Bereiten Sie den Knoten „Worker“ vor

Trident

NetApp
January 14, 2026

Inhalt

Bereiten Sie den Knoten „Worker“ vor

Alle Worker-Nodes im Kubernetes-Cluster müssen in der Lage sein, die Volumes, die Sie für Ihre Pods bereitgestellt haben, zu mounten. Um die Worker-Nodes vorzubereiten, müssen Sie auf der Grundlage Ihrer Treiberauswahl NFS-, iSCSI-, NVMe/TCP- oder FC-Tools installieren.

Auswahl der richtigen Werkzeuge

Wenn Sie eine Kombination von Treibern verwenden, sollten Sie alle erforderlichen Tools für Ihre Treiber installieren. Bei aktuellen Versionen von RedHat CoreOS sind die Tools standardmäßig installiert.

NFS Tools

"Installieren Sie die NFS Tools" Wenn Sie: `ontap-nas`, , , `ontap-nas-economy` `ontap-nas-flexgroup` , `azure-netapp-files` `gcp-cvs` .

ISCSI-Tools

"Installieren Sie die iSCSI-Tools" Wenn Sie: `ontap-san`, , `ontap-san-economy` `solidfire-san` .

NVMe-Tools

"Installation der NVMe Tools" Falls Sie das Protokoll Nonvolatile Memory Express (NVMe) over TCP (NVMe/TCP) verwenden `ontap-san`.

> Wir empfehlen ONTAP 9.12 oder höher für NVMe/TCP.

SCSI-über-FC-Tools

SCSI over Fibre Channel (FC) ist ein Tech Preview Feature in der Trident 24.10 Version.

"Installieren Sie die FC Tools" Wenn Sie mit sanType `fcp` (SCSI über FC) verwenden `ontap-san`.

Weitere Informationen finden Sie unter "Möglichkeiten zur Konfiguration von FC- FC-NVMe SAN-Hosts" .

Ermittlung des Node-Service

Trident versucht automatisch zu erkennen, ob auf dem Node iSCSI- oder NFS-Services ausgeführt werden können.

> Die Ermittlung des Node-Service erkennt erkannte Services, gewährleistet jedoch nicht, dass Services ordnungsgemäß konfiguriert wurden. Umgekehrt kann das Fehlen eines entdeckten Service nicht garantieren, dass die Volume-Bereitstellung fehlschlägt.

Überprüfen Sie Ereignisse

Trident erstellt Ereignisse für den Node, um die erkannten Services zu identifizieren. Um diese Ereignisse zu überprüfen, führen Sie folgende Schritte aus:

```
kubectl get event -A --field-selector involvedObject.name=<Kubernetes node name>
```

Überprüfen Sie erkannte Services

Trident erkennt Dienste, die für jeden Knoten auf dem Trident-Knoten CR aktiviert sind. Um die ermittelten Dienste anzuzeigen, führen Sie folgende Schritte aus:

```
tridentctl get node -o wide -n <Trident namespace>
```

NFS Volumes

Installieren Sie die NFS-Tools unter Verwendung der Befehle für Ihr Betriebssystem. Stellen Sie sicher, dass der NFS-Dienst während des Bootens gestartet wird.

RHEL 8 ODER HÖHER

```
sudo yum install -y nfs-utils
```

Ubuntu

```
sudo apt-get install -y nfs-common
```

Starten Sie die Worker-Nodes nach der Installation der NFS-Tools neu, um einen Fehler beim Anschließen von Volumes an Container zu vermeiden.

ISCSI-Volumes

Trident kann automatisch eine iSCSI-Sitzung einrichten, LUNs scannen, Multipath-Geräte erkennen, formatieren und in einen Pod einbinden.

ISCSI-Funktionen zur Selbstreparatur

Bei ONTAP Systemen führt Trident die iSCSI-Selbstreparatur alle fünf Minuten aus, um folgende Vorteile zu nutzen:

1. * Identifizieren Sie den gewünschten iSCSI-Sitzungsstatus und den aktuellen iSCSI-Sitzungsstatus.
2. **Vergleichen** der gewünschte Zustand mit dem aktuellen Zustand, um notwendige Reparaturen zu identifizieren. Trident bestimmt die Reparaturprioritäten und den Zeitpunkt, an dem Reparaturen vorbeugen müssen.
3. **Durchführung von Reparaturen** erforderlich, um den aktuellen iSCSI-Sitzungsstatus auf den gewünschten iSCSI-Sitzungsstatus zurückzusetzen.

