



Konzepte

Trident

NetApp
July 01, 2026

Inhalt

- Konzepte 1
 - Bereitstellung 1
 - Speicherklassenzuordnung 1
 - Volumenerstellung 1
 - Volume Snapshots 1
 - Erfahren Sie mehr über die Erstellung von Volume-Snapshots 1
 - Virtuelle Pools 2
 - Erfahren Sie mehr über virtuelle Pools 2
- Volumenzugriffsgruppen 4
 - Erfahren Sie mehr über Volumenzugriffsgruppen 4

Konzepte

Bereitstellung

Die Bereitstellung in Trident hat zwei Hauptphasen. Die erste Phase ordnet eine Speicherklasse dem Satz geeigneter Backend-Speicherpools zu und erfolgt als notwendige Vorbereitung vor der Bereitstellung. Die zweite Phase umfasst die eigentliche Volume-Erstellung und erfordert die Auswahl eines Speicherpools aus denen, die der Speicherklasse des ausstehenden Volumes zugeordnet sind.

Speicherklassenzuordnung

Die Zuordnung von Backend-Speicherpools zu einer Speicherklasse basiert sowohl auf den angeforderten Attributen der Speicherklasse als auch auf deren `storagePools`, `additionalStoragePools` und `excludeStoragePools` Listen. Wenn Sie eine Speicherklasse erstellen, vergleicht Trident die von jedem seiner Backends angebotenen Attribute und Pools mit denen, die von der Speicherklasse angefordert werden. Wenn die Attribute und der Name eines Speicherpools mit allen angeforderten Attributen und Poolnamen übereinstimmen, fügt Trident diesen Speicherpool der Menge geeigneter Speicherpools für diese Speicherklasse hinzu. Zusätzlich fügt Trident alle in der `additionalStoragePools` Liste aufgeführten Speicherpools dieser Menge hinzu, selbst wenn deren Attribute nicht alle oder keine der angeforderten Attribute der Speicherklasse erfüllen. Sie sollten die `excludeStoragePools` Liste verwenden, um Speicherpools für eine Speicherklasse außer Kraft zu setzen und aus der Nutzung zu entfernen. Trident führt einen ähnlichen Prozess jedes Mal durch, wenn Sie ein neues Backend hinzufügen, prüft, ob dessen Speicherpools die Anforderungen der bestehenden Speicherklassen erfüllen, und entfernt alle, die als ausgeschlossen markiert wurden.

Volumenerstellung

Trident verwendet dann die Zuordnungen zwischen Speicherklassen und Speicherpools, um zu bestimmen, wo Volumes bereitgestellt werden. Wenn Sie ein Volume erstellen, ermittelt Trident zunächst die Speicherpools für die Speicherklasse dieses Volumes, und wenn Sie ein Protokoll für das Volume angeben, entfernt Trident diejenigen Speicherpools, die das angeforderte Protokoll nicht bereitstellen können (zum Beispiel kann ein NetApp HCI/SolidFire Backend kein dateibasiertes Volume bereitstellen, während ein ONTAP NAS Backend kein blockbasiertes Volume bereitstellen kann). Trident randomisiert die Reihenfolge dieser resultierenden Menge, um eine gleichmäßige Verteilung der Volumes zu ermöglichen, und iteriert dann durch sie, wobei versucht wird, das Volume nacheinander auf jedem Speicherpool bereitzustellen. Wenn dies bei einem gelingt, wird erfolgreich zurückgegeben und alle während des Prozesses aufgetretenen Fehler werden protokolliert. Trident gibt nur dann einen Fehler zurück, **wenn** die Bereitstellung auf **allen** für die angeforderte Speicherklasse und das Protokoll verfügbaren Speicherpools fehlschlägt.

Volume Snapshots

Erfahren Sie mehr darüber, wie Trident die Erstellung von Volume-Snapshots für seine Treiber handhabt.

