



Wissen und Unterstützung

Trident

NetApp
October 29, 2026

Inhalt

Wissen und Unterstützung	1
Häufig gestellte Fragen	1
Allgemeine Fragen	1
Installieren und verwenden Sie Trident auf einem Kubernetes-Cluster	1
Fehlerbehebung und Support	2
Trident aktualisieren	4
Backends und Volumes verwalten	4
Fehlerbehebung	8
Allgemeine Fehlerbehebung	8
Fehlgeschlagene Trident-Bereitstellung mit dem Operator	10
Fehlgeschlagene Trident-Bereitstellung mit <code>tridentctl</code>	11
Trident und CRDs vollständig entfernen	12
NVMe-Knoten-Unstaging-Fehler mit RWX-Raw-Block-Namespaces auf Kubernetes 1.26	13
NFSv4.2-Clients melden „ungültiges Argument“ nach dem Upgrade von ONTAP, wenn sie erwarten, dass „v4.2-xattr“ aktiviert ist	13
Support	14
Trident Support-Lebenszyklus	14
Selbsthilfe	14
Community-Support	14
NetApp technische Unterstützung	15
Für weitere Informationen	15

Wissen und Unterstützung

Häufig gestellte Fragen

Hier finden Sie Antworten auf häufig gestellte Fragen zur Installation, Konfiguration, Aktualisierung und Fehlerbehebung von Trident.

Allgemeine Fragen

Wie häufig wird Trident veröffentlicht?

Ab der Version 24.02 wird Trident alle vier Monate veröffentlicht: Februar, Juni und Oktober.

Unterstützt Trident alle Funktionen, die in einer bestimmten Version von Kubernetes veröffentlicht werden?

Trident unterstützt in Kubernetes üblicherweise keine Alpha-Funktionen. Trident könnte Beta-Funktionen innerhalb der zwei Trident-Versionen unterstützen, die auf die Kubernetes-Beta-Version folgen.

Hat Trident Abhängigkeiten von anderen NetApp Produkten für seine Funktionsweise?

Trident hat keine Abhängigkeiten von anderen NetApp Softwareprodukten und funktioniert als eigenständige Anwendung. Sie sollten jedoch ein NetApp Backend-Speichergerät haben.

Wie kann ich vollständige Trident-Konfigurationsdetails erhalten?

Verwenden Sie den `tridentctl get` Befehl, um weitere Informationen zu Ihrer Trident-Konfiguration zu erhalten.

Kann ich Kennzahlen darüber erhalten, wie Speicher von Trident bereitgestellt wird?

Ja. Prometheus-Endpunkte können verwendet werden, um Informationen über den Betrieb von Trident zu erfassen, wie die Anzahl der verwalteten Backends, die Anzahl der bereitgestellten Volumes, den Datenverbrauch in Bytes und so weiter. Sie können auch ["Cloud Insights"](#) für Überwachung und Analyse verwenden.

Verändert sich die Benutzererfahrung bei der Verwendung von Trident als CSI-Provisioner?

Nein. Hinsichtlich Benutzerfreundlichkeit und Funktionalität gibt es keine Änderungen. Der verwendete Provisionierungsname ist `csi.trident.netapp.io`. Diese Methode der Installation von Trident wird empfohlen, wenn Sie alle neuen Funktionen aktueller und zukünftiger Versionen nutzen möchten.

Installieren und verwenden Sie Trident auf einem Kubernetes-Cluster

Unterstützt Trident eine Offline-Installation aus einer privaten Registry?

Ja, Trident kann offline installiert werden. Weitere Informationen enthält ["Erfahren Sie mehr über die Trident-Installation"](#).

Kann ich Trident remote installieren?

Ja. Trident 18.10 und höher unterstützen die Remote-Installationsfunktion von jedem Rechner, der `kubectl` Zugriff auf den Cluster hat. Nachdem `kubectl` der Zugriff verifiziert wurde (zum Beispiel, indem Sie einen `kubectl get nodes` Befehl vom Remote-Rechner initiieren, um dies zu überprüfen), folgen Sie den Installationsanweisungen.

Kann ich Hochverfügbarkeit mit Trident konfigurieren?

Trident wird als Kubernetes Deployment (ReplicaSet) mit einer Instanz installiert und verfügt daher über integrierte Hochverfügbarkeit. Sie sollten die Anzahl der Replikate in der Implementierung nicht erhöhen. Wenn der Knoten, auf dem Trident installiert ist, verloren geht oder der Pod anderweitig nicht zugänglich ist, stellt Kubernetes den Pod automatisch auf einem gesunden Knoten in Ihrem Cluster erneut bereit. Trident ist nur Steuerungsebene, daher sind aktuell eingebundene Pods nicht betroffen, wenn Trident neu bereitgestellt wird.

Benötigt Trident Zugriff auf den Namespace kube-system?

Trident liest vom Kubernetes API Server, um festzustellen, wann Anwendungen neue PVCs anfordern, daher benötigt es Zugriff auf kube-system.

Welche Rollen und Privilegien werden von Trident verwendet?