Protokolle der Selbstheilungsaktivität befinden sich im `trident-main` Container auf dem jeweiligen Demonset-Pod. Um Protokolle anzuzeigen, müssen Sie während der Trident-Installation auf „true“ gesetzt haben `debug`.

Trident iSCSI-Funktionen zur Selbstheilung verhindern Folgendes:

- Veraltete oder ungesunde iSCSI-Sitzungen, die nach einem Problem mit der Netzwerkverbindung auftreten können Im Falle einer veralteten Sitzung wartet Trident sieben Minuten, bevor er sich abmeldet, um die Verbindung zu einem Portal wiederherzustellen.

> Wenn beispielsweise CHAP-Schlüssel auf dem Speicher-Controller gedreht wurden und die Verbindung zum Netzwerk unterbrochen wird, können die alten (*Inated*) CHAP-Schlüssel bestehen bleiben. Selbstheilung kann dies erkennen und die Sitzung automatisch wiederherstellen, um die aktualisierten CHAP-Schlüssel anzuwenden.

- ISCSI-Sitzungen fehlen
- LUNs sind nicht vorhanden

Punkte, die Sie vor dem Upgrade von Trident beachten sollten

- Wenn nur Initiatorgruppen pro Node (eingeführt in 23.04+) verwendet werden, initiiert iSCSI Self-Healing SCSI-Rescans für alle Geräte im SCSI-Bus.
- Wenn nur Back-End-scoped-Initiatorgruppen (veraltet ab 23.04) verwendet werden, initiiert iSCSI-Selbstreparatur SCSI-Rescans für exakte LUN-IDs im SCSI-Bus.
- Wenn eine Kombination von Initiatorgruppen pro Node und mit Back-End-Scoped-Initiatorgruppen verwendet wird, initiiert iSCSI Self-Healing SCSI-Rescans für exakte LUN-IDs im SCSI-Bus.

Installieren Sie die iSCSI-Tools

Installieren Sie die iSCSI-Tools mit den Befehlen für Ihr Betriebssystem.

Bevor Sie beginnen

- Jeder Node im Kubernetes-Cluster muss über einen eindeutigen IQN verfügen. **Dies ist eine notwendige Voraussetzung**.
- Wenn Sie RHCOS Version 4.5 oder höher oder eine andere RHEL-kompatible Linux-Distribution mit dem Treiber und Element OS 12.5 oder früher verwenden `solidfire-san`, stellen Sie sicher, dass der CHAP-Authentifizierungsalgorithmus auf MD5 in eingestellt ist `/etc/iscsi/iscsid.conf`. Sichere FIPS-konforme CHAP-Algorithmen SHA1, SHA-256 und SHA3-256 sind mit Element 12.7 verfügbar.

```
sudo sed -i 's/^\(node.session.auth.chap_algs\).*/\1 = MD5/'
/etc/iscsi/iscsid.conf
```

- Geben Sie bei der Verwendung von Worker-Nodes, auf denen RHEL/RedHat CoreOS mit iSCSI-PVs ausgeführt wird, die MountOption in der StorageClass an `discard`, um Inline-Speicherplatzrückforderung durchzuführen. Siehe "Red hat-Dokumentation".

RHEL 8 ODER HÖHER

1. Installieren Sie die folgenden Systempakete:

```
sudo yum install -y lsscsi iscsi-initiator-utils device-mapper-
multipath
```

2. Überprüfen Sie, ob die Version von iscsi-Initiator-utils 6.2.0.874-2.el7 oder höher ist:

```
rpm -q iscsi-initiator-utils
```

3. Multipathing aktivieren:

```
sudo mpathconf --enable --with_multipathd y --find_multipaths n
```

> Stellen Sie sicher, dass `etc/multipath.conf` enthält `find_multipaths no` unter `defaults`.