Erfahren Sie mehr über die Erstellung von Volume-Snapshots

- Für die `ontap-nas`, `ontap-san` und `azure-netapp-files` Treiber wird jedes Persistent Volume (PV) einem FlexVol volume zugeordnet. Dadurch werden Volume-Snapshots als NetApp Snapshots erstellt. Die NetApp Snapshot-Technologie bietet mehr Stabilität, Skalierbarkeit, Wiederherstellbarkeit und Leistung als

konkurrierende Snapshot-Technologien. Diese Snapshot-Kopien sind äußerst effizient, sowohl in Bezug auf die benötigte Zeit für ihre Erstellung als auch auf den Speicherplatz.

- Für den `ontap-nas-flexgroup`-Treiber wird jedes Persistent Volume (PV) einem FlexGroup zugeordnet. Dadurch werden Volume-Snapshots als NetApp FlexGroup-Snapshots erstellt. Die NetApp Snapshot-Technologie bietet mehr Stabilität, Skalierbarkeit, Wiederherstellbarkeit und Leistung als konkurrierende Snapshot-Technologien. Diese Snapshot-Kopien sind äußerst effizient, sowohl in Bezug auf die benötigte Zeit für ihre Erstellung als auch auf den Speicherplatz.
- Für den `ontap-san-economy` Treiber werden PVs auf LUNs abgebildet, die auf gemeinsam genutzten FlexVol Volumes erstellt wurden. VolumeSnapshots von PVs werden erreicht, indem FlexClones der zugehörigen LUN durchgeführt werden. ONTAP FlexClone Technologie ermöglicht es, Kopien selbst der größten Datensätze nahezu augenblicklich zu erstellen. Kopien teilen sich Datenblöcke mit ihren übergeordneten Elementen und belegen keinen Speicherplatz außer dem, der für Metadaten benötigt wird.
- Für den `solidfire-san` Treiber wird jedes PV einer LUN zugeordnet, die auf der NetApp Element Software/NetApp HCI-Cluster erstellt wurde. VolumeSnapshots werden durch Element-Snapshots der zugrunde liegenden LUN repräsentiert. Diese Snapshots sind zeitpunktgenaue Kopien und beanspruchen nur wenig Systemressourcen und Speicherplatz.
- Bei der Arbeit mit dem `ontap-nas` und `ontap-san` Treiber sind ONTAP-Snapshots zeitpunktgenaue Kopien des FlexVol und belegen Speicherplatz auf dem FlexVol selbst. Dies kann dazu führen, dass der beschreibbare Speicherplatz im Volume mit der Zeit abnimmt, wenn Snapshots erstellt oder geplant werden. Eine einfache Möglichkeit, dies zu beheben, besteht darin, das Volume durch Resize über Kubernetes zu vergrößern. Eine weitere Option ist das Löschen von Snapshots, die nicht mehr benötigt werden. Wenn ein durch Kubernetes erstellter VolumeSnapshot gelöscht wird, löscht Trident den zugehörigen ONTAP-Snapshot. ONTAP-Snapshots, die nicht durch Kubernetes erstellt wurden, können ebenfalls gelöscht werden.