Der Trident-Installer erstellt eine Kubernetes-ClusterRole, die spezifischen Zugriff auf die PersistentVolume-, PersistentVolumeClaim-, StorageClass- und Secret-Ressourcen des Kubernetes-Clusters hat. Weitere Informationen enthält ["tridentctl-Installation anpassen"](#).

Kann ich die exakten Manifestdateien, die Trident für die Installation verwendet, lokal generieren?

Sie können die von Trident für die Installation verwendeten Manifestdateien bei Bedarf lokal generieren und bearbeiten. Weitere Informationen enthält ["tridentctl-Installation anpassen"](#).

Kann ich dieselbe ONTAP Backend-SVM für zwei separate Trident Instanzen für zwei separate Kubernetes-Cluster verwenden?

Obwohl es nicht empfohlen wird, können Sie dieselbe Backend-SVM für zwei Trident-Instanzen verwenden. Geben Sie während der Installation für jede Instanz einen eindeutigen Volume-Namen an und/oder definieren Sie einen eindeutigen `StoragePrefix` Parameter in der `setup/backend.json` Datei. Dies soll sicherstellen, dass nicht dasselbe FlexVol Volume für beide Instanzen verwendet wird.

Ist es möglich, Trident unter ContainerLinux (formerly CoreOS) zu installieren?

Trident ist einfach ein Kubernetes pod und kann überall dort installiert werden, wo Kubernetes läuft.

Kann ich Trident mit NetApp Cloud Volumes ONTAP verwenden?

Ja, Trident wird auf AWS, Google Cloud und Azure unterstützt.

Fehlerbehebung und Support

Unterstützt NetApp Trident?

Obwohl Trident Open Source ist und kostenlos zur Verfügung gestellt wird, wird es von NetApp vollständig unterstützt, sofern Ihr NetApp Backend unterstützt wird.

Wie kann ich einen Support-Fall eröffnen?

Um einen Supportfall zu eröffnen, führen Sie einen der folgenden Schritte aus:

1. Wenden Sie sich an Ihren Support Account Manager und lassen Sie sich bei der Erstellung eines Tickets helfen.
2. Eröffnen Sie einen Supportfall, indem Sie ["NetApp Support"](#) kontaktieren.

Wie erstelle ich ein Support-Log-Bundle?

Sie können ein Support-Bundle erstellen, indem Sie `tridentctl logs -a` ausführen. Zusätzlich zu den im Bundle erfassten Protokollen erfassen Sie das Kubelet-Protokoll, um die Mount-Probleme auf der Kubernetes-Seite zu diagnostizieren. Die Anweisungen zum Abrufen des Kubelet-Protokolls variieren je nachdem, wie Kubernetes installiert ist.

Was muss ich tun, wenn ich eine Anfrage für ein neues Feature stellen möchte?

Erstellen Sie ein Ticket auf ["Trident Github"](#) und erwähnen Sie **RFE** im Betreff und in der Beschreibung des Tickets.

Wo kann ich einen Defekt melden?

Erstellen Sie ein Ticket auf ["Trident Github"](#). Stellen Sie sicher, dass Sie alle notwendigen Informationen und Protokolle zu dem Problem angeben.

Was passiert, wenn ich eine kurze Frage zu Trident habe, die ich klären möchte? Gibt es eine Community oder ein Forum?

Bei Fragen, Problemen oder Anliegen kontaktieren Sie uns bitte über unseren Trident ["Discord-Kanal"](#) oder GitHub.

Das Passwort meines Speichersystems wurde geändert und Trident funktioniert nicht mehr, wie kann ich es wiederherstellen?

Aktualisieren Sie das Passwort des Backends mit `tridentctl update backend myBackend -f </path/to_new_backend.json> -n trident`. Ersetzen Sie `myBackend` im Beispiel durch Ihren Backend-Namen und `/path/to_new_backend.json` durch den Pfad zur richtigen `backend.json` Datei.

Trident kann meinen Kubernetes-Knoten nicht finden. Wie behebe ich das?

Es gibt zwei wahrscheinliche Szenarien, warum Trident einen Kubernetes-Knoten nicht finden kann. Dies kann an einem Netzwerkproblem innerhalb von Kubernetes oder an einem DNS-Problem liegen. Das Trident-Knoten-Daemonset, das auf jedem Kubernetes-Knoten läuft, muss mit dem Trident-Controller kommunizieren können, um den Knoten bei Trident zu registrieren. Wenn nach der Installation von Trident Netzwerkänderungen vorgenommen wurden, tritt dieses Problem nur bei neuen Kubernetes-Knoten auf, die dem Cluster hinzugefügt werden.

Wenn das Trident-Pod zerstört wird, gehen die Daten verloren?

Daten gehen nicht verloren, wenn der Trident-Pod zerstört wird. Trident-Metadaten werden in CRD-Objekten gespeichert. Alle von Trident bereitgestellten PVs funktionieren weiterhin normal.

Trident aktualisieren

Kann ich direkt von einer älteren Version auf eine neuere Version aktualisieren (einige Versionen überspringen)?

