



# Upgrade von Trident

Trident

NetApp

January 14, 2026

# Inhalt

Upgrade von Trident . . . . .	1
Upgrade von Trident . . . . .	1
Überlegungen vor dem Upgrade . . . . .	1
Schritt 1: Wählen Sie eine Version . . . . .	1
Schritt 2: Bestimmen Sie die ursprüngliche Installationsmethode . . . . .	2
Schritt 3: Wählen Sie eine Upgrade-Methode . . . . .	2
Upgrade mit dem Bediener . . . . .	2
Den Upgrade-Workflow für Bediener verstehen . . . . .	2
Aktualisieren Sie eine Trident-Installation mit Trident Operator oder Helm . . . . .	3
Upgrade mit tridentctl . . . . .	7

# Upgrade von Trident

## Upgrade von Trident

Ab Version 24.02 folgt Trident einem viermonatigen Release-Intervall und liefert drei wichtige Releases pro Kalenderjahr. Jede neue Version baut auf den vorherigen Versionen auf und bietet neue Funktionen, Performance-Verbesserungen, Bug Fixes und Verbesserungen. Wir empfehlen Ihnen, mindestens einmal pro Jahr ein Upgrade durchzuführen, um von den neuen Funktionen von Trident zu profitieren.

### Überlegungen vor dem Upgrade

Beachten Sie beim Upgrade auf die neueste Version von Trident Folgendes:

- In allen Namespaces in einem Kubernetes-Cluster sollte nur eine Trident Instanz installiert werden.
- Trident 23.07 und höher erfordert v1-Volumen-Snapshots und unterstützt keine Alpha- oder Beta-Snapshots mehr.
- Wenn Sie Cloud Volumes Service für Google Cloud im erstellt "[CVS-Diensttyp](#)" haben, müssen Sie die Backend-Konfiguration aktualisieren, um den oder zoneredundantstandardsw Service-Level beim Upgrade von Trident 23.01 zu verwenden standardsw. Wenn das im Backend nicht aktualisiert serviceLevel wird, kann es zu einem Fehlschlagen der Volumes kommen. Weitere Informationen finden Sie unter "[Beispiele für CVS-Diensttypen](#)".
- Beim Upgrade ist es wichtig, dass Sie StorageClasses von Trident verwendet angeben parameter.fsType. Sie können löschen und neu erstellen StorageClasses, ohne bereits vorhandene Volumes zu unterbrechen.
  - Dies ist eine **Anforderung** für die Durchsetzung von "[Sicherheitskontexten](#)" SAN-Volumes.
  - Das Verzeichnis [sample input](#) enthält Beispiele wie storage-class-basic.yaml.templ und Link:[Bekannte Probleme](#)".

### Schritt 1: Wählen Sie eine Version

Trident-Versionen folgen einer datumbasierten Namenskonvention YY.MM, wobei „YY“ die letzten beiden Ziffern des Jahres und „MM“ der Monat ist. Dot-Releases folgen einer YY.MM.X Konvention, wobei „X“ der Patch-Level ist. Sie wählen die Version, auf die Sie aktualisieren möchten, basierend auf der Version aus, von der Sie aktualisieren.

- Sie können ein direktes Upgrade auf jede Zielversion durchführen, die sich innerhalb eines Fensters mit vier Versionen Ihrer installierten Version befindet. Sie können beispielsweise direkt von 24.06 (oder einer beliebigen 24.06-Dot-Version) auf 25.02 aktualisieren.
- Wenn Sie ein Upgrade von einer Version außerhalb des Fensters mit vier Releases durchführen, führen Sie ein Upgrade in mehreren Schritten durch. Verwenden Sie die Upgrade-Anweisungen für das, von dem "[Frühere Version](#)" Sie aktualisieren, um auf die neueste Version zu aktualisieren, die für das Fenster mit vier Versionen passt. Wenn Sie beispielsweise 23.01 verwenden und ein Upgrade auf 25.02 durchführen möchten:
  - a. Erstes Upgrade von 23.01 auf 24.02.

b. Dann Upgrade von 24.02 auf 25.02.



Wenn Sie ein Upgrade über den Trident-Operator auf der OpenShift Container Platform durchführen, sollten Sie auf Trident 21.01.1 oder höher aktualisieren. Der mit 21.01.0 veröffentlichte Trident-Operator enthält ein bekanntes Problem, das in 21.01.1 behoben wurde. Weitere Informationen finden Sie im "[Details zur Ausgabe auf GitHub](#)".