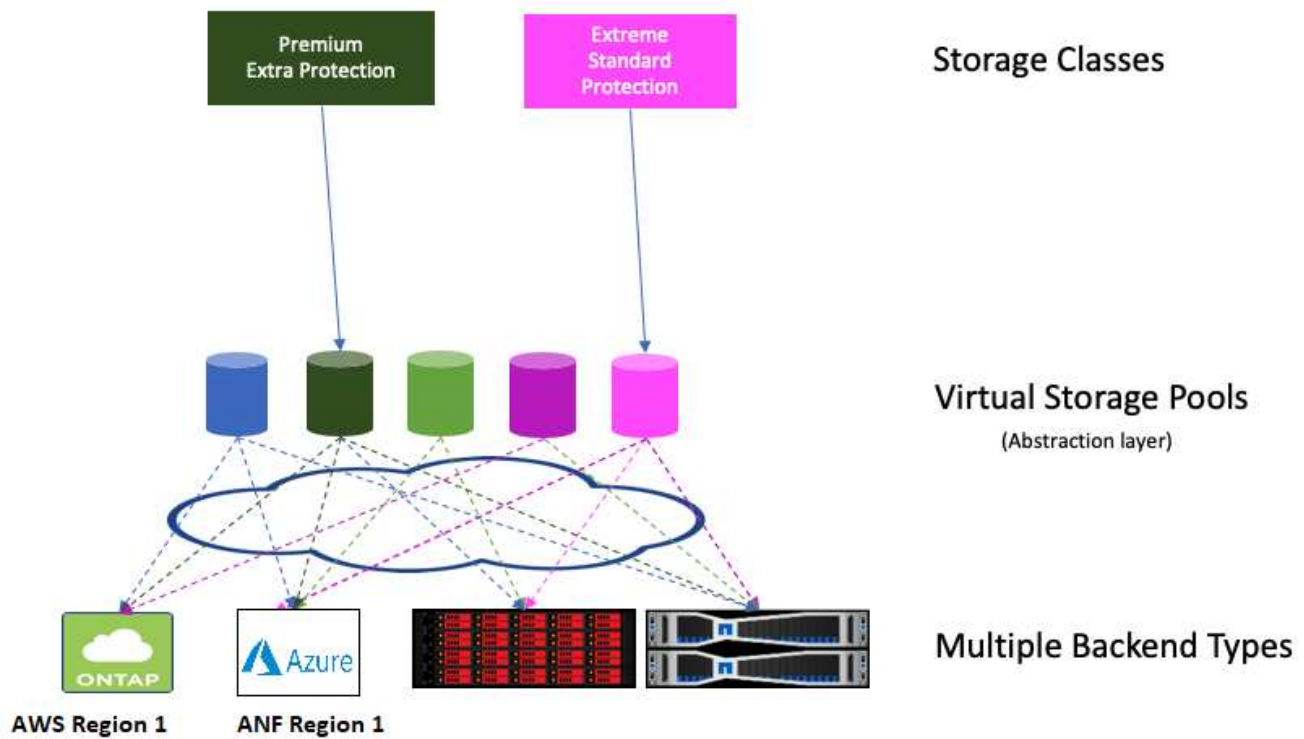
Mit Trident können Sie VolumeSnapshots verwenden, um neue PVs daraus zu erstellen. Das Erstellen von PVs aus diesen Snapshots erfolgt mithilfe der FlexClone-Technologie für unterstützte ONTAP-Backends. Beim Erstellen eines PVs aus einem Snapshot ist das zugrunde liegende Volume ein FlexClone des übergeordneten Volumes des Snapshots. Der `solidfire-san` Treiber verwendet Element-Software-Volume-Klone, um PVs aus Snapshots zu erstellen. Hier wird ein Klon des Element-Snapshots erstellt.

Virtuelle Pools

Virtuelle Pools bieten eine Abstraktionsschicht zwischen Trident-Speicher-Backends und Kubernetes `StorageClasses`. Sie ermöglichen es einem Administrator, Aspekte wie Standort, Leistung und Schutz für jedes Backend auf eine einheitliche, backendunabhängige Weise zu definieren, ohne eine `StorageClass` angeben zu müssen, welches physische Backend, welcher Backend-Pool oder welcher Backend-Typ verwendet werden soll, um die gewünschten Kriterien zu erfüllen.

Erfahren Sie mehr über virtuelle Pools

Der Speicheradministrator kann virtuelle Pools auf jedem der Trident Backends in einer JSON- oder YAML-Definitionsdatei definieren.



Alle Aspekte, die außerhalb der Liste der virtuellen Pools angegeben werden, sind global für das Backend und gelten für alle virtuellen Pools, während jeder virtuelle Pool einen oder mehrere Aspekte individuell angeben kann (wodurch globale Aspekte des Backends überschrieben werden).



- Beim Definieren virtueller Pools sollten Sie nicht versuchen, die Reihenfolge vorhandener virtueller Pools in einer Backend-Definition zu ändern.
- Wir raten davon ab, Attribute eines bestehenden virtuellen Pools zu ändern. Sie sollten einen neuen virtuellen Pool definieren, um Änderungen vorzunehmen.