NetApp unterstützt das Upgrade von Trident von einer Hauptversion auf die nächstfolgende Hauptversion. Sie können von Version 18.xx auf 19.xx, von 19.xx auf 20.xx und so weiter aktualisieren. Sie sollten das Upgrade in einer Testumgebung testen, bevor Sie die Implementierung in der Produktion durchführen.

Ist es möglich, Trident auf eine frühere Version zurückzusetzen?

Falls nach einem Upgrade Fehler, Abhängigkeitsprobleme oder ein fehlgeschlagenes bzw. unvollständiges Upgrade auftreten, sollten Sie ["Trident deinstallieren"](#) und die vorherige Version gemäß der entsprechenden Anleitung für diese Version neu installieren. Dies ist die einzige empfohlene Methode, um auf eine frühere Version zurückzukehren.

Backends und Volumes verwalten

Muss ich sowohl Management- als auch DataLIFs in einer ONTAP Backend-Definitionsdatei definieren?

Das Management-LIF ist obligatorisch. Das DataLIF variiert:

- ONTAP SAN: Nicht für iSCSI angeben. Trident verwendet ["ONTAP Selective LUN Map"](#) zur Erkennung der iSCSI-LIFs, die für die Einrichtung einer Multipath-Sitzung benötigt werden. Eine Warnung wird generiert, wenn `dataLIF` explizit definiert ist. Details sind in ["ONTAP SAN-Konfigurationsoptionen und Beispiele"](#) zu finden.
- ONTAP NAS: NetApp empfiehlt, `dataLIF` anzugeben. Falls nicht angegeben, ruft Trident `dataLIFs` vom SVM ab. Ein vollqualifizierter Domainname (FQDN) kann für die NFS-Mount-Operationen angegeben werden, wodurch die Erstellung eines Round-Robin-DNS zur Lastverteilung über mehrere `dataLIFs` ermöglicht wird. Weitere Informationen finden Sie unter ["ONTAP NAS-Konfigurationsoptionen und Beispiele"](#).

Kann Trident CHAP für ONTAP Backends konfigurieren?

Ja. Trident unterstützt bidirektionales CHAP für ONTAP Backends. Dies erfordert das Setzen von `useCHAP=true` in Ihrer Backend-Konfiguration.

Wie verwalte ich Export-Richtlinien mit Trident?

Trident kann ab Version 20.04 Exportrichtlinien dynamisch erstellen und verwalten. Dies ermöglicht es dem Speicheradministrator, in seiner Backend-Konfiguration einen oder mehrere CIDR-Blöcke anzugeben und Trident fügt die Knoten-IPs, die in diese Bereiche fallen, zu einer von ihm erstellten Exportrichtlinie hinzu. Auf diese Weise verwaltet Trident automatisch das Hinzufügen und Löschen von Regeln für Knoten mit IPs innerhalb der angegebenen CIDRs.

Können IPv6-Adressen für die Management- und DataLIFs verwendet werden?

Trident unterstützt die Definition von IPv6-Adressen für:

- `managementLIF` and `dataLIF` für ONTAP NAS-Backends.
- `managementLIF` für ONTAP SAN backends. Sie können `dataLIF` auf einem ONTAP SAN-Backend nicht angeben.

Trident muss mit dem Flag `--use-ipv6` (für `tridentctl` Installation), `IPv6` (für Trident operator) oder `tridentTPv6` (für Helm installation) installiert werden, damit es über IPv6 funktioniert.

Ist es möglich, das Management-LIF im Backend zu aktualisieren?

Ja, es ist möglich, das Backend-Management-LIF mit dem `tridentctl update backend` Befehl zu aktualisieren.

Ist es möglich, die DataLIF im Backend zu aktualisieren?

Sie können die DataLIF auf `ontap-nas` und ``ontap-nas-economy`` nur aktualisieren.

Kann ich mehrere Backends in Trident für Kubernetes erstellen?

Trident kann viele Backends gleichzeitig unterstützen, entweder mit dem gleichen Treiber oder mit verschiedenen Treibern.

Wie speichert Trident die Backend-Zugangsdaten?

Trident speichert die Backend-Zugangsdaten als Kubernetes Secrets.

Wie wählt Trident ein bestimmtes Backend aus?

Falls die Backend-Attribute nicht verwendet werden können, um automatisch die richtigen Pools für eine Klasse auszuwählen, werden die `storagePools` und `additionalStoragePools` Parameter verwendet, um einen bestimmten Satz von Pools auszuwählen.

Wie kann ich sicherstellen, dass Trident nicht von einem bestimmten Backend bereitstellt?

Der ``excludeStoragePools`` Parameter wird verwendet, um die Menge der Pools zu filtern, die Trident für die Bereitstellung verwendet, und entfernt alle Pools, die übereinstimmen.

Wenn mehrere Backends desselben Typs vorhanden sind, wie wählt Trident das zu verwendende Backend aus?