4. Stellen Sie sicher, dass `iscsid` und `multipathd` ausgeführt werden:

```
sudo systemctl enable --now iscsid multipathd
```

5. Aktivieren und starten `iscsi`:

```
sudo systemctl enable --now iscsi
```

Ubuntu

1. Installieren Sie die folgenden Systempakete:

```
sudo apt-get install -y open-iscsi lsscsi sg3-utils multipath-tools
scsitools
```

2. Stellen Sie sicher, dass Open-iscsi-Version 2.0.874-5ubuntu2.10 oder höher (für bionic) oder 2.0.874-7.1ubuntu6.1 oder höher (für Brennweite) ist:

```
dpkg -l open-iscsi
```

3. Scannen auf manuell einstellen:

```
sudo sed -i 's/^\(node.session.scan\).*/\1 = manual/'
/etc/iscsi/iscsid.conf
```

4. Multipathing aktivieren:

```
sudo tee /etc/multipath.conf <<-EOF
defaults {
    user_friendly_names yes
    find_multipaths no
}
EOF
sudo systemctl enable --now multipath-tools.service
sudo service multipath-tools restart
```

> Stellen Sie sicher, dass `etc/multipath.conf` enthält `find_multipaths no` unter `defaults`.

5. Stellen Sie sicher, dass `open-iscsi` und `multipath-tools` aktiviert sind und ausgeführt werden:

```
sudo systemctl status multipath-tools
sudo systemctl enable --now open-iscsi.service
sudo systemctl status open-iscsi
```

> Für Ubuntu 18.04 müssen Sie Zielports mit ermitteln `iscsiadm`, bevor der iSCSI-Daemon gestartet `open-iscsi` wird. Sie können den Dienst auch so ändern `iscsi`, dass er automatisch gestartet `iscsid` wird.

Konfigurieren oder deaktivieren Sie die iSCSI-Selbstheilung

Sie können die folgenden Trident iSCSI-Selbstreparatureinstellungen konfigurieren, um veraltete Sitzungen zu beheben:

- **ISCSI-Selbstheilungsintervall**: Bestimmt die Häufigkeit, mit der iSCSI-Selbstheilung aufgerufen wird (Standard: 5 Minuten). Sie können ihn so konfigurieren, dass er häufiger ausgeführt wird, indem Sie eine kleinere Zahl oder weniger häufig einstellen, indem Sie eine größere Zahl einstellen.

> Wenn Sie das iSCSI-Selbstreparaturintervall auf 0 setzen, wird die iSCSI-Selbstheilung vollständig beendet. Wir empfehlen keine Deaktivierung der iSCSI-Selbstheilung. Sie sollte nur in bestimmten Szenarien deaktiviert werden, wenn die iSCSI-Selbstheilung nicht wie vorgesehen funktioniert oder zu Debugging-Zwecken verwendet wird.

- **ISCSI Self-Healing-Wartezeit**: Bestimmt die Dauer, die iSCSI Self-Healing wartet, bevor Sie sich von einer ungesunden Sitzung abmelden und erneut anmelden (Standard: 7 Minuten). Sie können sie für eine

größere Anzahl konfigurieren, sodass Sitzungen, die als „fehlerhaft“ identifiziert werden, länger warten müssen, bevor sie abgemeldet werden. Anschließend wird versucht, sich erneut anzumelden, oder eine kleinere Zahl, um sich früher abzumelden und anzumelden.

Helm

Um iSCSI-Selbstreparatureinstellungen zu konfigurieren oder zu ändern, übergeben Sie die `iscsiSelfHealingInterval` Parameter und `iscsiSelfHealingWaitTime` während der Helm-Installation oder der Helm-Aktualisierung.

Im folgenden Beispiel wird das iSCSI-Intervall für die Selbstheilung auf 3 Minuten und die Wartezeit für die Selbstheilung auf 6 Minuten eingestellt:

```
helm install trident trident-operator-100.2410.0.tgz --set
iscsiSelfHealingInterval=3m0s --set iscsiSelfHealingWaitTime=6m0s -n
trident
```

Tridentctl

Um iSCSI-Selbstreparatureinstellungen zu konfigurieren oder zu ändern, übergeben Sie die `iscsi-self-healing-interval` Parameter und `iscsi-self-healing-wait-time` während der tridentctl-Installation oder -Aktualisierung.