Die meisten Aspekte werden in Backend-spezifischen Begriffen spezifiziert. Entscheidend ist, dass die Aspektwerte nicht außerhalb des Backend-Treibers zugänglich sind und nicht für den Abgleich in `StorageClasses` verfügbar sind. Stattdessen definiert der Administrator für jeden virtuellen Pool ein oder mehrere Labels. Jedes Label ist ein Schlüssel:Wert-Paar, und Labels können für verschiedene Backends identisch sein. Wie Aspekte können auch Labels pro Pool oder global für das Backend definiert werden. Im Gegensatz zu Aspekten, die vordefinierte Namen und Werte haben, kann der Administrator die Label-Schlüssel und -Werte nach Bedarf frei festlegen. Zur Vereinfachung können Speicheradministratoren Bezeichnungen pro virtuellem Pool definieren und Volumes nach Bezeichnung gruppieren.

Die virtuellen Poolbezeichnungen können mit diesen Zeichen definiert werden:

- Großbuchstaben A-Z
- Kleinbuchstaben a-z
- Zahlen 0-9
- Unterstriche _
- Bindestriche -

A `StorageClass` identifiziert den zu verwendenden virtuellen Pool durch Verweis auf die Bezeichnungen innerhalb eines Selektorparameters. Selektoren für virtuelle Pools unterstützen die folgenden Operatoren:

Operator	Beispiel	Der Labelwert eines Pools muss:
=	performance=premium	Übereinstimmen
!=	performance!=extreme	Keine Übereinstimmung
in	Standort in (east, west)	Teil der Wertemenge sein
notin	performance notin (Silber, Bronze)	Nicht in der Wertemenge enthalten sein
<key>	Schutz	Existiert mit beliebigem Wert
!<key>	!Schutz	Nicht vorhanden

Volumenzugriffsgruppen

Erfahren Sie mehr darüber, wie Trident "[Volumenzugriffsgruppen](#)" verwendet.



Ignorieren Sie diesen Abschnitt, wenn Sie CHAP verwenden, was empfohlen wird, um die Verwaltung zu vereinfachen und die unten beschriebene Skalierungsbeschränkung zu vermeiden. Wenn Sie Trident im CSI-Modus verwenden, können Sie diesen Abschnitt ebenfalls ignorieren. Trident verwendet CHAP, wenn es als erweiterter CSI-Provisioner installiert ist.

Erfahren Sie mehr über Volumenzugriffsgruppen

Trident kann Volume-Zugriffsgruppen verwenden, um den Zugriff auf die Volumes zu steuern, die es bereitstellt. Wenn CHAP deaktiviert ist, erwartet es, eine Zugriffsgruppe namens `trident` zu finden, es sei denn, Sie geben eine oder mehrere Zugriffsgruppen-IDs in der Konfiguration an.

Trident ordnet zwar neue Volumes den konfigurierten Zugriffsgruppen zu, erstellt oder verwaltet die Zugriffsgruppen jedoch nicht selbst. Die Zugriffsgruppen müssen existieren, bevor das Speicher-Backend zu Trident hinzugefügt wird, und sie müssen die iSCSI-IQNs von jedem Knoten im Kubernetes-Cluster enthalten, der potenziell die von diesem Backend bereitgestellten Volumes einbinden könnte. In den meisten Installationen umfasst dies alle Worker-Knoten im Cluster.

Für Kubernetes-Cluster mit mehr als 64 Knoten sollten Sie mehrere Zugriffsgruppen verwenden. Jede Zugriffsgruppe kann bis zu 64 IQNs enthalten, und jedes Volume kann zu vier Zugriffsgruppen gehören. Mit den maximal vier konfigurierten Zugriffsgruppen kann jeder Knoten in einem Cluster mit bis zu 256 Knoten auf jedes Volume zugreifen. Die aktuellen Beschränkungen für Volume-Zugriffsgruppen finden Sie unter "[hier](#)".

Wenn Sie die Konfiguration von einer, die die Standard `trident` Zugriffsgruppe verwendet, auf eine, die auch andere verwendet, ändern, fügen Sie die ID der `trident` Zugriffsgruppe in die Liste ein.

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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