Wenn mehrere Backends desselben Typs konfiguriert sind, wählt Trident das passende Backend basierend auf den Parametern in `StorageClass` und `PersistentVolumeClaim` aus. Wenn zum Beispiel mehrere `ontap-nas` Driver Backends vorhanden sind, versucht Trident, die Parameter in `StorageClass` und `PersistentVolumeClaim` zusammen abzugleichen und ein Backend zu finden, das die Anforderungen, die in `StorageClass` und `PersistentVolumeClaim` aufgeführt sind, erfüllen kann. Wenn mehrere Backends die Anfrage erfüllen, wählt Trident zufällig eines davon aus.

Unterstützt Trident bidirektionales CHAP mit Element/SolidFire?

Ja.

Wie stellt Trident Qtrees auf einem ONTAP-Volume bereit? Wie viele Qtrees können auf einem einzelnen Volume bereitgestellt werden?

Der `ontap-nas-economy` Treiber erstellt bis zu 200 Qtrees im selben FlexVol Volume (konfigurierbar zwischen 50 und 300), 100.000 Qtrees pro Clusterknoten und 2,4M pro Cluster. Wenn Sie einen neuen `PersistentVolumeClaim` Qtree eingeben, der vom Economy-Treiber bedient wird, prüft der Treiber, ob bereits ein FlexVol Volume existiert, das den neuen Qtree bedienen kann. Wenn das FlexVol Volume, das den Qtree bedienen kann, nicht existiert, wird ein neues FlexVol Volume erstellt.

Wie kann ich Unix-Berechtigungen für auf ONTAP NAS bereitgestellte Volumes festlegen?

Sie können Unix-Berechtigungen für das von Trident bereitgestellte Volume festlegen, indem Sie einen Parameter in der Backend-Definitionsdatei setzen.

Wie kann ich beim Bereitstellen eines Volumes einen expliziten Satz von ONTAP NFS-Mount-Optionen konfigurieren?

Standardmäßig setzt Trident bei Kubernetes keine Mount-Optionen. Um die Mount-Optionen in der Kubernetes-Speicherklasse festzulegen, folgen Sie dem angegebenen Beispiel ["hier"](#).

Wie kann ich die bereitgestellten Volumes auf eine bestimmte Exportrichtlinie einstellen?

Um den entsprechenden Hosts den Zugriff auf ein Volume zu ermöglichen, verwenden Sie den `exportPolicy` Parameter, der in der Backend-Definitionsdatei konfiguriert ist.

Wie stelle ich die Volumenverschlüsselung über Trident mit ONTAP ein?

Sie können die Verschlüsselung auf dem von Trident bereitgestellten Volume mithilfe des Verschlüsselungsparameters in der Backend-Definitionsdatei aktivieren. Weitere Informationen finden Sie unter: ["Wie Trident mit NVE und NAE zusammenarbeitet"](#)

Was ist der beste Weg, QoS für ONTAP über Trident zu implementieren?

Verwenden Sie `StorageClasses` zur Implementierung von QoS für ONTAP.

Wie gebe ich Thin oder Thick Provisioning über Trident an?

Die ONTAP-Treiber unterstützen entweder Thin oder Thick Provisioning. Die ONTAP-Treiber verwenden standardmäßig Thin Provisioning. Wenn Thick Provisioning gewünscht ist, sollten Sie entweder die Backend-Definitionsdatei oder die `StorageClass` konfigurieren. Wenn beide konfiguriert sind, hat `StorageClass` Vorrang. Konfigurieren Sie Folgendes für ONTAP:

1. Auf `StorageClass` das `provisioningType`-Attribut als dick setzen.
2. Aktivieren Sie in der Backend-Definitionsdatei Thick Volumes, indem Sie `backend spaceReserve parameter` als Volume festlegen.

Wie kann ich sicherstellen, dass die verwendeten Volumes nicht gelöscht werden, selbst wenn ich versehentlich das PVC lösche?

Der PVC-Schutz ist ab Kubernetes Version 1.10 automatisch aktiviert.

Kann ich NFS-PVCs, die von Trident erstellt wurden, vergrößern?

Ja. Sie können ein von Trident erstelltes PVC erweitern. Beachten Sie, dass die automatische Volumenvergrößerung eine ONTAP Funktion ist, die für Trident nicht anwendbar ist.

Kann ich ein Volume importieren, während es sich im SnapMirror Data Protection (DP) oder im Offline-Modus befindet?

Der Volume-Import schlägt fehl, wenn sich das externe Volume im DP-Modus befindet oder offline ist. Sie erhalten die folgende Fehlermeldung:

```
Error: could not import volume: volume import failed to get size of
volume: volume <name> was not found (400 Bad Request) command terminated
with exit code 1.
Make sure to remove the DP mode or put the volume online before importing
the volume.
```

Wie wird ein Ressourcenkontingent auf einen NetApp Cluster übertragen?

Kubernetes-Speicherressourcenkontingente sollten funktionieren, solange NetApp Storage über Kapazität verfügt. Wenn der NetApp Storage die Kubernetes-Kontingenteinstellungen aufgrund mangelnder Kapazität nicht einhalten kann, versucht Trident die Bereitstellung, schlägt jedoch fehl.

