident.netapp.io/replication: true`

Parameter.

Beispiel

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-nas
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  fsType: "nfs"
  trident.netapp.io/replication: "true"
```

b. PVC mit zuvor erstellter StorageClass erstellen.

Beispiel

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: csi-nas
```

c. Erstellen Sie eine MirrorRelation CR mit lokalen Informationen.

Beispiel

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  state: promoted
  volumeMappings:
    - localPVCName: csi-nas
```

Astra Control Provisioner ruft die internen Informationen für das Volume und den aktuellen DP-Status des Volumes ab und füllt dann das Statusfeld der MirrorRelationship aus.

d. Holen Sie sich den TridentMirrorRelationship CR, um den internen Namen und die SVM der PVC zu

erhalten.

```
kubectl get tmr csi-nas
```

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
  generation: 1
spec:
  state: promoted
  volumeMappings:
    - localPVCName: csi-nas
status:
  conditions:
    - state: promoted
    localVolumeHandle:
      "datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
    localPVCName: csi-nas
    observedGeneration: 1
```

2. Führen Sie auf dem sekundären Kubernetes-Cluster die folgenden Schritte aus:

a. Erstellen Sie eine StorageClass mit dem Parameter `trident.netapp.io/replication: true`.

Beispiel

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-nas
provisioner: csi.trident.netapp.io
parameters:
  trident.netapp.io/replication: true
```

b. Erstellen Sie eine MirrorRelationship-CR mit Ziel- und Quellinformationen.

Beispiel

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  state: established
  volumeMappings:
    - localPVCName: csi-nas
      remoteVolumeHandle:
        "datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
```

Astra Control Provisioner erstellt eine SnapMirror Beziehung zum Namen der konfigurierten Beziehungsrichtlinie (oder dem Standard für ONTAP) und initialisiert sie.

- c. PVC mit zuvor erstellter StorageClass erstellen, um als sekundäres Ziel zu fungieren (SnapMirror Ziel).

Beispiel

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
  annotations:
    trident.netapp.io/mirrorRelationship: csi-nas
spec:
  accessModes:
    - ReadWriteMany
resources:
  requests:
    storage: 1Gi
storageClassName: csi-nas
```

Astra Control Provisioner überprüft die CRD für die TridentMirrorRelationship und erstellt das Volume nicht, wenn die Beziehung nicht vorhanden ist. Falls die Beziehung besteht, stellt Astra Control Provisioner sicher, dass das neue FlexVol Volume auf eine SVM platziert wird, die mit der in MirrorRelation definierten Remote SVM verbunden ist.

Volume-Replikationsstatus

Eine Trident Mirror-Beziehung (TMR) ist eine CRD, die ein Ende einer Replizierungsbeziehung zwischen PVCs darstellt. Das Ziel-TMR verfügt über einen Status, der Astra Control Provisioner über den gewünschten Status informiert. Das Ziel-TMR hat die folgenden Zustände:

- **Etabliert:** Die lokale PVC ist das Zielvolumen einer Spiegelbeziehung, und das ist eine neue Beziehung.
- **Befördert:** Die lokale PVC ist ReadWrite und montierbar, ohne dass aktuell eine Spiegelbeziehung

besteht.

- **Wiederhergestellt:** Die lokale PVC ist das Zielvolumen einer Spiegelbeziehung und war zuvor auch in dieser Spiegelbeziehung.
 - Der neu eingerichtete Status muss verwendet werden, wenn das Ziel-Volume jemals in einer Beziehung zum Quell-Volume stand, da es den Inhalt des Ziel-Volume überschreibt.
 - Der neu eingerichtete Status schlägt fehl, wenn das Volume zuvor nicht in einer Beziehung zur Quelle stand.

Fördern Sie die sekundäre PVC während eines ungeplanten Failover

Führen Sie den folgenden Schritt auf dem sekundären Kubernetes-Cluster aus:

- Aktualisieren Sie das Feld *spec.State* von *TridentMirrorRelationship* auf *promoted*.

Fördern Sie die sekundäre PVC während eines geplanten Failover

Führen Sie während eines geplanten Failover (Migration) die folgenden Schritte durch, um die sekundäre PVC hochzustufen:

Schritte

1. Erstellen Sie auf dem primären Kubernetes-Cluster einen Snapshot der PVC und warten Sie, bis der Snapshot erstellt wurde.
2. Erstellen Sie auf dem primären Kubernetes-Cluster *SnapshotInfo* CR, um interne Details zu erhalten.

Beispiel

