



# **Best Practices und Empfehlungen**

Trident

NetApp

January 14, 2026

# Inhalt

|  |    |
|--|----|
| Best Practices und Empfehlungen .....  | 1  |
| Einsatz .....  | 1  |
| Implementieren Sie diesen in einem dedizierten Namespace .....                                 | 1  |
| Verwenden Sie Kontingente und Bereichsgrenzen, um den Storage-Verbrauch zu kontrollieren ..... | 1  |
| Storage-Konfiguration .....  | 1  |
| Plattformübersicht .....   | 1  |
| Best Practices für ONTAP und Cloud Volumes ONTAP .....   | 2  |
| SolidFire Best Practices in sich vereint .....   | 6  |
| Wo finden Sie weitere Informationen? .....   | 8  |
| Integration von Trident .....  | 8  |
| Auswahl und Implementierung der Treiber .....  | 8  |
| Design der Storage-Klasse .....  | 12 |
| Virtual Pool Design .....  | 13 |
| Volume-Vorgänge .....  | 14 |
| Kennzahlungsservice .....  | 18 |
| Datensicherung und Disaster Recovery .....   | 19 |
| Replizierung und Recovery mit Trident .....  | 19 |
| SVM-Replizierung und Recovery .....  | 20 |
| Volume-Replizierung und Recovery .....   | 21 |
| Snapshot Datensicherung .....  | 21 |
| Sicherheit .....   | 21 |
| Sicherheit .....   | 21 |
| Linux Unified Key Setup (LUKS) .....   | 23 |
| Kerberos Verschlüsselung während der Übertragung .....   | 29 |

# Best Practices und Empfehlungen

## Einsatz

Verwenden Sie bei der Implementierung von Trident die hier aufgeführten Empfehlungen.

### Implementieren Sie diesen in einem dedizierten Namespace

"Namespaces" Trennung von Administratoren zwischen verschiedenen Applikationen und Barriere für die gemeinsame Nutzung von Ressourcen. Beispielsweise kann eine PVC aus einem Namespace nicht von einem anderen genutzt werden. Trident stellt allen Namespaces im Kubernetes-Cluster PV-Ressourcen zur Verfügung und nutzt folglich ein Servicekonto mit erhöhten Privilegen.

Außerdem kann der Zugriff auf den Trident Pod dazu führen, dass Benutzer auf die Anmeldedaten des Storage-Systems und andere sensible Informationen zugreifen können. Es ist wichtig, dass Applikationsbenutzer und Management-Applikationen nicht in der Lage sind, auf die Trident Objektdefinitionen oder Pods selbst zuzugreifen.

### Verwenden Sie Kontingente und Bereichsgrenzen, um den Storage-Verbrauch zu kontrollieren

Kubernetes bietet zusammen zwei Funktionen, die einen leistungsstarken Mechanismus zur Begrenzung des Ressourcenverbrauchs durch Applikationen bieten. "[Mechanismus für Storage-Kontingente](#)" Administratoren können globale Verbrauchsbeschränkungen für Storage-Klassen, Kapazitäten und die Anzahl der Objekte pro Namespace implementieren. Außerdem stellt die Verwendung eines "[Bereichsgrenze](#)" sicher, dass die PVC-Anforderungen innerhalb eines minimalen und eines maximalen Werts liegen, bevor die Anforderung an die Provisionierung weitergeleitet wird.

Diese Werte werden pro Namespace definiert, was bedeutet, dass jeder Namespace Werte definiert haben sollte, die ihren Ressourcenanforderungen entsprechen. Siehe hier für Informationen über "[Wie man Quoten nutzt](#)".

## Storage-Konfiguration

Jede Storage-Plattform im NetApp Portfolio verfügt über einzigartige Funktionen für Applikationen, die in Containern oder nicht unterstützt werden.

### Plattformübersicht

Trident funktioniert mit ONTAP und Element. Es gibt keine Plattform, die besser für alle Anwendungen und Szenarien geeignet ist als die andere, aber bei der Auswahl einer Plattform sollten die Anforderungen der Anwendung und des Teams, das das Gerät verwaltet, berücksichtigt werden.

Sie sollten die Best Practices für das Host-Betriebssystem anhand des von Ihnen verwendeten Protokolls befolgen. Optional können Sie möglicherweise erwägen, falls verfügbar Best Practices für Applikationen mit Back-End-, Storage-Klassen- und PVC-Einstellungen zu integrieren, um den Storage für bestimmte Applikationen zu optimieren.

## Best Practices für ONTAP und Cloud Volumes ONTAP

Best Practices zur Konfiguration von ONTAP und Cloud Volumes ONTAP für Trident enthalten.

Die folgenden Empfehlungen sind Richtlinien zur Konfiguration von ONTAP für Container-Workloads, die Volumes nutzen, die von Trident dynamisch bereitgestellt werden. Jeder sollte in Betracht gezogen und auf Angemessenheit in Ihrer Umgebung überprüft werden.

### Verwenden Sie SVM(s) dediziert für Trident

Storage Virtual Machines (SVMs) sorgen für die Trennung von Mandanten auf einem ONTAP System. Durch die Zuweisung einer SVM für Applikationen können Berechtigungen delegation werden. Zudem lassen sich Best Practices anwenden, um den Ressourcenverbrauch zu begrenzen.

Für das Management der SVM sind verschiedene Optionen verfügbar:

- Stellen Sie die Cluster-Managementoberfläche in der Backend-Konfiguration zusammen mit entsprechenden Zugangsdaten bereit und geben Sie den SVM-Namen an.
- Erstellen Sie mit ONTAP System Manager oder der CLI eine dedizierte Managementoberfläche für die SVM.
- Teilen Sie die Managementrolle mit einer NFS-Datenschnittstelle.

In jedem Fall sollte sich die Schnittstelle im DNS enthalten, und beim Konfigurieren von Trident sollte der DNS-Name verwendet werden. Dadurch lassen sich einige DR-Szenarien, beispielsweise SVM-DR, vereinfachen, ohne die Aufbewahrung der Netzwerkidentität zu nutzen.

Es besteht keine Präferenz zwischen einer dedizierten oder gemeinsam genutzten Management-LIF für die SVM. Sie sollten jedoch sicherstellen, dass Ihre Netzwerksicherheitsrichtlinien mit dem von Ihnen gewählten Ansatz abgestimmt sind. Trotzdem sollte die Management-LIF über DNS zugänglich sein, um maximale Flexibilität zu ermöglichen, sollte ["SVM-DR"](#) in Verbindung mit Trident verwendet werden.

### Begrenzung der maximalen Volume-Anzahl

ONTAP Storage-Systeme besitzen eine maximale Anzahl an Volumes, die je nach Softwareversion und Hardwareplattform unterschiedlich sind. Informationen zu Ihren spezifischen Plattform- und ONTAP-Versionen finden Sie unter ["NetApp Hardware Universe"](#). Wenn die Anzahl der Volumes erschöpft ist, schlägt die Bereitstellung nicht nur für Trident fehl, sondern für alle Storage-Anforderungen.

Trident ontap-nas und ontap-san Treiber stellen für jedes erstellte Kubernetes Persistent Volume (PV) ein FlexVolume bereit. Der ontap-nas-economy Treiber erstellt ca. ein FlexVolume für je 200 PVs (konfigurierbar zwischen 50 und 300). Der ontap-san-economy Treiber erstellt ca. ein FlexVolume für je 100 PVs (konfigurierbar zwischen 50 und 200). Damit Trident nicht alle verfügbaren Volumes im Storage-System verbraucht, sollten Sie ein Limit für die SVM festlegen. Dies können Sie über die Befehlszeile ausführen:

```
vserver modify -vserver <svm_name> -max-volumes <num_of_volumes>
```

Der Wert für `max-volumes` variiert basierend auf verschiedenen Kriterien für Ihre spezifische Umgebung:

- Die Anzahl der vorhandenen Volumes im ONTAP Cluster
- Die Anzahl der Volumes, die für andere Applikationen außerhalb von Trident bereitgestellt werden
- Die Anzahl der persistenten Volumes, die von Kubernetes-Applikationen genutzt werden sollen

Der `max-volumes` Wert ist die Gesamtzahl der Volumes, die über alle Nodes im ONTAP Cluster bereitgestellt werden, nicht aber über einen einzelnen ONTAP Node. Aus diesem Grund treten möglicherweise einige Bedingungen auf, bei denen auf einem ONTAP Cluster-Node mehr oder weniger mit Trident bereitgestellte Volumes als ein anderer Node vorhanden sind.

Beispielsweise kann ein ONTAP Cluster mit zwei Nodes maximal 2000 FlexVol Volumes hosten. Eine auf 1250 eingestellte maximale Volumenzahl erscheint sehr vernünftig. Wenn jedoch nur ["Aggregate"](#) von einem Node der SVM zugewiesen wird oder die von einem Node zugewiesenen Aggregate nicht bereitgestellt werden können (z. B. aufgrund der Kapazität), dann wird der andere Node das Ziel aller über Trident bereitgestellten Volumes. Das bedeutet, dass das Volume-Limit für diesen Node vor dem Erreichen des Wertes erreicht werden kann `max-volumes`, was sich sowohl auf Trident als auch auf andere Volume-Operationen, die den Node verwenden, auswirkt. **Diese Situation kann vermieden werden, indem sichergestellt wird, dass die Aggregate von jedem Node im Cluster der von Trident verwendeten SVM in gleicher Anzahl zugewiesen werden.**

### **Begrenzung der maximalen Größe der durch Trident erstellten Volumes**

Verwenden Sie den Parameter in Ihrer `backend.json` Definition, um die maximale Größe für Volumes zu konfigurieren, die von Trident erstellt werden `limitVolumeSize` können.

Neben der Kontrolle der Volume-Größe im Storage-Array sollten auch Kubernetes-Funktionen genutzt werden.

### **Beschränkt die maximale Größe von FlexVols, die von Trident erstellt werden**

Um die maximale Größe für FlexVols zu konfigurieren, die als Pools für ONTAP-san-Economy- und ONTAP-nas-Economy-Treiber verwendet werden, verwenden Sie den `limitVolumePoolSize` Parameter in Ihrer `backend.json` Definition.

### **Trident für bidirektionales CHAP konfigurieren**

Sie können in der Back-End-Definition den CHAP-Initiator und die Benutzernamen und Passwörter für das Ziel angeben und Trident CHAP auf der SVM aktivieren. Mithilfe des `useCHAP` Parameters in Ihrer Backend-Konfiguration authentifiziert Trident iSCSI-Verbindungen für ONTAP-Back-Ends mit CHAP.

### **Erstellen und Verwenden einer SVM QoS-Richtlinie**

Die Nutzung einer ONTAP QoS-Richtlinie auf die SVM begrenzt die Anzahl der durch die von Trident bereitgestellten Volumes konsumierbaren IOPS. Dies hilft bei der ["Verhindern Sie einen Schläger"](#) Überwachung oder außer Kontrolle geraten durch Container, die Workloads außerhalb der Trident SVM beeinträchtigen.

Sie können in wenigen Schritten eine QoS-Richtlinie für die SVM erstellen. Die genauesten Informationen finden Sie in der Dokumentation Ihrer ONTAP-Version. Das folgende Beispiel erstellt eine QoS-Richtlinie, die die insgesamt für eine SVM verfügbaren IOPS auf 5000 begrenzt.

```

# create the policy group for the SVM
qos policy-group create -policy-group <policy_name> -vserver <svm_name>
-max-throughput 5000iops

# assign the policy group to the SVM, note this will not work
# if volumes or files in the SVM have existing QoS policies
vserver modify -vserver <svm_name> -qos-policy-group <policy_name>

```

Wenn zudem Ihre ONTAP Version sie unterstützt, können Sie den Einsatz eines minimalen QoS-Systems in Erwägung ziehen, um einen hohen Durchsatz für Container-Workloads zu gewährleisten. Die adaptive QoS ist nicht mit einer Richtlinie auf SVM-Ebene kompatibel.