Kann ich mit Trident Volume Snapshots erstellen?

Ja. Das Erstellen von On-Demand-Volume-Snapshots und Persistent Volumes aus Snapshots wird von Trident unterstützt. Um PVs aus Snapshots zu erstellen, stelle sicher, dass das `VolumeSnapshotDataSource` Feature-Gate aktiviert wurde.

Welche Treiber unterstützen Trident Volume-Snapshots?

Ab heute ist die Unterstützung für On-Demand-Snapshots für unsere `ontap-nas`, `ontap-nas-flexgroup`, `ontap-san`, `ontap-san-economy`, `solidfire-san` und `azure-netapp-files` Backend-Treiber verfügbar.

Wie erstelle ich eine Snapshot-Sicherung eines von Trident mit ONTAP bereitgestellten Volumes?

Dies ist verfügbar auf `ontap-nas`, `ontap-san` und `ontap-nas-flexgroup`-Treibern. Sie können auch ein `snapshotPolicy` für den `ontap-san-economy`-Treiber auf der FlexVol-Ebene angeben.

Dies ist auch auf den `ontap-nas-economy` Treibern verfügbar, jedoch auf der FlexVol Volume-Ebene der Granularität und nicht auf der Qtree-Ebene der Granularität. Um die Möglichkeit zu aktivieren, Snapshots von durch Trident bereitgestellten Volumes zu erstellen, setzen Sie die Backend-Parameteroption `snapshotPolicy` auf die gewünschte Snapshot-Richtlinie, wie sie im ONTAP-Backend definiert ist. Alle vom Storage-Controller erstellten Snapshots sind Trident nicht bekannt.

Kann ich einen Snapshot-Reservierungsprozentsatz für ein über Trident bereitgestelltes Volume festlegen?

Ja, Sie können einen bestimmten Prozentsatz des Speicherplatzes für die Speicherung der Snapshot-Kopien über Trident reservieren, indem Sie das `snapshotReserve` Attribut in der Backend-Definitionsdatei festlegen. Wenn Sie `snapshotPolicy` und `snapshotReserve` in der Backend-Definitionsdatei konfiguriert haben, wird der Snapshot-Reservierungsprozentsatz entsprechend dem im Backend-File angegebenen `snapshotReserve` Prozentsatz festgelegt. Wenn die `snapshotReserve` Prozentzahl nicht angegeben ist, nimmt ONTAP standardmäßig den Snapshot-Reservierungsprozentsatz als 5. Wenn die `snapshotPolicy` Option auf `none` gesetzt ist, beträgt der Snapshot-Reservierungsprozentsatz 0.

Kann ich direkt auf das Volume-Snapshot-Verzeichnis zugreifen und Dateien kopieren?

Ja, Sie können auf das Snapshot-Verzeichnis auf dem von Trident bereitgestellten Volume zugreifen, indem Sie den `snapshotDir` Parameter in der Backend-Definitionsdatei festlegen.

Kann ich SnapMirror für Volumes über Trident einrichten?

Derzeit muss SnapMirror extern über die ONTAP CLI oder OnCommand System Manager eingerichtet werden.

Wie kann ich persistente Volumes auf einen bestimmten ONTAP-Snapshot wiederherstellen?

Um ein Volume auf einen ONTAP-Snapshot wiederherzustellen, führen Sie die folgenden Schritte aus:

1. Versetzen Sie den Anwendungspod, der das Persistent Volume verwendet, in den Ruhezustand.
2. Stellen Sie den erforderlichen Snapshot über die ONTAP CLI oder OnCommand System Manager wieder her.
3. Starten Sie den Anwendungspod neu.

Kann Trident Volumes auf SVMs bereitstellen, die mit einem Load-Sharing Mirror konfiguriert sind?

Für Root-Volumes von SVMs, die Daten über NFS bereitstellen, können Load-Sharing-Mirrors erstellt werden. ONTAP aktualisiert Load-Sharing-Mirrors automatisch für Volumes, die von Trident erstellt wurden. Dies kann zu Verzögerungen beim Mounten von Volumes führen. Wenn mehrere Volumes mit Trident erstellt werden, hängt die Bereitstellung eines Volumes davon ab, dass ONTAP den Load-Sharing-Mirror aktualisiert.

Wie kann ich die Speicherklassennutzung für jeden Kunden/Mandanten separat aufschlüsseln?

Kubernetes erlaubt keine Speicherklassen in Namespaces. Sie können jedoch Kubernetes verwenden, um die Nutzung einer bestimmten Speicherklasse pro Namespace mithilfe von Speicherressourcenquoten (Storage Resource Quotas), die pro Namespace gelten, einzuschränken. Um einem bestimmten Namespace den Zugriff auf einen bestimmten Speicher zu verweigern, setzen Sie die Ressourcenquote für diese Speicherklasse auf 0.

Fehlerbehebung

Nutzen Sie die hier bereitgestellten Hinweise zur Fehlerbehebung bei Problemen, die während der Installation und Verwendung von Trident auftreten können.