```
kind: SnapshotInfo
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  snapshot-name: csi-nas-snapshot
```

3. Aktualisieren Sie im sekundären Kubernetes-Cluster das Feld *spec.State* des *tridentMirrorRelationship* CR auf *promoted* und *spec.promotedSnapshotHandle* als *InternalName* des Snapshots.
4. Bestätigen Sie auf sekundärem Kubernetes-Cluster den Status (Feld *Status.State*) von *TridentMirrorRelationship* auf hochgestuft.

Stellen Sie nach einem Failover eine gespiegelte Beziehung wieder her

Wählen Sie vor dem Wiederherstellen einer Spiegelbeziehung die Seite aus, die Sie als neuen primären festlegen möchten.

Schritte

1. Stellen Sie auf dem sekundären Kubernetes-Cluster sicher, dass die Werte für das Feld *spec.remoteVolumeHandle* auf dem TridentMirrorRelationship aktualisiert werden.
2. Aktualisieren Sie im sekundären Kubernetes-Cluster das Feld *spec.mirror* von TridentMirrorRelationship auf *reestablished*.

Zusätzliche Vorgänge

Astra Control Provisioner unterstützt die folgenden Vorgänge für primäre und sekundäre Volumes:

Replizieren der primären PVC auf eine neue sekundäre PVC

Stellen Sie sicher, dass Sie bereits über eine primäre PVC und eine sekundäre PVC verfügen.

Schritte

1. Löschen Sie die CRDs PersistentVolumeClaim und TridentMirrorRelationship aus dem eingerichteten sekundären Cluster (Ziel).
2. Löschen Sie die CRD für TridentMirrorRelationship aus dem primären (Quell-) Cluster.
3. Erstellen Sie eine neue TridentMirrorRelationship CRD auf dem primären (Quell-) Cluster für die neue sekundäre (Ziel-) PVC, die Sie einrichten möchten.

Ändern der Größe einer gespiegelten, primären oder sekundären PVC

Die PVC-Größe kann wie gewohnt geändert werden. ONTAP erweitert automatisch alle Zielflvxole, wenn die Datenmenge die aktuelle Größe überschreitet.

Entfernen Sie die Replikation aus einer PVC

Um die Replikation zu entfernen, führen Sie einen der folgenden Vorgänge auf dem aktuellen sekundären Volume aus:

- Löschen Sie MirrorRelation auf der sekundären PVC. Dadurch wird die Replikationsbeziehung unterbrochen.
- Oder aktualisieren Sie das Feld *spec.State* auf *promoted*.

Löschen einer PVC (die zuvor gespiegelt wurde)

Astra Control Provisioner überprüft nach replizierten PVCs und gibt die Replizierungsbeziehung frei, bevor versucht wird, das Volume zu löschen.

Löschen eines TMR

Das Löschen eines TMR auf einer Seite einer gespiegelten Beziehung führt dazu, dass der verbleibende TMR in den Status *promoted* übergeht, bevor Astra Control Provisioner den Löschvorgang abgeschlossen hat. Wenn der für den Löschvorgang ausgewählte TMR bereits den Status *promoted* hat, gibt es keine bestehende Spiegelbeziehung und der TMR wird entfernt und Astra Control Provisioner wird die lokale PVC auf *ReadWrite* hochstufen. Durch dieses Löschen werden SnapMirror Metadaten für das lokale Volume in ONTAP freigegeben. Wenn dieses Volume in Zukunft in einer Spiegelbeziehung verwendet wird, muss es beim Erstellen der neuen Spiegelbeziehung ein neues TMR mit einem *established* Volume-Replikationsstatus verwenden.

Aktualisieren Sie Spiegelbeziehungen, wenn ONTAP online ist

Spiegelbeziehungen können jederzeit nach ihrer Einrichtung aktualisiert werden. Sie können die Felder oder verwenden `state: promoted` `state: reestablished`, um die Beziehungen zu aktualisieren. Wenn Sie ein Zielvolume auf ein reguläres ReadWrite-Volume heraufstufen, können Sie `promotedSnapshotHandle` verwenden, um einen bestimmten Snapshot anzugeben, auf dem das aktuelle Volume wiederhergestellt werden soll.

Aktualisieren Sie Spiegelbeziehungen, wenn ONTAP offline ist

Sie können ein CRD verwenden, um ein SnapMirror Update durchzuführen, ohne dass Astra Control direkt mit dem ONTAP Cluster verbunden ist. Im folgenden Beispielformat finden Sie das `TridentActionMirrorUpdate`:

Beispiel