## Schritt 2: Bestimmen Sie die ursprüngliche Installationsmethode

So bestimmen Sie, welche Version Sie ursprünglich für die Installation von Trident verwendet haben:

1. Verwenden Sie `kubectl get pods -n trident` um die Pods zu untersuchen.
  - Wenn kein Operator Pod vorhanden ist, wurde Trident mit installiert `tridentctl`.
  - Wenn es einen Operator-Pod gibt, wurde Trident entweder manuell oder über Helm mit dem Trident-Operator installiert.
2. Wenn ein Benutzer-POD vorhanden ist, verwenden Sie `kubectl describe torc`, um zu ermitteln, ob Trident mit Helm installiert wurde.
  - Wenn ein Helm-Label vorhanden ist, wurde Trident mit Helm installiert.
  - Wenn kein Helm-Etikett vorhanden ist, wurde Trident manuell mit dem Trident-Operator installiert.

## Schritt 3: Wählen Sie eine Upgrade-Methode

Im Allgemeinen sollten Sie mit der gleichen Methode aktualisieren, die Sie für die Erstinstallation verwendet haben, jedoch können Sie "[Wechseln Sie zwischen den Installationsmethoden](#)". Es gibt zwei Optionen für ein Upgrade von Trident.

- "[Upgrade über den Trident-Operator](#)"



Wir empfehlen Ihnen, die Überprüfung "[Den Upgrade-Workflow für Bediener verstehen](#)" durchzuführen, bevor Sie mit dem Betreiber ein Upgrade durchführen.

\*

## Upgrade mit dem Bediener

### Den Upgrade-Workflow für Bediener verstehen

Bevor Sie ein Upgrade von Trident mit dem Trident Operator durchführen, sollten Sie sich über die während des Upgrades auftretenden Hintergrundprozesse informieren. Dies umfasst Änderungen am Trident Controller, am Controller Pod und an Node-Pods sowie am Node-DemonSet, die Rolling-Updates ermöglichen.

### Bearbeitung von Trident Upgrades für Betreiber

Eine der vielen "[Vorteile der Verwendung des Trident-Bediener](#)" Installationen und Upgrades von Trident ist die automatische Handhabung von Trident- und Kubernetes-Objekten ohne Unterbrechung vorhandener gemountete Volumes. So kann Trident Upgrades ohne Ausfallzeiten oder "[Rollierende Updates](#)" Insbesondere kommuniziert der Trident Betreiber mit dem Kubernetes-Cluster, um:

- Löschen Sie die Trident Controller-Implementierung und den Node DemonSet und erstellen Sie sie neu.
- Ersetzen Sie den Trident Controller Pod und die Trident Node Pods durch neue Versionen.
  - Wenn ein Node nicht aktualisiert wird, verhindert dies nicht, dass die verbleibenden Nodes aktualisiert werden.
  - Nur Nodes mit einem laufenden Trident Node Pod können Volumes mounten.



Weitere Informationen zur Trident-Architektur auf dem Kubernetes-Cluster finden Sie unter ["Architektur von Trident"](#).

## Arbeitsablauf für die Benutzeraktualisierung

Wenn Sie ein Upgrade mit dem Trident Operator initiieren:

1. **Der Trident-Operator:**
  - a. Erkennt die aktuell installierte Version von Trident (Version  $n$ ).
  - b. Aktualisiert alle Kubernetes-Objekte einschließlich CRDs, RBAC und Trident SVC.
  - c. Löscht die Trident Controller-Bereitstellung für Version  $n$ .
  - d. Erstellt die Trident-Controller-Bereitstellung für Version  $n+1$ .
2. **Kubernetes** erstellt Trident Controller Pod für  $n+1$ .
3. **Der Trident-Operator:**
  - a. Löscht das Trident Node DemonSet für  $n$ . Der Operator wartet nicht auf die Beendigung des Node-Pod.
  - b. Erstellt den Trident Node Demonset für  $n+1$ .
4. **Kubernetes** erstellt Trident Node Pods auf Nodes, auf denen Trident Node Pod  $n$  nicht ausgeführt wird. So wird sichergestellt, dass auf einem Node nie mehr als ein Trident Node Pod einer beliebigen Version vorhanden ist.

## Aktualisieren Sie eine Trident-Installation mit Trident Operator oder Helm

Sie können Trident mit dem Trident-Operator entweder manuell oder mit Helm aktualisieren. Sie können von einer Trident-Bedienerinstallation auf eine andere Trident-Bedienerinstallation aktualisieren oder von einer Installation auf eine Trident-Bedienerversion aktualisieren `tridentctl`. Vor dem Upgrade einer Trident-Bedienerinstallation überprüfen ["Wählen Sie eine Aktualisierungsmethode aus"](#).