Für Hilfe mit Trident erstellen Sie ein Support-Bundle mit `tridentctl logs -a -n trident` und senden Sie es an NetApp Support.

Allgemeine Fehlerbehebung

- Falls der Trident Pod nicht ordnungsgemäß startet (beispielsweise, wenn der Trident Pod in der ContainerCreating Phase mit weniger als zwei bereiten Containern festhängt), kann das Ausführen von `kubectl -n trident describe deployment trident` und `kubectl -n trident describe pod trident--**` zusätzliche Erkenntnisse liefern. Das Abrufen von kubelet-Logs (zum Beispiel über `journalctl -xeu kubelet`) kann ebenfalls hilfreich sein.
- Falls die Trident-Protokolle nicht genügend Informationen enthalten, können Sie versuchen, den Debug-Modus für Trident zu aktivieren, indem Sie das `-d` Flag an den Installationsparameter übergeben, abhängig von Ihrer Installationsoption.

Bestätigen Sie dann, dass Debug gesetzt ist, indem Sie `./tridentctl logs -n trident` verwenden und im Protokoll nach `level=debug msg` suchen.

Installiert mit Operator

```
kubectl patch torc trident -n <namespace> --type=merge -p
'{"spec":{"debug":true}}'
```

Dadurch werden alle Trident Pods neu gestartet, was einige Sekunden dauern kann. Sie können dies überprüfen, indem Sie die Spalte „AGE“ in der Ausgabe von `kubectl get pod -n trident` beobachten.

Für Trident 20.07 und 20.10 verwenden Sie `tprov` anstelle von `torc`.

Mit Helm installiert

```
helm upgrade <name> trident-operator-21.07.1-custom.tgz --set
tridentDebug=true`
```

Installiert mit tridentctl

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

- Sie können auch Debug-Logs für jedes Backend erhalten, indem Sie `debugTraceFlags` in Ihre Backend-Definition aufnehmen. Fügen Sie beispielsweise `debugTraceFlags: {"api":true, "method":true, }` hinzu, um API-Aufrufe und Methodendurchläufe in den Trident-Logs zu erhalten. Bestehende Backends können `debugTraceFlags` mit einem `tridentctl backend update` konfiguriert werden.
- Bei Verwendung von Red Hat Enterprise Linux CoreOS (RHCOS) muss sichergestellt werden, dass `iscsid` auf den Worker-Knoten aktiviert und standardmäßig gestartet ist. Dies kann durch die Verwendung von OpenShift MachineConfigs oder durch Anpassen der Ignition-Vorlagen erfolgen.
- Ein häufiges Problem, das bei der Verwendung von Trident mit ["Azure NetApp Files"](#) auftreten kann, besteht darin, dass die Mandanten- und Client-Secrets aus einer App-Registrierung mit unzureichenden Berechtigungen stammen. Eine vollständige Liste der Trident-Anforderungen finden Sie unter ["Azure NetApp Files"](#) Konfiguration.
- Wenn es Probleme beim Einbinden eines PV in einen Container gibt, stellen Sie sicher, dass `rpcbind` installiert und ausgeführt wird. Verwenden Sie den erforderlichen Paketmanager für das Host-Betriebssystem und prüfen Sie, ob `rpcbind` läuft. Sie können den Status des `rpcbind` Dienstes überprüfen, indem Sie einen `systemctl status rpcbind` oder einen entsprechenden Befehl ausführen.
- Wenn ein Trident-Backend meldet, dass es sich im `failed` Status befindet, obwohl es zuvor funktioniert hat, liegt dies wahrscheinlich an einer Änderung der mit dem Backend verbundenen SVM-/Admin-Zugangsdaten. Das Aktualisieren der Backend-Informationen mit `tridentctl update backend` oder ein Neustart des Trident-Pods behebt dieses Problem.
- Falls bei der Installation von Trident mit Docker als Container-Laufzeitumgebung Berechtigungsprobleme auftreten, versuchen Sie die Installation von Trident mit dem `--in cluster=false` Flag. Dadurch wird kein Installer-Pod verwendet und Berechtigungsprobleme, die durch den `trident-installer` Benutzer verursacht werden, werden vermieden.
- Verwenden Sie das `uninstall` parameter `<Uninstalling Trident>` zur Bereinigung nach einem

fehlgeschlagenen Lauf. Standardmäßig entfernt das Skript die von Trident erstellten CRDs nicht, sodass eine Deinstallation und Neuinstallation auch in einer laufenden Bereitstellung sicher ist.

- Wenn Sie auf eine frühere Version von Trident downgraden möchten, führen Sie zuerst den `tridentctl uninstall` Befehl aus, um Trident zu entfernen. Laden Sie die gewünschte "[Trident Version](#)" herunter und installieren Sie sie mit dem `tridentctl install` Befehl.
- Nach einer erfolgreichen Installation, wenn eine PVC in der Pending-Phase feststeckt, kann das Ausführen von `kubectl describe pvc` zusätzliche Informationen darüber liefern, warum Trident es nicht geschafft hat, eine PV für diese PVC bereitzustellen.