```
apiVersion: trident.netapp.io/v1
kind: TridentActionMirrorUpdate
metadata:
  name: update-mirror-b
spec:
  snapshotHandle: "pvc-1234/snapshot-1234"
  tridentMirrorRelationshipName: mirror-b
```

`status.state` Gibt den Status von `TridentActionMirrorUpdate` CRD wieder. Es kann einen Wert von *suileded*, *in progress* oder *failed* annehmen.

Astra Control Provisioner Aktivieren

Trident Version 23.10 und höher bieten die Option zur Verwendung von Astra Control Provisioner, damit Benutzer von Astra Control auf erweiterte Funktionen zur Storage-Bereitstellung zugreifen können. Astra Control Provisioner bietet diese erweiterte Funktionalität zusätzlich zu den auf Astra Trident basierenden Standardfunktionen. Mit diesem Verfahren können Sie Astra Control Provisioner aktivieren und installieren.

Im Abonnement für Astra Control Service ist automatisch die Lizenz für die Nutzung von Astra Control Provisioner enthalten.

Bei den neuesten Updates für Astra Control wird Astra Control Provisioner Astra Trident als Storage-bereitstellung und -Orchestrierung ersetzen und für die Verwendung von Astra Control obligatorisch sein. Aus diesem Grund wird dringend empfohlen, Astra Control für die Astra Control-Bereitstellung zu aktivieren. Astra Trident wird weiterhin Open Source bleiben und mit neuen CSI- und anderen Funktionen von NetApp veröffentlicht, gepflegt, unterstützt und auf dem neuesten Stand sein.

Wie kann ich feststellen, ob ich die Astra Control-Bereitstellung aktivieren muss?

Wenn Sie Astra Control Service einen Cluster hinzufügen, für den Astra Trident zuvor nicht installiert ist, wird der Cluster als markiert `Eligible`. Nach Ihnen ["Fügen Sie den Cluster zu Astra Control hinzu"](#) wird der Astra

Control Provisioner automatisch aktiviert.

Wenn Ihr Cluster nicht markiert ist `Eligible`, wird er aufgrund einer der folgenden Zeichen markiert `Partially eligible`:

- Es verwendet eine ältere Version von Astra Trident
- In Astra Trident 23.10 wird noch nicht die bereitstellungsoption aktiviert
- Es handelt sich um einen Cluster-Typ, der keine automatische Aktivierung zulässt

In `Partially eligible` Fällen können Sie mit diesen Anweisungen die Astra Control Provisioner für Ihr Cluster manuell aktivieren.

Add cluster STEP 2/4: CLUSTER

CLUSTER

Choose an Azure Kubernetes Service cluster to enable application data management and the Astra Control storage operator.

⚠ Some Kubernetes cluster(s) below have private networking. [Learn more](#)

Cluster	Location	Eligibility
sandbox-ragnarok-aks-02	centraluseup	Eligible
sandbox-ragnarok-aks-03	centraluseup	Partially eligible
sandbox-rstephe2-aks-01	centraluseup	Eligible

Configuration required
Failed to detect Astra Control Provisioner on cluster

← Back Next →

Bevor Sie Astra Control Provisioner aktivieren

Wenn Sie bereits Astra Trident ohne Astra Control Provisioner verwenden und Astra Control Provisioner aktivieren möchten, gehen Sie zuerst wie folgt vor:

- **Wenn Sie Astra Trident installiert haben, bestätigen Sie, dass seine Version innerhalb eines Fensters mit vier Versionen ist:** Sie können ein direktes Upgrade auf Astra Trident 24.02 mit Astra Control Provisioner durchführen, wenn Ihr Astra Trident innerhalb eines Fensters mit vier Versionen von Version 24.02 ist. Sie können beispielsweise direkt von Astra Trident 23.04 auf 24.02 aktualisieren.
- **Bestätigen Sie, dass Ihr Cluster über eine AMD64-Systemarchitektur verfügt:** Das Astra Control Provisioner-Image wird sowohl in AMD64- als auch in ARM64-CPU-Architekturen bereitgestellt, aber nur AMD64 wird von Astra Control unterstützt.

Schritte

1. Rufen Sie die NetApp Astra Control Image-Registry auf:

- a. Melden Sie sich an der Astra Control Service UI an und notieren Sie Ihre Astra Control Konto-ID.
 - i. Wählen Sie das Symbol oben rechts auf der Seite.
 - ii. Wählen Sie **API-Zugriff**.
 - iii. Notieren Sie sich Ihre Konto-ID.
- b. Wählen Sie auf derselben Seite **API-Token generieren** aus und kopieren Sie die API-Token-Zeichenfolge in die Zwischenablage und speichern Sie sie in Ihrem Editor.
- c. Melden Sie sich über Ihre bevorzugte Methode in der Astra Control Registry an:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