Im folgenden Beispiel wird das iSCSI-Intervall für die Selbstheilung auf 3 Minuten und die Wartezeit für die Selbstheilung auf 6 Minuten eingestellt:

```
tridentctl install --iscsi-self-healing-interval=3m0s --iscsi-self
-healing-wait-time=6m0s -n trident
```

NVMe/TCP-Volumes

Installieren Sie die NVMe Tools mithilfe der Befehle für Ihr Betriebssystem.

- Für NVMe ist RHEL 9 oder höher erforderlich.
- Wenn die Kernel-Version Ihres Kubernetes Node zu alt ist oder das NVMe-Paket für Ihre Kernel-Version nicht verfügbar ist, müssen Sie möglicherweise die Kernel-Version Ihres Node mit dem NVMe-Paket auf eine aktualisieren.

RHEL 9

```
sudo yum install nvme-cli
sudo yum install linux-modules-extra-$(uname -r)
sudo modprobe nvme-tcp
```

Ubuntu

```
sudo apt install nvme-cli
sudo apt -y install linux-modules-extra-$(uname -r)
sudo modprobe nvme-tcp
```

Überprüfen Sie die Installation

Überprüfen Sie nach der Installation mit dem Befehl, ob für jeden Node im Kubernetes-Cluster ein eindeutiges NQN verwendet wird:

```
cat /etc/nvme/hostnqn
```

Trident ändert den `ctrl_device_tmo` Wert, um zu gewährleisten, dass NVMe bei einem Ausfall nicht auf dem Pfad aufgibt. Ändern Sie diese Einstellung nicht.

Installieren Sie die FC Tools

Installieren Sie die FC-Tools unter Verwendung der Befehle für Ihr Betriebssystem.

- Geben Sie bei der Verwendung von Worker-Nodes, auf denen RHEL/RedHat CoreOS mit FC PVs ausgeführt wird, die MountOption in der StorageClass an `discard`, um Inline-Speicherplatz-Rückgewinnung durchzuführen. Siehe "Red hat-Dokumentation".

RHEL 8 ODER HÖHER

1. Installieren Sie die folgenden Systempakete:

```
sudo yum install -y lsscsi device-mapper-multipath
```

2. Multipathing aktivieren:

```
sudo mpathconf --enable --with_multipathd y --find_multipaths n
```

> Stellen Sie sicher, dass `etc/multipath.conf` enthält `find_multipaths no` unter `defaults`.

3. Stellen Sie sicher, dass `multipathd` Folgendes ausgeführt wird:

```
sudo systemctl enable --now multipathd
```

Ubuntu

1. Installieren Sie die folgenden Systempakete:

```
sudo apt-get install -y lsscsi sg3-utils multipath-tools scsitools
```

2. Multipathing aktivieren:

```
sudo tee /etc/multipath.conf <<-EOF
defaults {
    user_friendly_names yes
    find_multipaths no
}
EOF
sudo systemctl enable --now multipath-tools.service
sudo service multipath-tools restart
```

> Stellen Sie sicher, dass `etc/multipath.conf` enthält `find_multipaths no` unter `defaults`.

3. Stellen Sie sicher, dass `multipath-tools` aktiviert und ausgeführt wird:

```
sudo systemctl status multipath-tools
```

Unterstützung für Fibre Channel (FC)

Jetzt kann das Fibre Channel-Protokoll (FC) mit Trident verwendet werden, um Storage-Ressourcen auf ONTAP Systemen bereitzustellen und zu managen.

SCSI over Fibre Channel (FC) ist ein Tech Preview Feature in der Trident 24.10 Version.

Fibre Channel ist aufgrund seiner hohen Performance, Zuverlässigkeit und Skalierbarkeit ein weit verbreitetes Protokoll in Enterprise-Storage-Umgebungen. Er bietet einen robusten und effizienten Kommunikationskanal für Speichergeräte, der schnelle und sichere Datenübertragungen ermöglicht. Durch die Verwendung von SCSI über Fibre Channel können Sie ihre vorhandene SCSI-basierte Speicherinfrastruktur nutzen und gleichzeitig von den High-Performance- und Fernfunktionen von Fibre Channel profitieren. Sie unterstützt die Konsolidierung von Speicherressourcen und die Erstellung skalierbarer und effizienter Storage Area Networks (SANs), die große Datenmengen mit geringer Latenz verarbeiten können.