Die Anzahl der für Container-Workloads dedizierten IOPS hängt von vielen Aspekten ab. Dazu zählen unter anderem:

- Anderen Workloads, die das Storage-Array nutzen Bei anderen Workloads, die nicht mit der Kubernetes-Implementierung zusammenhängen und die Storage-Ressourcen nutzen, sollte darauf achten, dass diese Workloads nicht versehentlich beeinträchtigt werden.
- Erwartete Workloads werden in Containern ausgeführt. Wenn Workloads mit hohen IOPS-Anforderungen in Containern ausgeführt werden, führt eine niedrige QoS-Richtlinie zu schlechten Erfahrungen.

Es muss daran erinnert werden, dass eine auf SVM-Ebene zugewiesene QoS-Richtlinie alle Volumes zur Verfügung hat, die der SVM bereitgestellt werden und sich denselben IOPS-Pool teilen. Wenn eine oder nur eine kleine Zahl von Container-Applikationen sehr hohe IOPS-Anforderungen erfüllen, kann dies zu einem problematischer für die anderen Container-Workloads werden. In diesem Fall empfiehlt es sich, QoS-Richtlinien pro Volume mithilfe von externer Automatisierung zuzuweisen.



Sie sollten die QoS Policy Group der SVM **only** zuweisen, wenn Ihre ONTAP Version älter als 9.8 ist.

## Erstellen von QoS-Richtliniengruppen für Trident

Quality of Service (QoS) garantiert, dass die Performance kritischer Workloads nicht durch konkurrierende Workloads beeinträchtigt wird. ONTAP QoS-Richtliniengruppen bieten QoS-Optionen für Volumes und ermöglichen Benutzern, die Durchsatzgrenze für einen oder mehrere Workloads zu definieren. Weitere Informationen zur QoS finden Sie unter "[Garantierter Durchsatz durch QoS](#)". Sie können QoS-Richtliniengruppen im Backend oder im Storage-Pool festlegen und werden auf jedes in diesem Pool oder Backend erstellte Volume angewendet.

ONTAP verfügt über zwei Arten von QoS-Richtliniengruppen: Herkömmliche und anpassungsfähige. Herkömmliche Richtliniengruppen bieten einen flachen maximalen Durchsatz (oder minimalen Durchsatz in späteren Versionen) in IOPS. Adaptive QoS skaliert den Durchsatz automatisch auf die Workload-Größe und erhält das Verhältnis von IOPS zu TB-fähigen GB-Werten, wenn sich die Workload-Größe ändert. Wenn Sie Hunderte oder Tausende Workloads in einer großen Implementierung managen, bietet sich somit ein erheblicher Vorteil.

Beachten Sie beim Erstellen von QoS-Richtliniengruppen Folgendes:

- Sie sollten den Schlüssel im defaults Block der Backend-Konfiguration setzen qosPolicy. Im folgenden Back-End-Konfigurationsbeispiel:

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 0.0.0.0
dataLIF: 0.0.0.0
svm: svm0
username: user
password: pass
defaults:
  qosPolicy: standard-pg
storage:
  - labels:
      performance: extreme
    defaults:
      adaptiveQosPolicy: extremely-adaptive-pg
  - labels:
      performance: premium
    defaults:
      qosPolicy: premium-pg
```

- Sie sollten die Richtliniengruppen pro Volume anwenden, damit jedes Volume den gesamten von der Richtliniengruppe angegebenen Durchsatz erhält. Gemeinsame Richtliniengruppen werden nicht unterstützt.

Weitere Informationen zu QoS-Richtliniengruppen finden Sie unter "[ONTAP-Befehlsreferenz](#)".

### Beschränken Sie den Zugriff auf die Storage-Ressourcen auf Kubernetes-Cluster-Mitglieder

Die Beschränkung des Zugriffs auf die von Trident erstellten NFS-Volumes, iSCSI-LUNs und FC-LUNs ist eine wichtige Komponente für die Sicherheit Ihrer Kubernetes-Implementierung. Auf diese Weise wird verhindert, dass Hosts, die nicht zum Kubernetes Cluster gehören, auf die Volumes zugreifen und Daten unerwartet ändern können.

Es ist wichtig zu wissen, dass Namespaces die logische Grenze für Ressourcen in Kubernetes sind. Es wird angenommen, dass Ressourcen im selben Namespace gemeinsam genutzt werden können. Es gibt jedoch keine Cross-Namespace-Funktion. Dies bedeutet, dass PVCs zwar globale Objekte sind, aber wenn sie an ein PVC gebunden sind, nur über Pods zugänglich sind, die sich im selben Namespace befinden. **Es ist wichtig sicherzustellen, dass Namensräume verwendet werden, um eine Trennung zu gewährleisten, wenn angemessen.**

Die meisten Unternehmen haben im Zusammenhang mit der Datensicherheit bei Kubernetes die Sorge, dass ein Container-Prozess auf den Storage zugreifen kann, der am Host gemountet ist; dieser ist jedoch nicht für den Container bestimmt. **"Namespaces"** Sind so konzipiert, dass diese Art von Kompromiss verhindert wird. Allerdings gibt es eine Ausnahme: Privilegierte Container.

Ein privilegierter Container ist ein Container, der mit wesentlich mehr Berechtigungen auf Hostebene als normal ausgeführt wird. Diese werden standardmäßig nicht verweigert. Stellen Sie daher sicher, dass Sie die Funktion mithilfe von deaktivieren **"Pod-Sicherheitsrichtlinien"**.

Bei Volumes, für die der Zugriff von Kubernetes und externen Hosts gewünscht wird, sollte der Storage auf

herkömmliche Weise gemanagt werden. Dabei wird das PV durch den Administrator eingeführt und nicht von Trident gemanagt. So wird sichergestellt, dass das Storage Volume nur zerstört wird, wenn sowohl Kubernetes als auch externe Hosts getrennt haben und das Volume nicht mehr nutzen. Zusätzlich kann eine benutzerdefinierte Exportrichtlinie angewendet werden, die den Zugriff von den Kubernetes-Cluster-Nodes und Zielservern außerhalb des Kubernetes-Clusters ermöglicht.

Für Bereitstellungen mit dedizierten Infrastruktur-Nodes (z. B. OpenShift) oder anderen Nodes, die Benutzerapplikationen nicht planen können, sollten separate Exportrichtlinien verwendet werden, um den Zugriff auf Speicherressourcen weiter zu beschränken. Dies umfasst die Erstellung einer Exportrichtlinie für Services, die auf diesen Infrastruktur-Nodes bereitgestellt werden (z. B. OpenShift Metrics and Logging Services), sowie Standardanwendungen, die auf nicht-Infrastruktur-Nodes bereitgestellt werden.

### **Verwenden Sie eine dedizierte Exportrichtlinie**

Sie sollten sicherstellen, dass für jedes Backend eine Exportrichtlinie vorhanden ist, die nur den Zugriff auf die im Kubernetes-Cluster vorhandenen Nodes erlaubt. Trident kann Richtlinien für den Export automatisch erstellen und managen. So beschränkt Trident den Zugriff auf die Volumes, die ihm im Kubernetes Cluster zur Verfügung stehen, und vereinfacht das Hinzufügen/Löschen von Nodes.

Alternativ können Sie auch eine Exportrichtlinie manuell erstellen und mit einer oder mehreren Exportregeln füllen, die die Zugriffsanforderung für die einzelnen Knoten bearbeiten:

- Erstellen Sie die Exportrichtlinie mit `vserver export-policy create` dem ONTAP-CLI-Befehl.
- Fügen Sie der Exportrichtlinie Regeln mithilfe des ONTAP CLI-Befehls hinzu `vserver export-policy rule create`.

Wenn Sie diese Befehle ausführen, können Sie die Zugriffsrechte der Kubernetes-Nodes auf die Daten beschränken.

### **Deaktivieren showmount für die Anwendungs-SVM**

Die showmount Funktion ermöglicht es einem NFS-Client, die SVM nach einer Liste der verfügbaren NFS-Exporte abzufragen. Ein im Kubernetes-Cluster implementierter Pod kann den Befehl für den ausgeben `showmount -e` und eine Liste der verfügbaren Mounts erhalten, einschließlich derjenigen, auf die er keinen Zugriff hat. Obwohl dies für sich kein Sicherheitskompromiss ist, stellt es keine unnötigen Informationen bereit, die einem nicht autorisierten Benutzer die Verbindung zu einem NFS-Export ermöglichen.

Sie sollten die Deaktivierung `showmount` mit dem ONTAP CLI-Befehl auf SVM-Ebene verwenden:

```
vserver nfs modify -vserver <svm_name> -showmount disabled
```

## **SolidFire Best Practices in sich vereint**

Lesen Sie Best Practices zur Konfiguration von SolidFire Storage für Trident.

### **Erstellen Eines SolidFire-Kontos**

Jedes SolidFire-Konto stellt einen eindeutigen Volume-Eigentümer dar und erhält seine eigenen Anmeldeinformationen für das Challenge-Handshake Authentication Protocol (CHAP). Sie können auf Volumes zugreifen, die einem Konto zugewiesen sind, entweder über den Kontonamen und die relativen CHAP-Anmeldeinformationen oder über eine Zugriffsgruppe für Volumes. Einem Konto können bis zu zweitausend Volumes zugewiesen sein, ein Volume kann jedoch nur zu einem Konto gehören.

## Erstellen einer QoS-Richtlinie

Verwenden Sie QoS-Richtlinien (Quality of Service) von SolidFire, um eine standardisierte Quality of Service-Einstellung zu erstellen und zu speichern, die auf viele Volumes angewendet werden kann.

Sie können QoS-Parameter für einzelne Volumes festlegen. Die Performance für jedes Volume kann durch drei konfigurierbare Parameter bestimmt werden, die QoS definieren: Das IOPS-Minimum, das IOPS-Maximum und die Burst-IOPS.

Hier sind die möglichen Minimum-, Maximum- und Burst-IOPS für die 4-KB-Blockgröße.

| IOPS-Parameter | Definition   | Min. Wert | Standardwert | Max. Wert (4 KB) |
|----------------|--|-----------|--------------|------------------|
| IOPS-Minimum   | Das garantierte Performance-Level für ein Volume       | 50        | 50           | 15000            |
| IOPS-Maximum   | Die Leistung überschreitet dieses Limit nicht.         | 50        | 15000        | 200.000          |
| IOPS-Burst     | Maximale IOPS in einem kurzen Burst-Szenario zulässig. | 50        | 15000        | 200.000          |



Obwohl die IOPS-Maximum und die Burst-IOPS so hoch wie 200.000 sind, wird die tatsächliche maximale Performance eines Volumes durch die Nutzung von Clustern und die Performance pro Node begrenzt.

Die Blockgröße und die Bandbreite haben einen direkten Einfluss auf die Anzahl der IOPS. Mit zunehmender Blockgröße erhöht das System die Bandbreite auf ein Niveau, das für die Verarbeitung größerer Blockgrößen erforderlich ist. Mit der steigenden Bandbreite sinkt auch die Anzahl an IOPS, die das System erreichen kann. Weitere Informationen zur QoS und Performance finden Sie unter ["SolidFire Quality of Service"](#).

## SolidFire Authentifizierung

Element unterstützt zwei Authentifizierungsmethoden: CHAP und Volume Access Groups (VAG). CHAP verwendet das CHAP-Protokoll, um den Host am Backend zu authentifizieren. Volume Access Groups steuern den Zugriff auf die Volumes, die durch sie bereitgestellt werden. Da die Authentifizierung einfacher ist und über keine Grenzen für die Skalierung verfügt, empfiehlt NetApp die Verwendung von CHAP.



Trident mit dem erweiterten CSI-provisioner unterstützt die Verwendung von CHAP-Authentifizierung. Vags sollten nur im traditionellen nicht-CSI-Betriebsmodus verwendet werden.

CHAP-Authentifizierung (Verifizierung, dass der Initiator der vorgesehene Volume-Benutzer ist) wird nur mit der Account-basierten Zugriffssteuerung unterstützt. Wenn Sie CHAP zur Authentifizierung verwenden, stehen zwei Optionen zur Verfügung: Unidirektionales CHAP und bidirektionales CHAP. Unidirektionales CHAP authentifiziert den Volume-Zugriff mithilfe des SolidFire-Kontonamens und des Initiatorgeheimnisses. Die bidirektionale CHAP-Option bietet die sicherste Möglichkeit zur Authentifizierung des Volumes, da das Volume den Host über den Kontonamen und den Initiatorschlüssel authentifiziert und dann der Host das Volume über den Kontonamen und den Zielschlüssel authentifiziert.

Wenn CHAP jedoch nicht aktiviert werden kann und Vags erforderlich sind, erstellen Sie die Zugriffsgruppe und fügen Sie die Hostinitiatoren und Volumes der Zugriffsgruppe hinzu. Jeder IQN, den Sie einer Zugriffsgruppe hinzufügen, kann mit oder ohne CHAP-Authentifizierung auf jedes Volume in der Gruppe zugreifen. Wenn der iSCSI-Initiator für die Verwendung der CHAP-Authentifizierung konfiguriert ist, wird die kontenbasierte Zugriffssteuerung verwendet. Wenn der iSCSI-Initiator nicht für die Verwendung der CHAP-Authentifizierung konfiguriert ist, wird die Zugriffskontrolle für die Volume Access Group verwendet.

## Wo finden Sie weitere Informationen?

Einige der Best Practices-Dokumentationen sind unten aufgeführt. Suchen Sie im "[NetApp Bibliothek](#)" nach den aktuellsten Versionen.

### ONTAP

- "[NFS Best Practice- und Implementierungsleitfaden](#)"
- "[SAN-Administration](#)" (Für iSCSI)
- "[iSCSI Express-Konfiguration für RHEL](#)"

### Element Software

- "[Konfigurieren von SolidFire für Linux](#)"

### NetApp HCI

- "[Voraussetzungen für die NetApp HCI-Implementierung](#)"
- "[Rufen Sie die NetApp Deployment Engine auf](#)"

### Anwendung Best Practices Informationen

- "[Best Practices für MySQL auf ONTAP](#)"
- "[Best Practices für MySQL auf SolidFire](#)"
- "[NetApp SolidFire und Cassandra](#)"
- "[Best Practices für Oracle auf SolidFire](#)"
- "[Best Practices für PostgreSQL auf SolidFire](#)"

Da nicht alle Applikationen spezifische Richtlinien haben, ist es wichtig, mit Ihrem NetApp Team zusammenzuarbeiten und die aktuellste Dokumentation zu finden. "[NetApp Bibliothek](#)"

## Integration von Trident

Zur Integration von Trident müssen folgende Design- und Architekturelemente integriert werden: Treiberauswahl und -Implementierung, Storage-Klassendesign, Virtual Pool Design, Persistent Volume Claim (PVC) Auswirkungen auf die Storage-Provisionierung, Volume-Betrieb und OpenShift-Services mithilfe von Trident.

## Auswahl und Implementierung der Treiber

Wählen Sie einen Back-End-Treiber für Ihr Speichersystem aus und implementieren Sie ihn.

## Back-End-Treiber für ONTAP

Die Back-End-Treiber für ONTAP unterscheiden sich durch das verwendete Protokoll und die Art und Weise, wie die Volumes im Storage-System bereitgestellt werden. Daher sollten Sie bei der Entscheidung, welchen Treiber eingesetzt werden soll, sorgfältig überlegen.

Auf einer höheren Ebene, wenn Ihre Applikation Komponenten hat, die gemeinsamen Storage benötigen (mehrere Pods, die auf dasselbe PVC zugreifen), sind NAS-basierte Treiber die erste Wahl, während die blockbasierten iSCSI-Treiber die Anforderungen von nicht gemeinsam genutztem Storage erfüllen. Wählen Sie das Protokoll basierend auf den Anforderungen der Applikation und der Komfort-Ebene der Storage- und Infrastrukturteams. Generell besteht für die meisten Applikationen kein Unterschied zwischen ihnen. Oftmals basiert die Entscheidung darauf, ob gemeinsam genutzter Storage (wo mehr als ein POD den gleichzeitigen Zugriff benötigt) benötigt wird.

Die verfügbaren Back-End-Treiber für ONTAP sind:

- `ontap-nas`: Jedes bereitgestellte PV ist ein vollständiges ONTAP FlexVolume.
- `ontap-nas-economy`: Jedes bereitgestellte PV ist ein qtree, mit einer konfigurierbaren Anzahl von qtrees pro FlexVolume (Standard ist 200).
- `ontap-nas-flexgroup`: Jedes PV, das als vollständiges ONTAP FlexGroup bereitgestellt wird, und alle Aggregate, die einer SVM zugewiesen sind, werden verwendet.
- `ontap-san`: Jedes bereitgestellte PV ist eine LUN innerhalb seines eigenen FlexVolume.
- `ontap-san-economy`: Jedes bereitgestellte PV ist eine LUN, mit einer konfigurierbaren Anzahl von LUNs pro FlexVolume (Standard ist 100).

Die Auswahl zwischen den drei NAS-Treibern hat einige Auswirkungen auf die Funktionen, die der Applikation zur Verfügung gestellt werden.

Beachten Sie, dass in den folgenden Tabellen nicht alle Funktionen über Trident bereitgestellt werden. Einige müssen vom Storage-Administrator nach der Bereitstellung angewendet werden, wenn diese Funktion gewünscht wird. Die Super-Skript-Fußnoten unterscheiden die Funktionalität pro Feature und Treiber.

| ONTAP NAS-Treiber                | Snapshot s     | Klone  | Dynamische Exportrichtlinien | Multi-Anschlüsse | QoS            | Größe Ändern | Replizierung   |
|----------------------------------|----------------|--------|------------------------------|------------------|----------------|--------------|----------------|
| <code>ontap-nas</code>           | Ja.            | Ja.    | Jafußnote: 5[]               | Ja.              | Jafußnote: 1[] | Ja.          | Jafußnote: 1[] |
| <code>ontap-nas-economy</code>   | NO [3]         | NO [3] | Jafußnote: 5[]               | Ja.              | NO [3]         | Ja.          | NO [3]         |
| <code>ontap-nas-flexgroup</code> | Jafußnote: 1[] | NEIN   | Jafußnote: 5[]               | Ja.              | Jafußnote: 1[] | Ja.          | Jafußnote: 1[] |

Trident bietet 2 SAN-Treiber für ONTAP an, deren Funktionen unten dargestellt sind.

| ONTAP SAN-Treiber | Snapshot s | Klone | Multi-Anschlus s | Bidirektio nales CHAP | QoS            | Größe Ändern | Replizieru ng  |
|-------------------|------------|-------|------------------|-----------------------|----------------|--------------|----------------|
| ontap-san         | Ja.        | Ja.   | Jafußnote: 4[]   | Ja.                   | Jafußnote: 1[] | Ja.          | Jafußnote: 1[] |
| ontap-san-economy | Ja.        | Ja.   | Jafußnote: 4[]   | Ja.                   | NO [3]         | Ja.          | NO [3]         |

Fußnote für die obigen Tabellen: Yes [1]: Nicht von Trident verwaltet Yes [2]: Verwaltet von Trident, aber nicht von PV granular NO [3]: Nicht von Trident verwaltet und nicht von PV granular Yes [4]: Unterstützt für RAW-Block-Volumes Yes [5]: Unterstützt von Trident

Die Funktionen, die keine PV-Granularität sind, werden auf das gesamte FlexVolume angewendet, und alle PVs (also qtrees oder LUNs in gemeinsam genutzten FlexVols) teilen einen gemeinsamen Zeitplan.

Wie wir in den obigen Tabellen sehen können, ist ein Großteil der Funktionalität zwischen und ontap-nas-economy die ontap-nas gleiche. Da der Treiber jedoch ontap-nas-economy die Möglichkeit zur Steuerung des Zeitplans auf PV-Granularität beschränkt, kann dies insbesondere Ihre Disaster Recovery- und Backup-Planung beeinträchtigen. Für Entwicklungsteams, die die PVC-Klonfunktion auf dem ONTAP-Storage nutzen möchten, ist dies nur mit den, ontap-san oder ontap-san-economy-Treibern möglich ontap-nas.



Der solidfire-san Treiber kann auch VES klonen.

## Back-End-Treiber für Cloud Volumes ONTAP

Cloud Volumes ONTAP bietet Datenkontrolle und Storage-Funktionen der Enterprise-Klasse für verschiedene Anwendungsfälle, einschließlich Dateifreigaben und Storage-Funktionen auf Blockebene für NAS- und SAN-Protokolle (NFS, SMB/CIFS und iSCSI). Die kompatiblen Treiber für Cloud Volume ONTAP sind ontap-nas, ontap-nas-economy ontap-san und ontap-san-economy. Diese gelten für Cloud Volume ONTAP für Azure, Cloud Volume ONTAP für GCP.

## Back-End-Treiber für Amazon FSX for ONTAP

Amazon FSX for NetApp ONTAP ermöglicht Ihnen die Nutzung von NetApp Funktionen, Performance und Administrationsfunktionen, mit denen Sie vertraut sind, und gleichzeitig die Einfachheit, Agilität, Sicherheit und Skalierbarkeit der Speicherung von Daten auf AWS zu nutzen. FSX für ONTAP unterstützt viele ONTAP-Dateisystemfunktionen und Administrations-APIs. Die kompatiblen Treiber für Cloud Volume ONTAP sind ontap-nas, , ontap-nas-economy ontap-nas-flexgroup ontap-san und ontap-san-economy.

## Back-End-Treiber für NetApp HCI/SolidFire

Der solidfire-san Treiber, der mit den NetApp HCI/SolidFire-Plattformen verwendet wird, hilft dem Administrator, ein Element Backend für Trident auf der Grundlage von QoS Limits zu konfigurieren. Wenn Sie Ihr Backend so gestalten möchten, dass die spezifischen QoS-Limits für die durch Trident bereitgestellten Volumes festgelegt werden, verwenden Sie den `type` Parameter in der Backend-Datei. Der Admin kann auch die Volume-Größe einschränken, die mit dem Parameter auf dem Storage erstellt werden `limitVolumeSize` kann. Derzeit werden Element Storage-Funktionen wie die Größenanpassung von Volumes und die Volume-Replizierung nicht durch den Treiber unterstützt solidfire-san. Diese Vorgänge sollten manuell über die Web-UI von Element Software durchgeführt werden.

| SolidFire-Treiber | Snapshot s | Klonen | Multi-Anschluss | CHAP | QoS | Größe Ändern | Replizierung   |
|-------------------|------------|--------|-----------------|------|-----|--------------|----------------|
| solidfire-san     | Ja.        | Ja.    | Jafußnote: 2[]  | Ja.  | Ja. | Ja.          | Jafußnote: 1[] |

Fußnote: Ja [1]: Nicht verwaltet von Trident Yes [2]: Unterstützt für RAW-Block-Volumes

### Back-End-Treiber für Azure NetApp Files

Trident verwendet den `azure-netapp-files` Treiber für die Verwaltung des "[Azure NetApp Dateien](#)" Dienstes.

Weitere Informationen zu diesem Treiber und zur Konfiguration finden Sie unter "["Trident Back-End-Konfiguration für Azure NetApp Files"](#)".

| Azure NetApp Files-Treiber      | Snapshots | Klonen | Multi-Anschluss | QoS | Erweitern | Replizierung  |
|---------------------------------|-----------|--------|-----------------|-----|-----------|---------------|
| <code>azure-netapp-files</code> | Ja.       | Ja.    | Ja.             | Ja. | Ja.       | Jafußnote:1[] |

Fußnote: JaFußnote:1[]: Nicht von Trident verwaltet

### Cloud Volumes Service auf Google Cloud Backend-Treiber

Trident verwendet den `gcp-cvs` Treiber für die Verbindung mit dem Cloud Volumes Service auf Google Cloud.

Der `gcp-cvs` Treiber verwendet virtuelle Pools, um das Backend zu abstrahieren und Trident die Volume-Platzierung zu bestimmen. Der Administrator definiert die virtuellen Pools in den `backend.json` Dateien. Storage-Klassen verwenden Selektoren, um virtuelle Pools nach Etikett zu identifizieren.

- Wenn im Back-End virtuelle Pools definiert werden, versucht Trident, ein Volume in den Google Cloud Storage-Pools zu erstellen, auf das diese virtuellen Pools begrenzt sind.
- Wenn virtuelle Pools nicht im Backend definiert sind, wählt Trident einen Google Cloud-Speicherpool aus den verfügbaren Speicherpools in der Region aus.

Um das Google Cloud-Backend auf Trident zu konfigurieren, müssen Sie `apiRegion` und `apiKey` in der Backend-Datei angeben `projectNumber`. Die Projektnummer finden Sie in der Google Cloud-Konsole. Der API-Schlüssel wird aus der Datei mit dem privaten Schlüssel des Dienstkontos entnommen, die Sie beim Einrichten des API-Zugriffs für Cloud Volumes Service in der Google Cloud erstellt haben.

Weitere Informationen zu Cloud Volumes Service auf Google Cloud Service-Typen und Service-Leveln finden Sie in "["Erfahren Sie mehr zur Unterstützung von Trident für CVS für GCP"](#)".

| Cloud Volumes Service für Google Cloud Treiber | Snapshots | Klonen | Multi-Anschluss | QoS | Erweitern | Replizierung                                     |
|--|-----------|--------|-----------------|-----|-----------|--|
| gcp-cvs  | Ja.       | Ja.    | Ja.             | Ja. | Ja.       | Nur für den CVS-Performance-Diensttyp verfügbar. |

#### Hinweise zur Replikation



- Die Replizierung wird nicht von Trident gemanagt.
- Der Klon wird im selben Speicherpool erstellt wie das Quell-Volume.

## Design der Storage-Klasse

Individuelle Storage-Klassen müssen konfiguriert und angewendet werden, um ein Kubernetes Storage Class-Objekt zu erstellen. Dieser Abschnitt erläutert, wie Sie eine Storage-Klasse für Ihre Applikation entwerfen.

### Spezifische Back-End-Auslastung

Die Filterung kann innerhalb eines bestimmten Storage-Klassenobjekts verwendet werden, um festzulegen, welcher Storage-Pool bzw. welche Pools für die jeweilige Storage-Klasse verwendet werden sollen. In der Storage Class können drei Filtersätze eingestellt werden: `storagePools`, `additionalStoragePools` Und/oder `excludeStoragePools`.

Mit dem `storagePools` Parameter kann der Speicher auf die Gruppe von Pools beschränkt werden, die mit allen angegebenen Attributen übereinstimmen. Mit dem `additionalStoragePools` Parameter wird der Pool-Satz erweitert, den Trident für das Provisioning verwendet, zusammen mit dem durch die Attribute und Parameter ausgewählten Pool-Satz `storagePools`. Sie können entweder nur einen der Parameter oder beide zusammen verwenden, um sicherzustellen, dass der entsprechende Satz von Speicherpools ausgewählt wird.

Der `excludeStoragePools` Parameter wird verwendet, um speziell die aufgelisteten Pools auszuschließen, die mit den Attributen übereinstimmen.

### QoS-Richtlinien emulieren

Wenn Sie Storage-Klassen so entwerfen möchten, dass sie Quality of Service-Richtlinien emulieren, erstellen Sie eine Storage-Klasse mit dem `media` Attribut `hdd` oder `ssd`. Auf der Grundlage des `media` in der Storage-Klasse bereits erwähnten Attributs wählt Trident das geeignete Back-End mit Servern oder `ssd` Aggregaten aus, das `hdd` dem Medienattribut entspricht, und leitet die Bereitstellung der Volumes dann an das spezifische Aggregat weiter. Daher können wir einen PREMIUM-Storage-Klasse erstellen, für `media` den Attribute festgelegt werden, die als `ssd` PREMIUM-QoS-Richtlinie klassifiziert werden könnten. Wir können einen weiteren STANDARD der Storage-Klasse erstellen, bei dem das Medienattribut auf `'hdd'` gesetzt wäre. Dieser Standard könnte die QoS-Richtlinie SEIN. Darüber hinaus könnten wir das Attribut `'IOPS'` in der Storage-Klasse verwenden, um die Bereitstellung zu einer Element Appliance umzuleiten, die als QoS-Richtlinie definiert werden kann.

### Nutzung von Backend basierend auf bestimmten Funktionen

Storage-Klassen ermöglichen die direkte Volume-Bereitstellung an einem bestimmten Back-End, bei dem Funktionen wie Thin Provisioning und Thick Provisioning, Snapshots, Klonen und Verschlüsselung aktiviert sind.

Um festzulegen, welchen Speicher verwendet werden soll, erstellen Sie Speicherklassen, die das entsprechende Back-End mit aktiver Funktion angeben.

## Virtuelle Pools

Virtuelle Pools sind für alle Trident Back-Ends verfügbar. Sie können virtuelle Pools für jedes Back-End definieren, indem Sie einen beliebigen Treiber von Trident verwenden.

Mit virtuellen Pools kann ein Administrator eine Abstraktionsebene über Back-Ends erstellen, auf die über Storage-Klassen verwiesen werden kann. So werden Volumes auf Back-Ends flexibler und effizienter platziert. Verschiedene Back-Ends können mit derselben Serviceklasse definiert werden. Darüber hinaus können mehrere Storage Pools auf demselben Backend erstellt werden, jedoch mit unterschiedlichen Eigenschaften. Wenn eine Speicherklasse mit einem Selektor mit den spezifischen Bezeichnungen konfiguriert ist, wählt Trident ein Backend aus, das allen Selektor-Labels entspricht, um das Volume zu platzieren. Wenn die Auswahlbezeichnungen für Speicherklassen mit mehreren Speicherpools übereinstimmen, wählt Trident einen dieser Speicherpools aus, um das Volume bereitzustellen.

## Virtual Pool Design

Beim Erstellen eines Backend können Sie im Allgemeinen eine Reihe von Parametern angeben. Der Administrator konnte kein weiteres Back-End mit denselben Storage Credentials und anderen Parametern erstellen. Mit der Einführung von virtuellen Pools wurde dieses Problem behoben. Virtual Pools ist eine Ebene-Abstraktion, die zwischen dem Backend und der Kubernetes Storage Class eingeführt wird. So kann der Administrator Parameter zusammen mit Labels definieren, die über Kubernetes Storage Klassen als Selektion auf Backend-unabhängige Weise referenziert werden können. Virtuelle Pools können für alle unterstützten NetApp-Back-Ends mit Trident definiert werden. Dazu zählen SolidFire/NetApp HCI, ONTAP, Cloud Volumes Service auf GCP und Azure NetApp Files.

 Bei der Definition von virtuellen Pools wird empfohlen, nicht zu versuchen, die Reihenfolge vorhandener virtueller Pools in einer Backend-Definition neu anzurufen. Es wird auch empfohlen, Attribute für einen vorhandenen virtuellen Pool nicht zu bearbeiten/zu ändern und stattdessen einen neuen virtuellen Pool zu definieren.

## Emulation verschiedener Service-Level/QoS

Es ist möglich, virtuelle Pools zur Emulation von Serviceklassen zu entwerfen. Untersuchen wir mit der Implementierung des virtuellen Pools für den Cloud Volume Service für Azure NetApp Files, wie wir verschiedene Serviceklassen einrichten können. Konfigurieren Sie das Azure NetApp Files Back-End mit mehreren Labels, die unterschiedliche Performance-Levels repräsentieren. Stellen Sie `servicelevel` Aspect auf das entsprechende Leistungsniveau ein, und fügen Sie weitere erforderliche Aspekte unter den einzelnen Beschriftungen hinzu. Erstellen Sie nun verschiedene Kubernetes Storage-Klassen, die verschiedenen virtuellen Pools zugeordnet werden würden. Über das `parameters.selector` Feld ruft jede StorageClass ab, welche virtuellen Pools zum Hosten eines Volumes verwendet werden können.