```
crane auth login cr.astra.netapp.io -u <account-id> -p <api-token>
```

2. (Nur benutzerdefinierte Registrierungen) Befolgen Sie diese Schritte, um das Bild in Ihre benutzerdefinierte Registrierung zu verschieben. Wenn Sie keine Registrierung verwenden, befolgen Sie die Schritte des Trident-Operators im [Nächster Abschnitt](#).



Sie können Podman anstelle von Docker für die folgenden Befehle verwenden. Wenn Sie eine Windows-Umgebung verwenden, wird PowerShell empfohlen.

Docker

- a. Rufen Sie das Astra Control Provisioner-Image aus der Registrierung ab:



Das abgezogene Image unterstützt nicht mehrere Plattformen und unterstützt nur die gleiche Plattform wie der Host, der das Image gezogen hat, wie z. B. Linux AMD64.

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0
--platform <cluster platform>
```

Beispiel:

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0
--platform linux/amd64
```

- b. Markieren Sie das Bild:

```
docker tag cr.astra.netapp.io/astra/trident-acp:24.02.0
<my_custom_registry>/trident-acp:24.02.0
```

- c. Laden Sie das Bild in Ihre benutzerdefinierte Registrierung:

```
docker push <my_custom_registry>/trident-acp:24.02.0
```

Kran

- a. Kopieren Sie das Astra Control Provisioner-Manifest in Ihre benutzerdefinierte Registry:

```
crane copy cr.astra.netapp.io/astra/trident-acp:24.02.0
<my_custom_registry>/trident-acp:24.02.0
```

3. Stellen Sie fest, ob die ursprüngliche Astra Trident Installationsmethode einen verwendethat.
4. Aktivieren Sie Astra Control Provisioner in Astra Trident mit der ursprünglich verwendeten Installationsmethode:

Astra Trident Betreiber

- a. ["Laden Sie das Astra Trident Installationsprogramm herunter und extrahieren Sie es"](#).
- b. Führen Sie diese Schritte aus, wenn Sie Astra Trident noch nicht installiert haben oder den Operator aus der ursprünglichen Astra Trident-Implementierung entfernt haben:
 - i. Erstellen des CRD:

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.1
6.yaml
```

- ii. Erstellen Sie den dreigesichtigen Namespace (`kubectl create namespace trident`) oder bestätigen Sie, dass der dreigesichtigen Namespace noch existiert (`kubectl get all -n trident`). Wenn der Namespace entfernt wurde, erstellen Sie ihn erneut.