### Aktualisieren einer manuellen Installation

Sie können von einer Installation eines Trident Operators mit Cluster-Umfang auf eine andere Installation eines Trident Operators mit Cluster-Umfang aktualisieren. Alle Trident-Versionen 21.01 und höher verwenden einen Clusteroperator.



Um ein Upgrade von Trident durchzuführen, das mit dem Namespace-Skopierten-Operator (Versionen 20.07 bis 20.10) installiert wurde, verwenden Sie die Upgrade-Anweisungen für ["Ihre installierte Version"](#) von Trident.

### Über diese Aufgabe

Trident bietet eine Bundle-Datei, mit der Sie den Operator installieren und zugehörige Objekte für Ihre Kubernetes-Version erstellen können.

- Verwenden Sie für Cluster mit Kubernetes 1.24 "[Bundle\\_pre\\_1\\_25.yaml](#)".
- Verwenden Sie für Cluster mit Kubernetes 1.25 oder höher "[Bundle\\_Post\\_1\\_25.yaml](#)".

## Bevor Sie beginnen

Stellen Sie sicher, dass Sie ein Kubernetes Cluster verwenden "[Eine unterstützte Kubernetes Version](#)", das ausgeführt wird.

## Schritte

1. Überprüfen Sie Ihre Trident-Version:

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

2. Löschen Sie den Trident-Operator, der zur Installation der aktuellen Trident-Instanz verwendet wurde. Wenn Sie beispielsweise ein Upgrade von 23.07 durchführen, führen Sie den folgenden Befehl aus:

```
kubectl delete -f 23.07.0/trident-installer/deploy/<bundle.yaml> -n  
trident
```

3. Wenn Sie Ihre Erstinstallation mithilfe von Attributen angepasst haben `TridentOrchestrator`, können Sie das Objekt bearbeiten `TridentOrchestrator`, um die Installationsparameter zu ändern. Dies kann auch Änderungen umfassen, die an der Angabe gespiegelter Trident- und CSI-Image-Register für den Offline-Modus vorgenommen wurden, Debug-Protokolle aktivieren oder Geheimnisse für die Bildausziehung angeben.
4. Installieren Sie Trident mit der richtigen YAML-Bundle-Datei für Ihre Umgebung, wobei `<bundle.yaml>` `bundle_pre_1_25.yaml` `bundle_post_1_25.yaml` auf Ihrer Kubernetes-Version basiert. Wenn Sie beispielsweise Trident 25.02 installieren, führen Sie den folgenden Befehl aus:

```
kubectl create -f 25.02.0/trident-installer/deploy/<bundle.yaml> -n  
trident
```

## Aktualisieren einer Helm-Installation

Sie können eine Trident Helm-Installation aktualisieren.



Wenn Sie ein Kubernetes-Cluster von 1.24 auf 1.25 oder höher aktualisieren, auf dem Trident installiert ist, müssen Sie `values.yaml` aktualisieren, um den `helm upgrade` Befehl auf `true` festzulegen `excludePodSecurityPolicy` oder hinzuzufügen `--set excludePodSecurityPolicy=true`, bevor Sie das Cluster aktualisieren können.

Wenn Sie Ihr Kubernetes-Cluster bereits von 1.24 auf 1.25 aktualisiert haben, ohne das Trident Helm zu aktualisieren, schlägt das Helm Upgrade fehl. Führen Sie die folgenden Schritte aus, damit das Ruder-Upgrade durchgeführt wird:

1. Installieren Sie das Helm-mapkubeapis Plugin von <https://github.com/helm/helm-mapkubeapis>.
2. Führen Sie einen Probelauf für die Trident-Version im Namespace durch, in dem Trident installiert ist. Hier werden die Ressourcen aufgelistet, die bereinigt werden.

```
helm mapkubeapis --dry-run trident --namespace trident
```

3. Führen Sie einen vollständigen Durchlauf mit Ruder durch, um die Bereinigung durchzuführen.

```
helm mapkubeapis trident --namespace trident
```

## Schritte

1. Wenn Sie "Trident mit Helm installiert", können Sie verwenden `helm upgrade trident netapp-trident/trident-operator --version 100.2502.0`, um ein Upgrade in einem Schritt. Wenn Sie den Helm Repo nicht hinzugefügt haben oder ihn nicht zum Upgrade verwenden können:
  - a. Laden Sie die neueste Trident-Version von "[Die Sektion Assets auf GitHub](#)" herunter.
  - b. Verwenden Sie den `helm upgrade` Befehl where zeigt die Version an `trident-operator-25.02.0.tgz`, auf die Sie aktualisieren möchten.

```
helm upgrade <name> trident-operator-25.02.0.tgz
```



Wenn Sie während der Erstinstallation benutzerdefinierte Optionen festlegen (z. B. `private`, gespiegelte Registrierungen für Trident- und CSI-Images angeben), fügen Sie den Befehl mit `--set` an `helm upgrade`, um sicherzustellen, dass diese Optionen im Aktualisierungsbefehl enthalten sind, andernfalls werden die Werte auf die Standardeinstellung zurückgesetzt.