## Zuweisen eines spezifischen Satzes von Aspekten

Mehrere virtuelle Pools mit spezifischen Aspekten können über ein einzelnes Storage-Back-End entwickelt werden. Konfigurieren Sie dazu das Backend mit mehreren Beschriftungen und legen Sie die erforderlichen Aspekte unter jedem Etikett fest. Erstellen Sie nun mithilfe des Felds, das verschiedenen virtuellen Pools zugeordnet wird, verschiedene Kubernetes-Storage-Klassen `parameters.selector`. Die Volumes, die im Backend bereitgestellt werden, werden im ausgewählten virtuellen Pool über die Aspekte definiert.

## PVC-Merkmale, die die Storage-Bereitstellung beeinflussen

Einige Parameter, die über die angeforderte Storage-Klasse hinausgehen, können sich bei der Erstellung einer PVC auf den Entscheidungsprozess für die Bereitstellung von Trident auswirken.

### Zugriffsmodus

Wenn Sie Speicher über ein PVC anfordern, ist eines der Pflichtfelder der Zugriffsmodus. Der gewünschte Modus kann sich auf das ausgewählte Backend auswirken, um die Speicheranforderung zu hosten.

Trident versucht, das verwendete Storage-Protokoll mit der gemäß der folgenden Matrix angegebenen Zugriffsmethode abzustimmen. Dies ist unabhängig von der zugrunde liegenden Storage-Plattform.

|       | <b>ReadWriteOnce</b> | <b>ReadOnlyManche</b> | <b>ReadWriteViele</b> |
|-------|----------------------|-----------------------|-----------------------|
| ISCSI | Ja.                  | Ja.                   | Ja (Raw Block)        |
| NFS   | Ja.                  | Ja.                   | Ja.                   |

Eine Anfrage nach einem **ReadWriteManche** PVC, die an eine Trident-Implementierung ohne konfiguriertes NFS-Backend gesendet werden, führt dazu, dass kein Volume bereitgestellt wird. Aus diesem Grund sollte der Anforderer den Zugriffsmodus verwenden, der für seine Anwendung geeignet ist.

## Volume-Vorgänge

### Persistente Volumes ändern

Persistente Volumes sind mit zwei Ausnahmen unveränderliche Objekte in Kubernetes. Sobald die Rückgewinnungsrichtlinie erstellt wurde, kann die Größe geändert werden. Dies hindert jedoch nicht daran, einige Aspekte des Volumes außerhalb von Kubernetes zu ändern. Das kann durchaus wünschenswert sein, wenn das Volume für spezifische Applikationen angepasst werden soll, um sicherzustellen, dass die Kapazität nicht versehentlich verbraucht wird oder das Volume einfach aus irgendeinem Grund auf einen anderen Storage Controller verschoben werden kann.



Kubernetes in-Tree-Provisionierer unterstützen derzeit keine Volume-Größenänderungen für NFS, iSCSI oder FC PVs. Trident unterstützt die Erweiterung von NFS-, iSCSI- und FC-Volumes.

Die Verbindungsdetails des PV können nach der Erstellung nicht geändert werden.

### Erstellung von On-Demand-Volume-Snapshots

Trident unterstützt die Erstellung von On-Demand-Volume-Snapshots und die Erstellung von VES aus Snapshots mithilfe des CSI-Frameworks. Snapshots bieten eine bequeme Methode, zeitpunktgenaue Kopien der Daten zu erstellen und haben unabhängig vom Quell-PV in Kubernetes einen Lebenszyklus. Diese Snapshots können zum Klonen von PVCs verwendet werden.

### Volumes-Erstellung aus Snapshots

Trident unterstützt außerdem die Erstellung von PersistentVolumes aus Volume Snapshots. Um dies zu erreichen, erstellen Sie einfach ein PersistentVolumeClaim und erwähnen Sie den `datasource` als den erforderlichen Snapshot, aus dem das Volume erstellt werden muss. Trident wird diese PVC behandeln, indem ein Volume mit den auf dem Snapshot vorhandenen Daten erstellt wird. Mit dieser Funktion können Daten regionsübergreifend dupliziert, Testumgebungen erstellt, ein defektes oder defektes Produktionsvolumen

vollständig ersetzt oder bestimmte Dateien und Verzeichnisse abgerufen und auf ein anderes angeschlossenes Volume übertragen werden.

## **Verschieben Sie Volumes im Cluster**

Storage-Administratoren können Volumes zwischen Aggregaten und Controllern im ONTAP Cluster unterbrechungsfrei für den Storage-Nutzer verschieben. Dieser Vorgang wirkt sich nicht auf die Trident oder das Kubernetes-Cluster aus, sofern es sich bei dem Zielaggregat um ein Aggregat handelt, auf das die SVM von Trident zugreifen kann. Wichtig: Wenn das Aggregat neu zur SVM hinzugefügt wurde, muss das Backend durch erneutes Hinzufügen zur Trident aktualisiert werden. Dies wird dazu führen, dass Trident die SVM erneut inventarisiert, damit das neue Aggregat erkannt wird.

Das Verschieben von Volumes zwischen Back-Ends wird von Trident jedoch nicht automatisch unterstützt. Dies umfasst auch zwischen SVMs im selben Cluster, zwischen Clustern oder auf eine andere Storage-Plattform (selbst dann, wenn es sich bei dem Storage-System um einen mit Trident verbundenen handelt).

Wenn ein Volume an einen anderen Speicherort kopiert wird, kann die Volume-Importfunktion verwendet werden, um aktuelle Volumes in Trident zu importieren.

## **Erweitern Sie Volumes**

Trident unterstützt die Anpassung von NFS-, iSCSI- und FC-PVS. Dadurch können Benutzer ihre Volumes direkt über die Kubernetes-Ebene skalieren. Eine Volume-Erweiterung ist für alle größeren NetApp Storage-Plattformen möglich, einschließlich ONTAP, SolidFire/NetApp HCI und Cloud Volumes Service Back-Ends. Um später eine mögliche Erweiterung zu ermöglichen, setzen Sie `allowVolumeExpansion` in der mit dem Volume verknüpften StorageClass auf `true`. Wenn die Größe des persistenten Volumes geändert werden muss, bearbeiten Sie die `spec.resources.requests.storage` Anmerkung im Persistent Volume Claim auf die erforderliche Volume-Größe. Trident übernimmt automatisch die Anpassung der Größe des Volumes im Storage-Cluster.

## **Importieren eines vorhandenen Volumes in Kubernetes**

Mit dem Volume-Import kann ein vorhandenes Storage Volume in eine Kubernetes-Umgebung importiert werden. Dies wird derzeit von den „ontap-nas-flexgroup“, „solidfire-san“ „azure-netapp-files“ und „gcp-cvs“ Treibern unterstützt „ontap-nas“. Diese Funktion ist hilfreich, wenn Sie eine vorhandene Applikation in Kubernetes oder während Disaster-Recovery-Szenarien portieren.

Verwenden Sie bei Verwendung der ONTAP und solidfire-san Treiber den Befehl, `tridentctl import volume <backend-name> <volume-name> -f /path/pvc.yaml` um ein vorhandenes Volume in Kubernetes zu importieren, das von Trident gemanagt werden soll. Die im Befehl des Import-Volumes verwendete PVC-YAML- oder JSON-Datei verweist auf eine Storage-Klasse, die Trident als bereitstellung identifiziert. Stellen Sie bei Verwendung eines NetApp HCI/SolidFire Backend sicher, dass die Volume-Namen eindeutig sind. Wenn die Volume-Namen dupliziert sind, klonen Sie das Volume auf einen eindeutigen Namen, sodass die Funktion zum Importieren des Volumes zwischen diesen Namen unterscheiden kann.

Verwenden Sie bei Verwendung des „azure-netapp-files“ Treibers oder „gcp-cvs“ den Befehl, `tridentctl import volume <backend-name> <volume path> -f /path/pvc.yaml` um das Volume in Kubernetes zu importieren, das von Trident gemanagt werden soll. Dadurch wird eine eindeutige Volumenreferenz sichergestellt.

Wenn der obige Befehl ausgeführt wird, findet Trident das Volume auf dem Backend und liest seine Größe. Die Volume-Größe der konfigurierten PVC wird automatisch hinzugefügt (und bei Bedarf überschrieben). Trident erstellt dann das neue PV und Kubernetes bindet die PVC an das PV.

Wenn ein Container so eingesetzt wurde, dass er das spezifische importierte PVC benötigt, bleibt er in einem ausstehenden Zustand, bis das PVC/PV-Paar über den Volumenimport gebunden ist. Nachdem das PVC/PV-Paar gebunden ist, sollte der Behälter aufstehen, sofern keine anderen Probleme auftreten.

## Registry-Service

Die Bereitstellung und Verwaltung von Speicher für die Registrierung wurde im dokumentiert "[netapp.io/Blog](http://netapp.io/Blog)".

## Protokollierungsservice

Wie andere OpenShift-Services wird auch der Protokollierungsservice mithilfe von Ansible implementiert. Die Konfigurationsparameter werden von der Inventardatei, auch als Hosts bekannt, bereitgestellt für das Playbook. Es gibt zwei Installationsmethoden: Die Bereitstellung von Protokollierung während der ersten OpenShift-Installation und die Bereitstellung von Protokollierung nach der Installation von OpenShift.

Ab Red hat OpenShift Version 3.9 empfiehlt die offizielle Dokumentation gegen NFS für den Protokollierungsservice, da sie Bedenken hinsichtlich Datenbeschädigung hat. Dies basiert auf Red hat Tests ihrer Produkte. Der ONTAP NFS-Server weist diese Probleme nicht auf und kann problemlos eine Protokollierungsbereitstellung zurücksichern. Letztendlich liegt die Wahl des Protokolls für den Protokollierungsservice bei Ihnen. Ich weiß nur, dass beide bei der Nutzung von NetApp Plattformen hervorragend funktionieren. Es gibt keinen Grund, NFS zu vermeiden, wenn dies Ihre Präferenz ist.

Wenn Sie NFS mit dem Protokollierungsdienst verwenden, müssen Sie die Ansible-Variable so einstellen `openshift_enable_unsupported_configurations`, dass `true` das Installationsprogramm nicht fehlschlägt.

### Los geht's

Der Protokollierungsservice kann optional sowohl für Applikationen als auch für die Kernvorgänge des OpenShift-Clusters selbst implementiert werden. Wenn Sie sich für die Bereitstellung von Operationen entscheiden, werden durch Angabe der Variable `openshift_logging_use_ops` als `true` zwei Instanzen des Dienstes erstellt. Die Variablen, die die Protokollierungsinstanz für Vorgänge steuern, enthalten darin "OPS", während die Instanz für Anwendungen nicht.

Das Konfigurieren der Ansible-Variablen gemäß der Implementierungsmethode ist wichtig, um sicherzustellen, dass der richtige Storage von den zugrunde liegenden Services verwendet wird. Betrachten wir nun die Optionen für die einzelnen Bereitstellungsmethoden.

Die folgenden Tabellen enthalten nur die für die Speicherkonfiguration relevanten Variablen, die sich auf den Protokollierungsservice beziehen. Sie können andere Optionen finden, in "["Dokumentation der Red hat OpenShift -Protokollierung"](#)" denen Sie entsprechend Ihrer Bereitstellung prüfen, konfigurieren und verwenden sollten.

Die Variablen in der folgenden Tabelle führen dazu, dass im Ansible-Playbook ein PV und eine PVC für den Protokollierungsservice erstellt werden. Diese Details werden verwendet. Diese Methode ist wesentlich weniger flexibel als nach der Installation von OpenShift das Playbook für die Komponenteninstallation zu verwenden. Wenn Sie jedoch vorhandene Volumes zur Verfügung haben, ist dies eine Option.

| Variabell                                   | Details  |
|---|--|
| <code>openshift_logging_storage_kind</code> | Legen Sie fest <code>nfs</code> , dass der Installer ein NFS-PV für den Protokollierungsdienst erstellen soll. |

| Variabel                                | Details  |
|---|--|
| openshift_logging_storage_host          | Der Hostname oder die IP-Adresse des NFS-Hosts. Dies sollte auf die DatenLIF für Ihre Virtual Machine festgelegt werden.                                     |
| openshift_logging_storage_nfs_directory | Der Mount-Pfad für den NFS-Export. Wenn das Volume beispielsweise als verbunden ist, /openshift_logging würden Sie diesen Pfad für diese Variable verwenden. |
| openshift_logging_storage_volume_name   | Der Name, z. B. pv_ose_logs, des zu erstellenden PV.   |
| openshift_logging_storage_volume_size   | Die Größe des NFS-Exports, zum Beispiel 100Gi.   |

Wenn Ihr OpenShift-Cluster bereits ausgeführt wird und daher Trident implementiert und konfiguriert wurde, kann das Installationsprogramm die Volumes mithilfe der dynamischen Provisionierung erstellen. Die folgenden Variablen müssen konfiguriert werden.

| Variabel  | Details   |
|---|---|
| openshift_logging_es_pvc_dynamic                | Setzen Sie auf „true“, um dynamisch bereitgestellte Volumes zu verwenden.   |
| openshift_logging_es_pvc_storage_class_name     | Der Name der Speicherklasse, die in der PVC verwendet wird.   |
| openshift_logging_es_pvc_size                   | Die Größe des im PVC angeforderten Volumens.  |
| openshift_logging_es_pvc_prefix                 | Ein Präfix für die vom Protokollierungsservice verwendeten VES.   |
| openshift_logging_es_ops_pvc_dynamic            | Legen Sie fest true, dass dynamisch bereitgestellte Volumes für die OPS-Protokollinstanz verwendet werden sollen. |
| openshift_logging_es_ops_pvc_storage_class_name | Der Name der Speicherklasse für die OPS-Protokollierungsinstanz.  |
| openshift_logging_es_ops_pvc_size               | Die Größe der Volume-Anforderung für die OPS-Instanz.   |
| openshift_logging_es_ops_pvc_prefix             | Ein Präfix für die OPS-Instanz VES.   |

### Bereitstellen des Protokollierungs-Stacks

Wenn Sie die Protokollierung als Teil des ursprünglichen OpenShift-Installationsprozesses bereitstellen, müssen Sie nur den Standardprozess für die Bereitstellung befolgen. Ansible konfiguriert und implementiert die erforderlichen Services und OpenShift-Objekte, sodass der Service sobald Ansible abgeschlossen ist.

Wenn Sie die Implementierung jedoch nach der Erstinstallation durchführen, muss das Komponenten-Playbook von Ansible verwendet werden. Dieser Vorgang kann sich bei verschiedenen Versionen von OpenShift geringfügig ändern. Lesen Sie daher unbedingt ["Dokumentation zur Red hat OpenShift Container Platform 3.11"](#) die Informationen zu Ihrer Version.

## Kennzahlungsservice

Der Kennzahlungsservice liefert dem Administrator wertvolle Informationen zum Status, zur Ressourcenauslastung und zur Verfügbarkeit des OpenShift-Clusters. Dies ist zudem für die automatische Pod-Funktionalität erforderlich, und viele Unternehmen nutzen die Daten des Kennzahlungsservice für ihre Kostenabrechnung und/oder die Anzeige von Applikationen.

Wie beim Protokollierungsservice und OpenShift als Ganzes wird auch Ansible für die Implementierung des Kennzahlungsservice verwendet. Ebenso wie der Protokollierungsservice kann der Metrikservice während der ersten Einrichtung des Clusters oder nach dessen Betrieb mithilfe der Installationsmethode für Komponenten bereitgestellt werden. Die folgenden Tabellen enthalten die Variablen, die für die Konfiguration von persistentem Storage für den Kennzahlungsservice wichtig sind.

 Die nachfolgenden Tabellen enthalten nur die Variablen, die für die Storage-Konfiguration relevant sind, da sie sich auf den Kennzahlenservice beziehen. Es gibt viele andere Optionen in der Dokumentation gefunden, die entsprechend Ihrer Bereitstellung überprüft, konfiguriert und verwendet werden sollten.

| Variabel                                | Details   |
|---|---|
| openshift_metrics_storage_kind          | Legen Sie fest <code>nfs</code> , dass der Installer ein NFS-PV für den Protokollierungsdienst erstellen soll.  |
| openshift_metrics_storage_host          | Der Hostname oder die IP-Adresse des NFS-Hosts. Dies sollte auf die DatenLIF für Ihre SVM eingestellt werden.   |
| openshift_metrics_storage_nfs_directory | Der Mount-Pfad für den NFS-Export. Wenn das Volume beispielsweise als verbunden ist, <code>/openshift_metrics</code> würden Sie diesen Pfad für diese Variable verwenden. |
| openshift_metrics_storage_volume_name   | Der Name, z. B. <code>pv_ose_metrics</code> , des zu erstellenden PV.   |
| openshift_metrics_storage_volume_size   | Die Größe des NFS-Exports, zum Beispiel <code>100Gi</code> .  |

Wenn Ihr OpenShift-Cluster bereits ausgeführt wird und daher Trident implementiert und konfiguriert wurde, kann das Installationsprogramm die Volumes mithilfe der dynamischen Provisionierung erstellen. Die folgenden Variablen müssen konfiguriert werden.

| Variabel   | Details   |
|--|---|
| openshift_metrics_cassandra_pvc_prefix             | Ein Präfix, das für die PVCs der Kennzahlen verwendet wird.   |
| openshift_metrics_cassandra_pvc_size               | Die Größe der Volumes, die angefordert werden sollen.   |
| openshift_metrics_cassandra_storage_type           | Der Storage-Typ, der für Metriken verwendet werden soll. Dieser muss für Ansible auf dynamisch festgelegt sein, um PVCs mit der entsprechenden Storage-Klasse zu erstellen. |
| openshift_metrics_cassandra_pvc_storage_class_name | Der Name der zu verwendenden Speicherklasse.  |

## Bereitstellen des Kennzahlenservice

Implementieren Sie den Service mithilfe von Ansible, wenn Sie die entsprechenden Ansible-Variablen in der Host-/Inventardatei festlegen. Wenn Sie zur Installationszeit OpenShift bereitstellen, wird das PV automatisch erstellt und verwendet. Wenn Sie nach der Installation von OpenShift mit den Komponenten-Playbooks implementieren, erstellt Ansible alle erforderlichen PVCs. Nachdem Trident Storage für sie bereitgestellt hat, kann der Service implementiert werden.

Die oben genannten Variablen und der Prozess für die Bereitstellung können sich mit jeder Version von OpenShift ändern. Überprüfen und befolgen Sie ["Red hat OpenShift Deployment Guide"](#) Ihre Version, damit sie für Ihre Umgebung konfiguriert ist.

# Datensicherung und Disaster Recovery

Informieren Sie sich über Sicherungs- und Recovery-Optionen für Trident und Volumes, die mit Trident erstellt wurden. Für jede Applikation mit einer Persistenzanforderung sollte eine Datensicherungs- und Recovery-Strategie eingesetzt werden.

## Replizierung und Recovery mit Trident

Sie können ein Backup erstellen, um Trident im Notfall wiederherzustellen.

### Replizierung mit Trident

Trident verwendet Kubernetes CRDs zum Speichern und Managen seines eigenen Zustands sowie des Kubernetes-Clusters und etcd zum Speichern seiner Metadaten.

#### Schritte

1. Backup des Kubernetes-Clusters etcd mit ["Kubernetes: Backup eines uscd-Clusters"](#).
2. Platzieren Sie die Backup-Artefakte auf einer FlexVol volume



NetApp empfiehlt die Sicherung der SVM, auf der sich die FlexVol mit einer SnapMirror-Beziehung zu einer anderen SVM befindet.

### Recovery von Trident

Mit Kubernetes-CRDs und dem Kubernetes-Cluster und Snapshot können Sie Trident wiederherstellen.

#### Schritte

1. Mounten Sie von der Ziel-SVM das Volume, das die Kubernetes usw.-Datendateien und Zertifikate enthält, auf dem Host, der als Master-Node eingerichtet wird.
2. Kopieren Sie alle erforderlichen Zertifikate zum Kubernetes-Cluster unter /etc/kubernetes/pki und die etcd-Mitgliedsdateien unter /var/lib/etcd.
3. Stellen Sie den Kubernetes-Cluster aus dem etcd ["Kubernetes: Wiederherstellung eines uscd-Clusters"](#)-Backup mit wieder her.
4. Führen Sie aus kubectl get crd, um zu überprüfen, ob alle benutzerdefinierten Trident-Ressourcen eingerichtet sind, und rufen Sie die Trident-Objekte ab, um zu überprüfen, ob alle Daten verfügbar sind.

## SVM-Replizierung und Recovery

Trident kann keine Replizierungsbeziehungen konfigurieren. Der Storage-Administrator kann jedoch zur Replizierung einer SVM verwenden "[ONTAP SnapMirror](#)".

Bei einem Notfall können Sie die SnapMirror Ziel-SVM aktivieren, um die Datenbereitstellung zu starten. Sie können zurück zum primären System wechseln, wenn die Systeme wiederhergestellt sind.

### Über diese Aufgabe

Bei Verwendung der SnapMirror SVM-Replizierungsfunktion sind die folgenden Überlegungen zu beachten:

- Sie sollten für jede SVM ein eigene Back-End mit aktiver SVM-DR erstellen.
- Konfigurieren Sie die Storage-Klassen so, dass die replizierten Back-Ends nur bei Bedarf ausgewählt werden, um zu vermeiden, dass Volumes ohne Replizierung auf den Back-Ends bereitgestellt werden, die SVM-DR unterstützen.
- Applikationsadministratoren sollten sich über die zusätzlichen Kosten und die Komplexität der Replizierung informieren und ihren Recovery-Plan vor Beginn des Prozesses sorgfältig prüfen.

### SVM-Replizierung

Sie können zum Erstellen der SVM-Replizierungsbeziehung verwenden "[ONTAP: SnapMirror SVM-Replizierung](#)".

Mit SnapMirror können Sie festlegen, was repliziert werden soll. Sie müssen wissen, welche Optionen Sie beim Preforming ausgewählt [SVM-Recovery mit Trident](#) haben.

- "[-Identität-bewahren wahr](#)" Replizierung der gesamten SVM-Konfiguration
- "[-Discard-configs Netzwerk](#)" Davon sind LIFs und zugehörige Netzwerkeinstellungen nicht enthalten.
- "[-Identity-preserve false](#)" Repliziert nur die Volumes und die Sicherheitskonfiguration.

### SVM-Recovery mit Trident

Trident erkennt SVM-Fehler nicht automatisch. Bei einem Notfall kann der Administrator das Trident Failover manuell auf die neue SVM initialisieren.

#### Schritte

1. Abbrechen geplanter und laufender SnapMirror Übertragungen, Abbrechen der Replizierungsbeziehung, stoppen Sie die Quell-SVM und aktivieren Sie dann die SnapMirror Ziel-SVM.
2. Wenn Sie die SVM-Replikation angegeben `-identity-preserve false` oder `-discard-config network` konfiguriert haben, aktualisieren Sie `managementLIF` und `dataLIF` in der Trident-Backend-Definitionsdatei.
3. Bestätigen `storagePrefix` ist in der Trident-Backend-Definitionsdatei vorhanden. Dieser Parameter kann nicht geändert werden. Wenn Sie das Backend nicht `storagePrefix` mehr verwenden, schlägt das Update fehl.
4. Aktualisieren Sie alle erforderlichen Back-Ends, um den neuen Ziel-SVM-Namen widerzuspiegeln. Verwenden Sie dazu Folgendes:

```
./tridentctl update backend <backend-name> -f <backend-json-file> -n <namespace>
```

5. Wenn Sie oder `discard-config` network angegeben `-identity-preserve false` haben, müssen Sie alle Anwendungspads zurückspringen.



Wenn Sie angegeben haben `-identity-preserve true`, beginnen alle von Trident bereitgestellten Volumes mit der Bereitstellung von Daten, wenn die Ziel-SVM aktiviert ist.

## Volume-Replizierung und Recovery

Trident kann keine SnapMirror-Replizierungsbeziehungen konfigurieren. Der Storage-Administrator kann jedoch zur Replizierung von Volumes verwenden "["Replizierung und Recovery mit ONTAP SnapMirror"](#)", die von Trident erstellt wurden.

Sie können dann importieren Sie die wiederhergestellten Volumes in Trident mit "["Tridentctl-Volumenimport"](#)".



Import wird auf `, ontap-san-economy` oder `ontap-flexgroup-economy` Treibern nicht unterstützt `ontap-nas-economy`.

## Snapshot Datensicherung

Sie können Daten schützen und wiederherstellen mit:

- Ein externer Snapshot-Controller und CRDs zum Erstellen von Kubernetes-Volume-Snapshots von persistenten Volumes (PVs).

["Volume Snapshots"](#)

- ONTAP Snapshots zur Wiederherstellung der gesamten Inhalte eines Volumes oder zur Wiederherstellung einzelner Dateien oder LUNs.

["ONTAP Snapshots"](#)

## Sicherheit

### Sicherheit

Mit den hier aufgeführten Empfehlungen können Sie sicherstellen, dass Ihre Trident-Installation sicher ist.

#### Ausführen von Trident in seinem eigenen Namespace

Es ist wichtig, zu verhindern, dass Applikationen, Applikationsadministratoren, Benutzer und Managementapplikationen auf Trident-Objektdefinitionen oder Pods zugreifen, um zuverlässigen Storage sicherzustellen und potenzielle böswillige Aktivitäten zu blockieren.

Um die anderen Anwendungen und Benutzer von Trident (`trident`` zu trennen, installieren Sie Trident immer in seinem eigenen Kubernetes Namespace ). Wenn Trident in seinen eigenen Namespace gelegt wird, wird sichergestellt, dass nur das Kubernetes-Administratorpersonal Zugriff auf den Trident Pod hat und auf die Artefakte (z. B. Backend- und CHAP-Geheimnisse, falls zutreffend), die in den nameschritt-CRD-Objekten gespeichert sind. Sie sollten sicherstellen, dass nur Administratoren

Zugriff auf den Trident-Namespace und damit auf die `tridentctl` Anwendung haben.

## Verwenden Sie CHAP-Authentifizierung mit ONTAP SAN Back-Ends

Trident unterstützt die CHAP-basierte Authentifizierung für ONTAP-SAN-Workloads (unter Verwendung der `ontap-san` Treiber und `ontap-san-economy`). NetApp empfiehlt zur Authentifizierung zwischen einem Host und dem Storage-Back-End die Verwendung von bidirektionalem CHAP mit Trident.

Für ONTAP-Back-Ends, die die SAN-Speichertreiber verwenden, kann Trident bidirektionales CHAP einrichten und CHAP-Benutzernamen und -Schlüssel über verwalten `tridentctl`. Weitere Informationen zur Trident Konfiguration von CHAP auf ONTAP-Back-Ends finden Sie unter "["Vorbereiten der Back-End-Konfiguration mit ONTAP-SAN-Treibern"](#)".

## Verwenden Sie CHAP-Authentifizierung mit NetApp HCI und SolidFire Back-Ends

NetApp empfiehlt die Implementierung von bidirektionalem CHAP, um die Authentifizierung zwischen einem Host und den NetApp HCI und SolidFire Back-Ends zu gewährleisten. Trident verwendet ein geheimes Objekt, das zwei CHAP-Passwörter pro Mandant enthält. Wenn Trident installiert ist, verwaltet es die CHAP-Schlüssel und speichert sie in einem `tridentvolume` CR-Objekt für das jeweilige PV. Wenn Sie ein PV erstellen, verwendet Trident die CHAP-Schlüssel, um eine iSCSI-Sitzung zu initiieren und über CHAP mit dem NetApp HCI- und SolidFire-System zu kommunizieren.



Die Volumes, die von Trident erstellt werden, sind keiner Volume Access Group zugeordnet.

## Verwenden Sie Trident mit NVE und NAE

NetApp ONTAP bietet Verschlüsselung ruhender Daten zum Schutz sensibler Daten, wenn eine Festplatte gestohlen, zurückgegeben oder einer neuen Verwendung zugewiesen wird. Weitere Informationen finden Sie unter "["NetApp Volume Encryption Übersicht konfigurieren"](#)".

- Wenn auf dem Backend NAE aktiviert ist, wird jedes in Trident bereitgestellte Volume NAE-aktiviert.
  - Sie können das NVE-Verschlüsselungs-Flag auf festlegen "", um NAE-fähige Volumes zu erstellen.
- Wenn NAE im Back-End nicht aktiviert ist, wird jedes in Trident bereitgestellte Volume NVE-aktiviert, es sei denn, das NVE-Verschlüsselungs-Flag ist in der Back-End-Konfiguration auf (Standardwert) gesetzt `false`.

Volumes, die in Trident auf einem NAE-fähigen Back-End erstellt wurden, müssen mit NVE oder NAE verschlüsselt werden.



- Sie können in der Trident-Backend-Konfiguration das NVE-Verschlüsselungsflag auf `true` setzen, um die NAE-Verschlüsselung außer Kraft zu setzen und für jedes Volume einen bestimmten Verschlüsselungsschlüssel zu verwenden.
- Wenn Sie das NVE-Verschlüsselungsflag auf ein NAE-fähiges Back-End setzen `false`, wird ein NAE-fähiges Volume erstellt. Sie können die NAE-Verschlüsselung nicht deaktivieren, indem Sie das NVE-Verschlüsselungsflag auf `false`.

- Sie können ein NVE Volume manuell in Trident erstellen, indem Sie das NVE Verschlüsselungs-Flag explizit auf setzen `true`.

Weitere Informationen zu Back-End-Konfigurationsoptionen finden Sie unter:

- "[SAN-Konfigurationsoptionen von ONTAP](#)"
- "[NAS-Konfigurationsoptionen von ONTAP](#)"

## Linux Unified Key Setup (LUKS)

Sie können Linux Unified Key Setup (LUKS) aktivieren, um ONTAP SAN und ONTAP SAN ECONOMY Volumes auf Trident zu verschlüsseln. Trident unterstützt die Rotation der Passphrase und die Volume-Erweiterung für LUKS-verschlüsselte Volumes.

In Trident verwenden LUKS-verschlüsselte Volumes den aes-xts-plain64-Cypher und -Modus, wie von empfohlen "[NIST](#)".

### Bevor Sie beginnen

- Worker Nodes müssen cryptsetup 2.1 oder höher (aber unter 3.0) installiert sein. Weitere Informationen finden Sie unter "[Gitlab: Cryptsetup](#)".
- Aus Performance-Gründen empfiehlt NetApp, dass Workerknoten die AES-NI (Advanced Encryption Standard New Instructions) unterstützen. Führen Sie den folgenden Befehl aus, um die Unterstützung von AES-NI zu überprüfen:

```
grep "aes" /proc/cpuinfo
```

Wenn nichts zurückgegeben wird, unterstützt Ihr Prozessor nicht AES-NI. Weitere Informationen zu AES-NI finden Sie unter "[Intel: Advanced Encryption Standard Instructions \(AES-NI\)](#)".

### Aktivieren Sie die LUKS-Verschlüsselung

Sie können die Verschlüsselung auf Host-Seite pro Volume mithilfe von Linux Unified Key Setup (LUKS) für ONTAP SAN und ONTAP SAN ECONOMY Volumes aktivieren.

#### Schritte

1. Definieren Sie LUKS-Verschlüsselungsattribute in der Backend-Konfiguration. Weitere Informationen zu den Back-End-Konfigurationsoptionen für ONTAP-SAN finden Sie unter "[SAN-Konfigurationsoptionen von ONTAP](#)".

```
{
  "storage": [
    {
      "labels": {
        "luks": "true"
      },
      "zone": "us_east_1a",
      "defaults": {
        "luksEncryption": "true"
      }
    },
    {
      "labels": {
        "luks": "false"
      },
      "zone": "us_east_1a",
      "defaults": {
        "luksEncryption": "false"
      }
    }
  ]
}
```

2. `parameters.selector` Zum Definieren der Speicherpools mit LUKS-Verschlüsselung. Beispiel:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: csi.trident.netapp.io
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```

3. Erstellen Sie ein Geheimnis, das die LUKS-Passphrase enthält. Beispiel:

```
kubectl -n trident create -f luks-pvc1.yaml
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: A
  luks-passphrase: secretA
```

## Einschränkungen

LUKS-verschlüsselte Volumes können die ONTAP Deduplizierung und Komprimierung nicht nutzen.

## Back-End-Konfiguration zum Importieren von LUKS-Volumes

Um ein LUKS-Volume zu importieren, müssen Sie auf dem Backend festlegen `luksEncryption`. Die `luksEncryption` Option zeigt Trident an, ob das Volume LUKS-konform ist (`true`) oder nicht LUKS-konform (`false`), wie im folgenden Beispiel gezeigt.

```
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: trident_svm
username: admin
password: password
defaults:
  luksEncryption: 'true'
  spaceAllocation: 'false'
  snapshotPolicy: default
  snapshotReserve: '10'
```

## PVC-Konfiguration für den Import von LUKS-Volumes

Um LUKS-Volumes dynamisch zu importieren, setzen Sie die Beschriftung `trident.netapp.io/luksEncryption` auf `true` und fügen Sie eine LUKS-fähige Storage-Klasse in die PVC ein, wie in diesem Beispiel gezeigt.

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: luks-pvc
  namespace: trident
  annotations:
    trident.netapp.io/luksEncryption: "true"
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: luks-sc

```

## Eine LUKS-Passphrase drehen

Sie können die LUKS-Passphrase drehen und die Drehung bestätigen.



Vergessen Sie keine Passphrase, bis Sie überprüft haben, dass sie nicht mehr von einem Volume, einem Snapshot oder einem geheimen Schlüssel referenziert wird. Wenn eine referenzierte Passphrase verloren geht, können Sie das Volume möglicherweise nicht mounten und die Daten bleiben verschlüsselt und unzugänglich.

## Über diese Aufgabe

DIE Drehung der LUKS-Passphrase erfolgt, wenn ein Pod, das das Volume bindet, nach der Angabe einer neuen LUKS-Passphrase erstellt wird. Wenn ein neuer Pod erstellt wird, vergleicht Trident die LUKS-Passphrase auf dem Volume mit der aktiven Passphrase im Secret.

- Wenn die Passphrase auf dem Volume nicht mit der aktiven Passphrase im Geheimnis übereinstimmt, erfolgt die Drehung.
- Wenn die Passphrase auf dem Volume mit der aktiven Passphrase im Secret übereinstimmt, wird der `previous-luks-passphrase` Parameter ignoriert.

## Schritte

1. Fügen Sie die Parameter und `node-publish-secret-namespace` StorageClass hinzu `node-publish-secret-name`. Beispiel:

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-san
provisioner: csi.trident.netapp.io
parameters:
  trident.netapp.io/backendType: "ontap-san"
  csi.storage.k8s.io/node-stage-secret-name: luks
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-publish-secret-name: luks
  csi.storage.k8s.io/node-publish-secret-namespace: ${pvc.namespace}

```

2. Identifizieren Sie vorhandene Passphrases auf dem Volume oder Snapshot.

#### Datenmenge

```

tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames: ["A"]

```

#### Snapshot

```

tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames: ["A"]

```

3. Aktualisieren Sie das LUKS-Geheimnis für das Volume, um die neuen und vorherigen Passphrases anzugeben. Stellen Sie sicher, dass `previous-luke-passphrase-name` `previous-luks-passphrase` die vorherige Passphrase übereinstimmt.

```

apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: B
  luks-passphrase: secretB
  previous-luks-passphrase-name: A
  previous-luks-passphrase: secretA

```

4. Erstellen Sie einen neuen Pod, der das Volume montiert. Dies ist erforderlich, um die Rotation zu initiieren.
5. Überprüfen Sie, ob die Passphrase gedreht wurde.

## Datenmenge

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames: ["B"]
```

## Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames: ["B"]
```

## Ergebnisse

Die Passphrase wurde gedreht, wenn nur die neue Passphrase auf dem Volume und dem Snapshot zurückgegeben wird.



Werden beispielsweise zwei Passphrasen zurückgegeben, luksPassphraseNames: ["B", "A"] ist die Rotation unvollständig. Sie können einen neuen Pod auslösen, um zu versuchen, die Rotation abzuschließen.

## Aktivieren Sie die Volume-Erweiterung

Sie können Volume-Erweiterung auf einem LUKS-verschlüsselten Volume aktivieren.

### Schritte

1. Aktivieren Sie das `CSINodeExpandSecret` Feature Gate (Beta 1.25+). Weitere Informationen finden Sie unter ["Kubernetes 1.25: Verwenden Sie Secrets zur Node-gesteuerten Erweiterung von CSI Volumes"](#).
2. Fügen Sie die Parameter und `node-expand-secret-namespace` `StorageClass` hinzu `node-expand-secret-name`. Beispiel:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: csi.trident.netapp.io
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-expand-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-expand-secret-namespace: ${pvc.namespace}
allowVolumeExpansion: true
```

## Ergebnisse

Wenn Sie die Online-Speichererweiterung initiieren, gibt das Kubelet die entsprechenden Zugangsdaten an den Treiber weiter.

## Kerberos Verschlüsselung während der Übertragung

Mit der Kerberos-Verschlüsselung während der Übertragung können Sie die Datensicherheit verbessern, indem Sie die Verschlüsselung für den Datenverkehr zwischen dem verwalteten Cluster und dem Storage-Back-End aktivieren.

Trident unterstützt Kerberos Verschlüsselung für ONTAP als Storage-Back-End:

- **On-Premise-ONTAP** – Trident unterstützt Kerberos-Verschlüsselung über NFSv3- und NFSv4-Verbindungen von Red Hat OpenShift und Upstream-Kubernetes-Clustern zu lokalen ONTAP-Volumes.

Sie können Snapshots, Klone, schreibgeschütztes Klonen und Importieren von Volumes mit NFS-Verschlüsselung.

## Konfiguration der in-Flight-Kerberos-Verschlüsselung mit lokalen ONTAP-Volumes

Sie können die Kerberos-Verschlüsselung auf dem Storage-Datenverkehr zwischen dem verwalteten Cluster und einem lokalen ONTAP-Storage-Back-End aktivieren.



Kerberos-Verschlüsselung für NFS-Datenverkehr mit On-Premise ONTAP-Storage-Back-Ends wird nur mithilfe des Speichertreibers unterstützt `ontap-nas`.

## Bevor Sie beginnen

- Stellen Sie sicher, dass Sie Zugriff auf das Dienstprogramm haben `tridentctl` .
- Stellen Sie sicher, dass Sie Administratorzugriff auf das ONTAP Storage Back-End haben.
- Stellen Sie sicher, dass Sie den Namen des Volumes oder der Volumes kennen, die Sie über das ONTAP-Speicher-Back-End freigeben werden.
- Stellen Sie sicher, dass Sie die ONTAP-Storage-VM auf die Unterstützung der Kerberos-Verschlüsselung für NFS-Volumes vorbereitet haben. Anweisungen hierzu finden Sie unter ["Aktivieren Sie Kerberos auf einer Daten-LIF"](#) .
- Stellen Sie sicher, dass alle NFSv4-Volumes, die Sie mit Kerberos-Verschlüsselung verwenden, korrekt konfiguriert sind. Weitere Informationen finden Sie im Abschnitt NetApp NFSv4-Domänenkonfiguration (Seite 13) der ["NetApp Leitfaden zu NFSv4-Verbesserungen und Best Practices"](#) .