Mithilfe der FC-Funktion mit Trident können Sie folgende Aufgaben ausführen:

- Dynamische Bereitstellung von VES mithilfe einer Implementierungsspezifikation
- Erstellen Sie Volume-Snapshots und ein neues Volume aus dem Snapshot.
- Klonen einer vorhandenen FC-PVC.
- Die Größe eines bereits bereitgestellten Volumes ändern.

Voraussetzungen

Konfigurieren Sie die erforderlichen Netzwerk- und Node-Einstellungen für FC.

Netzwerkeinstellungen

1. Erhalten Sie den WWPN der Zielschnittstellen. Weitere Informationen finden Sie unter "Netzwerkschnittstelle wird angezeigt" .
2. Abrufen der WWPN für die Schnittstellen auf Initiator (Host).

   Weitere Informationen finden Sie in den entsprechenden Dienstprogrammen des Host-Betriebssystems.
3. Konfigurieren Sie das Zoning auf dem FC-Switch mithilfe von WWPNs des Hosts und Ziels.

   Weitere Informationen finden Sie in der Dokumentation des jeweiligen Switch-Anbieters.

   Details finden Sie in der folgenden ONTAP Dokumentation:

   - "Übersicht über Fibre Channel und FCoE Zoning"
   - "Möglichkeiten zur Konfiguration von FC- FC-NVMe SAN-Hosts"

Bereiten Sie den Knoten „Worker“ vor

Alle Worker-Nodes im Kubernetes-Cluster müssen in der Lage sein, die Volumes, die Sie für Ihre Pods bereitgestellt haben, zu mounten. Um die Worker-Nodes für FC vorzubereiten, müssen Sie die erforderlichen Tools installieren.

Installieren Sie die FC Tools

Installieren Sie die FC-Tools unter Verwendung der Befehle für Ihr Betriebssystem.

- Geben Sie bei der Verwendung von Worker-Nodes, auf denen RHEL/RedHat CoreOS mit FC PVs ausgeführt wird, die MountOption in der StorageClass an `discard`, um Inline-Speicherplatz-Rückgewinnung durchzuführen. Siehe "Red hat-Dokumentation".

RHEL 8 ODER HÖHER

1. Installieren Sie die folgenden Systempakete:

```
sudo yum install -y lsscsi device-mapper-multipath
```

2. Multipathing aktivieren:

```
sudo mpathconf --enable --with_multipathd y --find_multipaths n
```

> Stellen Sie sicher, dass `etc/multipath.conf` enthält `find_multipaths no` unter `defaults`.

3. Stellen Sie sicher, dass `multipathd` Folgendes ausgeführt wird:

```
sudo systemctl enable --now multipathd
```

Ubuntu

1. Installieren Sie die folgenden Systempakete:

```
sudo apt-get install -y lsscsi sg3-utils multipath-tools scsitools
```

2. Multipathing aktivieren:

```
sudo tee /etc/multipath.conf <<-EOF
defaults {
    user_friendly_names yes
    find_multipaths no
}
EOF
sudo systemctl enable --now multipath-tools.service
sudo service multipath-tools restart
```

> Stellen Sie sicher, dass `etc/multipath.conf` enthält `find_multipaths no` unter `defaults`.

3. Stellen Sie sicher, dass `multipath-tools` aktiviert und ausgeführt wird:

```
sudo systemctl status multipath-tools
```

Erstellen Sie eine Backend-Konfiguration

Erstellen Sie ein Trident-Backend für den `ontap-san` Treiber und `fcp` als sanType.

Siehe:

- "Vorbereiten der Back-End-Konfiguration mit ONTAP-SAN-Treibern"
- "ONTAP-SAN-Konfigurationsoptionen und Beispiele"

Beispiel für eine Back-End-Konfiguration mit FC

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-san
spec:
  version: 1
  backendName: ontap-san-backend
  storageDriverName: ontap-san
  managementLIF: 10.0.0.1
  sanType: fcp
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-san-secret
```

Erstellen Sie eine Speicherklasse

Weitere Informationen finden Sie unter:

- "Optionen für die Storage-Konfiguration"

Beispiel für Storage-Klasse

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: fcp-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
  storagePools: "ontap-san-backend:.*"
  fsType: "ext4"
allowVolumeExpansion: True
```