Fehlgeschlagene Trident-Bereitstellung mit dem Operator

Wenn Sie Trident mithilfe des Operators bereitstellen, ändert sich der Status von `TridentOrchestrator` `Installing` zu `Installed`. Wenn Sie den `Failed` Status beobachten und der Operator sich nicht selbst wiederherstellen kann, sollten Sie die Protokolle des Operators mit folgendem Befehl überprüfen:

```
tridentctl logs -l trident-operator
```

Das Verfolgen der Logs des `trident-operator`-Containers kann darauf hinweisen, wo das Problem liegt. Ein solches Problem könnte beispielsweise darin bestehen, dass die erforderlichen Container-Images in einer abgeschotteten Umgebung nicht von Upstream-Registries abgerufen werden können.

Um zu verstehen, warum die Installation von Trident fehlgeschlagen ist, sollten Sie sich den `TridentOrchestrator` Status ansehen.

```
kubectl describe torc trident-2
Name:          trident-2
Namespace:
Labels:        <none>
Annotations:   <none>
API Version:   trident.netapp.io/v1
Kind:          TridentOrchestrator
...
Status:
  Current Installation Params:
    IPv6:
    Autosupport Hostname:
    Autosupport Image:
    Autosupport Proxy:
    Autosupport Serial Number:
    Debug:
    Image Pull Secrets:          <nil>
    Image Registry:
    k8sTimeout:
    Kubelet Dir:
    Log Format:
    Silence Autosupport:
```

```

    Trident Image:
  Message:          Trident is bound to another CR 'trident'
  Namespace:        trident-2
  Status:           Error
  Version:
Events:
  Type      Reason      Age           From           Message
  ----      -
Warning    Error        16s (x2 over 16s)  trident-operator.netapp.io  Trident
is bound to another CR 'trident'

```

Dieser Fehler weist darauf hin, dass bereits eine `TridentOrchestrator` existiert, die zur Installation von Trident verwendet wurde. Da jeder Kubernetes-Cluster nur eine Instanz von Trident haben kann, stellt der Operator sicher, dass zu jedem Zeitpunkt nur eine aktive `TridentOrchestrator` existiert, die er erstellen kann.

Darüber hinaus kann die Beobachtung des Zustands der Trident-Pods oft darauf hinweisen, ob etwas nicht stimmt.

```

kubectl get pods -n trident

NAME                                READY   STATUS              RESTARTS
AGE
trident-csi-4p5kq                   1/2     ImagePullBackOff    0
5m18s
trident-csi-6f45bfd8b6-vfrkw       4/5     ImagePullBackOff    0
5m19s
trident-csi-9q5xc                   1/2     ImagePullBackOff    0
5m18s
trident-csi-9v95z                   1/2     ImagePullBackOff    0
5m18s
trident-operator-766f7b8658-ldzsv  1/1     Running             0
8m17s

```

Sie können deutlich sehen, dass die Pods nicht vollständig initialisiert werden können, weil ein oder mehrere Container-Images nicht abgerufen wurden.

Um das Problem zu beheben, sollten Sie die `TridentOrchestrator` CR bearbeiten. Alternativ können Sie `TridentOrchestrator` löschen und eine neue mit der geänderten und korrekten Definition erstellen.

Fehlgeschlagene Trident-Bereitstellung mit `tridentctl`

Um herauszufinden, was schiefgelaufen ist, können Sie das Installationsprogramm erneut mit dem `-d` Argument ausführen, das den Debug-Modus aktiviert und Ihnen hilft, das Problem zu verstehen:

```
./tridentctl install -n trident -d
```

Nachdem das Problem behoben wurde, können Sie die Installation wie folgt bereinigen und dann den `tridentctl install` Befehl erneut ausführen:

```
./tridentctl uninstall -n trident
INFO Deleted Trident deployment.
INFO Deleted cluster role binding.
INFO Deleted cluster role.
INFO Deleted service account.
INFO Removed Trident user from security context constraint.
INFO Trident uninstallation succeeded.
```

Trident und CRDs vollständig entfernen

Sie können Trident und alle erstellten CRDs und zugehörigen benutzerdefinierten Ressourcen vollständig entfernen.



Dies kann nicht rückgängig gemacht werden. Führen Sie dies nur durch, wenn Sie eine komplett neue Installation von Trident wünschen. Um Trident zu deinstallieren, ohne die CRDs zu entfernen, siehe ["Trident deinstallieren"](#).

Trident Operator

So deinstallieren Sie Trident und entfernen CRDs vollständig mit dem Trident Operator:

```
kubectl patch torc <trident-orchestrator-name> --type=merge -p
'{"spec":{"wipeout":["crds"],"uninstall":true}}'
```

Helm

So deinstallieren Sie Trident und entfernen CRDs vollständig mit Helm:

```
kubectl patch torc trident --type=merge -p
'{"spec":{"wipeout":["crds"],"uninstall":true}}'
```

`tridentctl`

Um CRDs nach der Deinstallation von Trident vollständig zu entfernen, verwenden Sie `tridentctl`

```
tridentctl obliviate crd
```

NVMe-Knoten-Unstaging-Fehler mit RWX-Raw-Block-Namespaces auf Kubernetes 1.26

Wenn Sie Kubernetes 1.26 ausführen, kann das Unstaging von Knoten fehlschlagen, wenn NVMe/TCP mit RWX Raw Block Namespaces verwendet wird. Die folgenden Szenarien bieten eine Problemumgehung für den Fehler. Alternativ können Sie Kubernetes auf 1.27 aktualisieren.