## ONTAP-Exportrichtlinien hinzufügen oder ändern

Sie müssen bestehenden ONTAP-Exportrichtlinien Regeln hinzufügen oder neue Exportrichtlinien erstellen, die Kerberos-Verschlüsselung für das ONTAP Storage-VM-Root-Volume sowie alle mit dem Upstream-Kubernetes-Cluster gemeinsam genutzten ONTAP-Volumes unterstützen. Die von Ihnen hinzugefügten Regeln für die Exportrichtlinie oder neu erstellte Richtlinien für den Export müssen die folgenden Zugriffsprotokolle und Zugriffsberechtigungen unterstützen:

### Zugriffsprotokolle

Konfigurieren Sie die Exportrichtlinie mit NFS-, NFSv3- und NFSv4-Zugriffsprotokollen.

### Zugriffsdetails

Sie können eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung konfigurieren, je nach Ihren Anforderungen für das Volume:

- **Kerberos 5** - (Authentifizierung und Verschlüsselung)
- **Kerberos 5i** - (Authentifizierung und Verschlüsselung mit Identitätsschutz)
- **Kerberos 5p** - (Authentifizierung und Verschlüsselung mit Identitäts- und Datenschutz)

Konfigurieren Sie die ONTAP-Exportrichtlinie mit den entsprechenden Zugriffsberechtigungen. Wenn beispielsweise Cluster die NFS-Volumes mit einer Mischung aus Kerberos 5i- und Kerberos 5p-Verschlüsselung mounten, verwenden Sie die folgenden Zugriffseinstellungen:

| Typ         | Schreibgeschützter Zugriff | Lese-/Schreibzugriff | Superuser-Zugriff |
|-------------|----------------------------|----------------------|-------------------|
| UNIX        | Aktiviert                  | Aktiviert            | Aktiviert         |
| Kerberos 5i | Aktiviert                  | Aktiviert            | Aktiviert         |
| Kerberos 5p | Aktiviert                  | Aktiviert            | Aktiviert         |

Informationen zum Erstellen von ONTAP Exportrichtlinien und Exportrichtlinienregeln finden Sie in der folgenden Dokumentation:

- "[Erstellen Sie eine Exportrichtlinie](#)"
- "[Fügen Sie eine Regel zu einer Exportrichtlinie hinzu](#)"

### Erstellen eines Storage-Backends

Sie können eine Trident-Storage-Back-End-Konfiguration mit Kerberos Verschlüsselungsfunktion erstellen.

### Über diese Aufgabe

Wenn Sie eine Speicher-Back-End-Konfigurationsdatei erstellen, die die Kerberos-Verschlüsselung konfiguriert, können Sie eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung mithilfe des Parameters angeben `spec.nfsMountOptions`:

- `spec.nfsMountOptions: sec=krb5` (Authentifizierung und Verschlüsselung)
- `spec.nfsMountOptions: sec=krb5i` (Authentifizierung und Verschlüsselung mit Identitätsschutz)
- `spec.nfsMountOptions: sec=krb5p` (Authentifizierung und Verschlüsselung mit Identitäts- und Datenschutz)

Geben Sie nur eine Kerberos-Ebene an. Wenn Sie in der Parameterliste mehr als eine Kerberos-Verschlüsselungsebene angeben, wird nur die erste Option verwendet.

### Schritte

1. Erstellen Sie auf dem verwalteten Cluster mithilfe des folgenden Beispiels eine Speicher-Back-End-Konfigurationsdatei. Ersetzen Sie Werte in Klammern `<>` durch Informationen aus Ihrer Umgebung:

```

apiVersion: v1
kind: Secret
metadata:
  name: backend-ontap-nas-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-ontap-nas
spec:
  version: 1
  storageDriverName: "ontap-nas"
  managementLIF: <STORAGE_VM_MGMT_LIF_IP_ADDRESS>
  dataLIF: <PROTOCOL_LIF_FQDN_OR_IP_ADDRESS>
  svm: <STORAGE_VM_NAME>
  username: <STORAGE_VM_USERNAME_CREDENTIAL>
  password: <STORAGE_VM_PASSWORD_CREDENTIAL>
  nasType: nfs
  nfsMountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
  qtreesPerFlexvol:
  credentials:
    name: backend-ontap-nas-secret

```

2. Verwenden Sie die Konfigurationsdatei, die Sie im vorherigen Schritt erstellt haben, um das Backend zu erstellen:

```
tridentctl create backend -f <backend-configuration-file>
```

Wenn die Backend-Erstellung fehlschlägt, ist mit der Back-End-Konfiguration ein Fehler aufgetreten. Sie können die Protokolle zur Bestimmung der Ursache anzeigen, indem Sie den folgenden Befehl ausführen:

```
tridentctl logs
```

Nachdem Sie das Problem mit der Konfigurationsdatei identifiziert und korrigiert haben, können Sie den Befehl „Erstellen“ erneut ausführen.

#### **Erstellen Sie eine Speicherklasse**

Sie können eine Storage-Klasse für die Bereitstellung von Volumes mit Kerberos-Verschlüsselung erstellen.

## Über diese Aufgabe

Wenn Sie ein Storage-Klasse-Objekt erstellen, können Sie mit dem Parameter eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung angeben `mountOptions`:

- `mountOptions: sec=krb5` (Authentifizierung und Verschlüsselung)
- `mountOptions: sec=krb5i` (Authentifizierung und Verschlüsselung mit Identitätsschutz)
- `mountOptions: sec=krb5p` (Authentifizierung und Verschlüsselung mit Identitäts- und Datenschutz)

Geben Sie nur eine Kerberos-Ebene an. Wenn Sie in der Parameterliste mehr als eine Kerberos-Verschlüsselungsebene angeben, wird nur die erste Option verwendet. Wenn die in der Storage-Backend-Konfiguration angegebene Verschlüsselungsebene von der Ebene abweicht, die Sie im Storage-Klasse-Objekt angeben, hat das Storage-Klasse-Objekt Vorrang.

## Schritte

1. Erstellen Sie mithilfe des folgenden Beispiels ein StorageClass-Kubernetes-Objekt:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas-sc
provisioner: csi.trident.netapp.io
mountOptions:
  - sec=krb5i #can be krb5, krb5i, or krb5p
parameters:
  backendType: ontap-nas
  storagePools: ontapnas_pool
  trident.netapp.io/nasType: nfs
  allowVolumeExpansion: true
```

2. Speicherklasse erstellen:

```
kubectl create -f sample-input/storage-class-ontap-nas-sc.yaml
```

3. Stellen Sie sicher, dass die Storage-Klasse erstellt wurde:

```
kubectl get sc ontap-nas-sc
```

Sie sollten eine Ausgabe wie die folgende sehen:

| NAME         | PROVISIONER           | AGE |
|--------------|-----------------------|-----|
| ontap-nas-sc | csi.trident.netapp.io | 15h |

## Bereitstellen von Volumes

Nachdem Sie ein Storage-Back-End und eine Storage-Klasse erstellt haben, können Sie nun ein Volume bereitstellen. Anweisungen hierzu finden Sie unter "[Bereitstellen eines Volumes](#)".

## Konfiguration der Verschlüsselung von Kerberos während der Übertragung mit Azure NetApp Files Volumes

Sie können die Kerberos-Verschlüsselung für den Storage-Datenverkehr zwischen dem gemanagten Cluster und einem einzelnen Azure NetApp Files Storage-Back-End oder einem virtuellen Pool von Azure NetApp Files Storage-Back-Ends aktivieren.

### Bevor Sie beginnen

- Stellen Sie sicher, dass Sie Trident auf dem verwalteten Red hat OpenShift-Cluster aktiviert haben.
- Stellen Sie sicher, dass Sie Zugriff auf das Dienstprogramm haben `tridentctl`.
- Stellen Sie sicher, dass Sie das Azure NetApp Files-Speicher-Back-End für die Kerberos-Verschlüsselung vorbereitet haben, indem Sie die Anforderungen beachten und die Anweisungen in befolgen "[Azure NetApp Files-Dokumentation](#)".
- Stellen Sie sicher, dass alle NFSv4-Volumes, die Sie mit Kerberos-Verschlüsselung verwenden, korrekt konfiguriert sind. Weitere Informationen finden Sie im Abschnitt NetApp NFSv4-Domänenkonfiguration (Seite 13) der "[NetApp Leitfaden zu NFSv4-Verbesserungen und Best Practices](#)".

### Erstellen eines Storage-Backends

Sie können eine Azure NetApp Files-Storage-Back-End-Konfiguration mit Kerberos Verschlüsselungsfunktionen erstellen.

### Über diese Aufgabe

Wenn Sie eine Speicher-Backend-Konfigurationsdatei erstellen, die die Kerberos-Verschlüsselung konfiguriert, können Sie sie so definieren, dass sie auf einer der zwei möglichen Ebenen angewendet werden sollte:

- Die **Speicher-Backend-Ebene** mit dem `spec.kerberos` Feld
- Die **virtuelle Pool-Ebene** mit dem `spec.storage.kerberos` Feld

Wenn Sie die Konfiguration auf der Ebene des virtuellen Pools definieren, wird der Pool mithilfe der Beschriftung in der Speicherklasse ausgewählt.

Auf beiden Ebenen können Sie eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung angeben:

- `kerberos: sec=krb5` (Authentifizierung und Verschlüsselung)
- `kerberos: sec=krb5i` (Authentifizierung und Verschlüsselung mit Identitätsschutz)
- `kerberos: sec=krb5p` (Authentifizierung und Verschlüsselung mit Identitäts- und Datenschutz)

### Schritte

1. Erstellen Sie auf dem verwalteten Cluster eine Speicher-Backend-Konfigurationsdatei mit einem der folgenden Beispiele, je nachdem, wo Sie das Speicher-Back-End definieren müssen (Speicher-Back-End-Ebene oder virtuelle Pool-Ebene). Ersetzen Sie Werte in Klammern <> durch Informationen aus Ihrer Umgebung:

### Beispiel auf Storage-Back-End-Ebene

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>

---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-secret
```

### Beispiel auf Ebene des virtuellen Pools

```

---
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>

---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  storage:
    - labels:
        type: encryption
        kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-secret

```

2. Verwenden Sie die Konfigurationsdatei, die Sie im vorherigen Schritt erstellt haben, um das Backend zu erstellen:

```
tridentctl create backend -f <backend-configuration-file>
```

Wenn die Backend-Erstellung fehlschlägt, ist mit der Back-End-Konfiguration ein Fehler aufgetreten. Sie können die Protokolle zur Bestimmung der Ursache anzeigen, indem Sie den folgenden Befehl ausführen:

```
tridentctl logs
```

Nachdem Sie das Problem mit der Konfigurationsdatei identifiziert und korrigiert haben, können Sie den Befehl „Erstellen“ erneut ausführen.

#### Erstellen Sie eine Speicherklasse

Sie können eine Storage-Klasse für die Bereitstellung von Volumes mit Kerberos-Verschlüsselung erstellen.

#### Schritte

1. Erstellen Sie mithilfe des folgenden Beispiels ein StorageClass-Kubernetes-Objekt:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: sc-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: azure-netapp-files
  trident.netapp.io/nasType: nfs
  selector: type=encryption
```

2. Speicherklasse erstellen:

```
kubectl create -f sample-input/storage-class-sc-nfs.yaml
```

3. Stellen Sie sicher, dass die Storage-Klasse erstellt wurde:

```
kubectl get sc -sc-nfs
```

Sie sollten eine Ausgabe wie die folgende sehen:

| NAME   | PROVISIONER           | AGE |
|--------|-----------------------|-----|
| sc-nfs | csi.trident.netapp.io | 15h |

#### Bereitstellen von Volumes

Nachdem Sie ein Storage-Back-End und eine Storage-Klasse erstellt haben, können Sie nun ein Volume bereitstellen. Anweisungen hierzu finden Sie unter ["Bereitstellen eines Volumes"](#).

## 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 VERTRÄGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER 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.