- c. Update von Astra Trident auf 24.02.0:



Verwenden Sie für Cluster mit Kubernetes 1.24 oder früher

`bundle_pre_1_25.yaml`: Verwenden Sie für Cluster mit Kubernetes 1.25 oder höher `bundle_post_1_25.yaml`.

```
kubectl -n trident apply -f trident-installer/deploy/<bundle-
name.yaml>
```

- d. Überprüfen Sie, ob Astra Trident ausgeführt wird:

```
kubectl get torc -n trident
```

Antwort:

NAME	AGE
trident	21m

- e. Wenn Sie eine Registry mit Geheimnissen haben, erstellen Sie ein Geheimnis, mit dem Sie das Astra Control Provisioner-Bild abrufen können:

```
kubectl create secret docker-registry <secret_name> -n trident
--docker-server=<my_custom_registry> --docker-username=<username>
--docker-password=<token>
```

- f. Bearbeiten Sie den TridentOrchestrator CR, und nehmen Sie die folgenden Änderungen vor:

```
kubectl edit torc trident -n trident
```

- i. Legen Sie einen benutzerdefinierten Registrierungsort für das Astra Trident-Image fest oder ziehen Sie es aus der Astra Control-Registry (`tridentImage: <my_custom_registry>/trident:24.02.0` oder `tridentImage: netapp/trident:24.02.0`).
- ii. Aktivieren Sie Astra Control Provisioner (`enableACP: true`).
- iii. Legen Sie den benutzerdefinierten Registrierungsport für das Astra Control Provisioner-Image fest oder ziehen Sie es aus der Astra Control Registry (`acpImage: <my_custom_registry>/trident-acp:24.02.0` oder `acpImage: cr.astra.netapp.io/astra/trident-acp:24.02.0`).
- iv. Wenn Sie in diesem Verfahren bereits einmal eingerichtet [Geheimnisse der Bildausziehung](#) haben, können Sie diese hier einstellen (`imagePullSecrets: - <secret_name>`). Verwenden Sie den gleichen geheimen Namen, den Sie in den vorherigen Schritten festgelegt haben.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  tridentImage: <registry>/trident:24.02.0
  enableACP: true
  acpImage: <registry>/trident-acp:24.02.0
  imagePullSecrets:
    - <secret_name>
```

- g. Speichern und beenden Sie die Datei. Der Bereitstellungsprozess wird automatisch gestartet.
- h. Überprüfen Sie, ob der Operator, die Bereitstellung und Replikasets erstellt wurden.

```
kubectl get all -n trident
```



Es sollte nur eine Instanz* des Operators in einem Kubernetes-Cluster geben. Erstellen Sie nicht mehrere Implementierungen des Astra Trident Operators.

- i. Überprüfen Sie, ob der `trident-acp` Container läuft und der `acpVersion` Status lautet `24.02.0 Installed`:

```
kubectl get torc -o yaml
```

Antwort:

```
status:
  acpVersion: 24.02.0
  currentInstallationParams:
    ...
    acpImage: <registry>/trident-acp:24.02.0
    enableACP: "true"
    ...
  ...
status: Installed
```

Tridentctl

- "Laden Sie das Astra Trident Installationsprogramm herunter und extrahieren Sie es".
- "Wenn Sie bereits Astra Trident verwenden, deinstallieren Sie ihn aus dem Cluster, das ihn hostet".
- Astra Trident mit aktivierter Astra Control Provisioner installieren (`--enable-acp=true`):

```
./tridentctl -n trident install --enable-acp=true --acp
-image=mycustomregistry/trident-acp:24.02
```

- Aktivieren Sie die Astra Control Provisioner-Funktion:

```
./tridentctl -n trident version
```

Antwort:

```
+-----+-----+-----+ | SERVER
VERSION | CLIENT VERSION | ACP VERSION | +-----+
+-----+-----+-----+ | 24.02.0 | 24.02.0 | 24.02.0. |
+-----+-----+-----+
```

Helm

- Bei Installation von Astra Trident 23.07.1 oder einer früheren Version sind der Operator und andere Komponenten installiert **"Deinstallieren"**.
- Wenn auf dem Kubernetes-Cluster 1.24 oder eine frühere Version ausgeführt wird, löschen Sie psp:

```
kubectl delete psp tridentoperatorpod
```

- Fügen Sie das Helm Repository von Astra Trident hinzu:

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-chart
```

d. Aktualisieren Sie das Helm-Diagramm:

```
helm repo update netapp-trident
```

Antwort:

```
Hang tight while we grab the latest from your chart
repositories...
...Successfully got an update from the "netapp-trident" chart
repository
Update Complete. ☐Happy Helming!☐
```

e. Auflisten der Bilder:

```
./tridentctl images -n trident
```

Antwort:

```
| v1.28.0          | netapp/trident:24.02.0|
|                  | docker.io/netapp/trident-
autosupport:24.02|
|                  | registry.k8s.io/sig-storage/csi-
provisioner:v4.0.0|
|                  | registry.k8s.io/sig-storage/csi-
attacher:v4.5.0|
|                  | registry.k8s.io/sig-storage/csi-
resizer:v1.9.3|
|                  | registry.k8s.io/sig-storage/csi-
snapshotter:v6.3.3|
|                  | registry.k8s.io/sig-storage/csi-node-
driver-registrar:v2.10.0 |
|                  | netapp/trident-operator:24.02.0 (optional)
```

f. Stellen Sie sicher, dass Dreizack-Bediener 24.02.0 verfügbar ist:

```
helm search repo netapp-trident/trident-operator --versions
```

Antwort:

NAME	CHART VERSION	APP VERSION	
DESCRIPTION			
netapp-trident/trident-operator	100.2402.0	24.02.0	A

g. Verwenden Sie `helm install` eine der folgenden Optionen, die diese Einstellungen enthalten, und führen Sie sie aus:

- Ein Name für Ihren Bereitstellungsort
- Die Version Astra Trident
- Der Name des Bildes für die Astra Control-Bereitstellung
- Das Flag, mit dem die provisionierung aktiviert wird
- (Optional) Ein lokaler Registrierungspfad. Wenn Sie eine lokale Registrierung verwenden, kann sich Ihr ["Trident Images"](#) in einer Registrierung oder in verschiedenen Registrierungen befinden, aber alle CSI-Images müssen sich in derselben Registrierung befinden.
- Der Trident Namespace

Optionen

- Bilder ohne Registrierung

```
helm install trident netapp-trident/trident-operator --version 100.2402.0 --set acpImage=cr.astra.netapp.io/astra/trident-acp:24.02.0 --set enableACP=true --set operatorImage=netapp/trident-operator:24.02.0 --set tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.02 --set tridentImage=netapp/trident:24.02.0 --namespace trident
```

- Bilder in einer oder mehreren Registern

```
helm install trident netapp-trident/trident-operator --version 100.2402.0 --set acpImage=<your-registry>:<acp image> --set enableACP=true --set imageRegistry=<your-registry>/sig-storage --set operatorImage=netapp/trident-operator:24.02.0 --set tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.02 --set tridentImage=netapp/trident:24.02.0 --namespace trident
```

Verwenden Sie können `helm list` So prüfen Sie Installationsdetails wie Name, Namespace, Diagramm, Status, App-Version, Und Revisionsnummer.

Falls Sie Probleme bei der Implementierung von Trident mit Helm haben, führen Sie diesen Befehl aus, um Astra Trident vollständig zu deinstallieren:

```
./tridentctl uninstall -n trident
```

Nicht ["Astra Trident CRDs vollständig entfernen"](#) als Teil Ihrer Deinstallation, bevor Sie versuchen, Astra Control Provisioner wieder zu aktivieren.

Ergebnis

Die Bereitstellungsfunktion von Astra Control ist aktiviert und Sie können alle Funktionen der verwendeten Version verwenden.

Nach der Installation von Astra Control provisioner wird im Cluster, das die provisionierung in der Astra Control UI hostet, ein Feld statt und die aktuelle installierte Versionsnummer angezeigt ACP version Trident version .

~ CLUSTER STATUS

✓ Available

Version v1.24.9+rke2r2	Managed 2024/03/15 17:32 UTC	Kube-system namespace UID 	ACP Version
Private route identifier .. ⓘ	Cloud instance private ⓘ	Default bucket astra-bucket1 (inherited) ⓘ	

Overview

Namespaces

Storage

Activity

Finden Sie weitere Informationen

- ["Dokumentation für Astra Trident Upgrades"](#)

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.