2. Führen Sie aus `helm list`, um zu überprüfen, ob die Karte und die App-Version aktualisiert wurden. Ausführen `tridentctl logs`, um alle Debug-Meldungen zu überprüfen.

## Upgrade von einer `tridentctl` Installation auf einen Trident-Operator

Sie können von einer Installation aus auf die neueste Version des Trident-Bedieners aktualisieren `tridentctl`. Die vorhandenen Back-Ends und VES stehen automatisch zur Verfügung.



Bevor Sie zwischen den Installationsmethoden wechseln, lesen Sie "[Wechseln zwischen den Installationsmethoden](#)".

## Schritte

1. Laden Sie die neueste Trident Version herunter.

```
# Download the release required [25.02.0]
mkdir 25.02.0
cd 25.02.0
wget
https://github.com/NetApp/trident/releases/download/v25.02.0/trident-
installer-25.02.0.tar.gz
tar -xf trident-installer-25.02.0.tar.gz
cd trident-installer
```

2. Erstellen Sie die `tridentorchestrator` CRD aus dem Manifest.

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.yaml
```

3. Stellen Sie den Clusteroperator im selben Namespace bereit.

```
kubectl create -f deploy/<bundle-name.yaml>

serviceaccount/trident-operator created
clusterrole.rbac.authorization.k8s.io/trident-operator created
clusterrolebinding.rbac.authorization.k8s.io/trident-operator created
deployment.apps/trident-operator created
podsecuritypolicy.policy/tridentoperatorpods created

#Examine the pods in the Trident namespace
NAME                      READY   STATUS    RESTARTS   AGE
trident-controller-79df798bdc-m79dc   6/6     Running   0          150d
trident-node-linux-xrst8            2/2     Running   0          150d
trident-operator-5574dbbc68-nthjv    1/1     Running   0          1m30s
```

4. Erstellen Sie ein `TridentOrchestrator` CR für die Installation von Trident.

```

cat deploy/crds/tridentorchestrator_cr.yaml
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident

kubectl create -f deploy/crds/tridentorchestrator_cr.yaml

#Examine the pods in the Trident namespace
NAME                      READY   STATUS    RESTARTS   AGE
trident-csi-79df798bdc-m79dc   6/6     Running   0          1m
trident-csi-xrst8            2/2     Running   0          1m
trident-operator-5574dbbc68-nthjv  1/1     Running   0          5m41s

```

- Bestätigen Sie, dass das Upgrade von Trident auf die beabsichtigte Version durchgeführt wurde.

```

kubectl describe torc trident | grep Message -A 3

Message:          Trident installed
Namespace:        trident
Status:           Installed
Version:          v25.02.0

```

## Upgrade mit tridentctl

Sie können eine vorhandene Trident-Installation ganz einfach mit aktualisieren tridentctl.

### Über diese Aufgabe

Die Deinstallation und Neuinstallation von Trident dient als Upgrade. Wenn Sie Trident deinstallieren, werden die Persistent Volume Claim (PVC) und das Persistent Volume (PV), die von der Trident-Bereitstellung verwendet werden, nicht gelöscht. Bereits bereitgestellte PVS bleiben verfügbar, während Trident offline ist, und Trident stellt Volumes für alle PVCs bereit, die in der Zwischenzeit erstellt werden, nachdem sie wieder online sind.

### Bevor Sie beginnen

Überprüfen Sie "[Wählen Sie eine Aktualisierungsmethode aus](#)" vor dem Upgrade mit tridentctl.

### Schritte

- Führen Sie den Deinstallationsbefehl in tridentctl aus, um alle mit Trident verbundenen Ressourcen mit Ausnahme der CRDs und zugehörigen Objekte zu entfernen.

```
./tridentctl uninstall -n <namespace>
```

2. Installieren Sie Trident neu. Siehe "[Installieren Sie Trident mit tridentctl](#)".



Unterbrechen Sie den Upgrade-Prozess nicht. Stellen Sie sicher, dass das Installationsprogramm bis zum Abschluss ausgeführt wird.

## **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 BESCHRÄNKKT 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, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT 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 IRGENDERWEINER 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.