Namespace und Pod gelöscht

Stellen Sie sich ein Szenario vor, in dem ein von Trident verwalteter Namespace (NVMe-Persistent Volume) an einen Pod angehängt ist. Wenn Sie den Namespace direkt vom ONTAP Backend löschen, bleibt der Unstaging-Prozess nach dem Versuch, den Pod zu löschen, hängen. Dieses Szenario hat keine Auswirkungen auf den Kubernetes-Cluster oder andere Funktionen.

Problemumgehung

Hängen Sie das persistente Volume (das diesem Namespace entspricht) vom jeweiligen Knoten aus und löschen Sie es.

Blockierte dataLIFs

If you block (or bring down) all the dataLIFs of the NVMe Trident backend, the unstaging process gets stuck when you attempt to delete the pod. In this scenario, you cannot run any NVMe CLI commands on the Kubernetes node.

.Problemumgehung

Aktivieren Sie die dataLIFs, um die volle Funktionalität wiederherzustellen.

Gelöschte Namespace-Zuordnung

If you remove the `hostNQN` of the worker node from the corresponding subsystem, the unstaging process gets stuck when you attempt to delete the pod. In this scenario, you cannot run any NVMe CLI commands on the Kubernetes node.

.Problemumgehung

Fügen Sie das `hostNQN` zurück zum Subsystem hinzu.

NFSv4.2-Clients melden „ungültiges Argument“ nach dem Upgrade von ONTAP, wenn sie erwarten, dass „v4.2-xattrs“ aktiviert ist

Nach dem Upgrade von ONTAP können NFSv4.2-Clients beim Versuch, NFSv4.2-Exporte einzubinden, „invalid argument“-Fehler melden. Dieses Problem tritt auf, wenn die `v4.2-xattrs` Option auf der SVM nicht aktiviert ist. Abhilfe: Aktivieren Sie die `v4.2-xattrs` Option auf der SVM oder aktualisieren Sie auf ONTAP 9.12.1 oder höher, wo diese Option standardmäßig aktiviert ist.

Support

NetApp bietet Unterstützung für Trident auf verschiedene Weise. Umfangreiche kostenlose Selbsthilfeoptionen stehen rund um die Uhr zur Verfügung, wie zum Beispiel Knowledgebase (KB)-Artikel und ein Discord-Kanal.

Trident Support-Lebenszyklus

Trident bietet drei Supportstufen basierend auf Ihrer Version. Weitere Informationen enthält ["NetApp Softwareversionsunterstützung für Definitionen"](#).

Volle Unterstützung

Trident bietet vollen Support für zwölf Monate ab dem Veröffentlichungsdatum.

Eingeschränkte Unterstützung

Trident bietet nur eingeschränkten Support für die Monate 13 bis 24 ab dem Veröffentlichungsdatum.

Selbsthilfe

Die Trident-Dokumentation ist für die Monate 25 bis 36 ab dem Veröffentlichungsdatum verfügbar.

Version	Ende der vollständigen Unterstützung	Ende der eingeschränkten Unterstützung	Ende des Self-Support
"26,06"	Juli 2027	Juli 2028	Juli 2029
"26,02"	Februar 2027	Februar 2028	Februar 2029
"25,10"	Oktober 2026	Oktober 2027	Oktober 2028
"25,06"	Juni 2026	Juni 2027	Juni 2028
"25,02"	Februar 2026	Februar 2027	Februar 2028
"24,10"	—	Oktober 2026	Oktober 2027
"24,06"	—	Juni 2026	Juni 2027
"24,02"	—	Februar 2026	Februar 2027
"23,10"	—	—	Oktober 2026
"23,07"	—	—	Juli 2026

Selbsthilfe

Eine vollständige Liste der Artikel zur Fehlerbehebung finden Sie unter ["NetApp Knowledgebase \(Anmeldung erforderlich\)"](#).

Community-Support

Es gibt eine lebendige öffentliche Community von Container-Nutzern (einschließlich Trident-Entwicklern) auf unserer ["Discord-Kanal"](#). Dies ist ein großartiger Ort, um allgemeine Fragen zum Projekt zu stellen und verwandte Themen mit Gleichgesinnten zu diskutieren.

NetApp technische Unterstützung

Um Hilfe mit Trident zu erhalten, erstellen Sie ein Support-Bundle mit `tridentctl logs -a -n trident` und senden Sie es an NetApp Support <Getting Help>.

Für weitere Informationen

- ["Trident-Ressourcen"](#)
- ["Kubernetes Hub"](#)

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.