Bewährte Verfahren und Empfehlungen

Trident

NetApp
March 05, 2026

Inhalt

Bewährte Verfahren und Empfehlungen

Einsatz

Beachten Sie bei der Bereitstellung von Trident die hier aufgeführten Empfehlungen.

In einem dedizierten Namensraum bereitstellen

"Namensräume"Sie sorgen für eine administrative Trennung zwischen verschiedenen Anwendungen und stellen ein Hindernis für die gemeinsame Nutzung von Ressourcen dar. Beispielsweise kann ein PVC aus einem Namespace nicht aus einem anderen Namespace verwendet werden. Trident stellt PV-Ressourcen für alle Namespaces im Kubernetes-Cluster bereit und nutzt daher ein Servicekonto mit erhöhten Berechtigungen.

Darüber hinaus könnte der Zugriff auf den Trident Pod einem Benutzer den Zugriff auf Anmeldeinformationen des Speichersystems und andere sensible Informationen ermöglichen. Es ist wichtig sicherzustellen, dass Anwendungsbenutzer und Verwaltungsanwendungen keinen Zugriff auf die Trident -Objektdefinitionen oder die Pods selbst haben.

Nutzen Sie Quoten und Bereichsgrenzen, um den Speicherverbrauch zu kontrollieren.

Kubernetes verfügt über zwei Funktionen, die in Kombination einen leistungsstarken Mechanismus zur Begrenzung des Ressourcenverbrauchs von Anwendungen bieten. Der "Speicherquotenmechanismus" Ermöglicht dem Administrator die Implementierung globaler und speicherklassenspezifischer Kapazitäts- und Objektanzahlbeschränkungen pro Namespace. Des Weiteren, unter Verwendung eines "Reichweitenbegrenzung" stellt sicher, dass die PVC-Anfragen sowohl einen minimalen als auch einen maximalen Wert nicht überschreiten, bevor die Anfrage an den Provisionierer weitergeleitet wird.

Diese Werte werden pro Namespace definiert, was bedeutet, dass für jeden Namespace Werte definiert sein sollten, die seinen Ressourcenanforderungen entsprechen. Hier finden Sie weitere Informationen zu "wie man Quoten optimal nutzt" .

Storage-Konfiguration

Jede Speicherplattform im NetApp Portfolio verfügt über einzigartige Funktionen, die Anwendungen zugutekommen, unabhängig davon, ob sie containerisiert sind oder nicht.

Plattformübersicht

Trident ist mit ONTAP und Element kompatibel. Es gibt keine Plattform, die für alle Anwendungen und Szenarien besser geeignet ist als eine andere. Bei der Auswahl einer Plattform sollten jedoch die Bedürfnisse der Anwendung und des Teams, das das Gerät verwaltet, berücksichtigt werden.

Sie sollten die grundlegenden Best Practices für das Host-Betriebssystem mit dem von Ihnen verwendeten Protokoll befolgen. Optional können Sie, sofern verfügbar, die Best Practices der Anwendung in die Backend-, Speicherklassen- und PVC-Einstellungen einbeziehen, um den Speicher für bestimmte Anwendungen zu optimieren.

ONTAP und Cloud Volumes ONTAP Best Practices

Lernen Sie die besten Vorgehensweisen für die Konfiguration von ONTAP und Cloud Volumes ONTAP für Trident kennen.

Die folgenden Empfehlungen sind Richtlinien für die Konfiguration von ONTAP für containerisierte Workloads, die Volumes nutzen, die von Trident dynamisch bereitgestellt werden. Jede dieser Optionen sollte auf ihre Eignung für Ihr Umfeld hin geprüft und bewertet werden.

Verwenden Sie SVMs, die speziell für Trident vorgesehen sind.

Storage Virtual Machines (SVMs) bieten Isolation und administrative Trennung zwischen Mandanten auf einem ONTAP System. Die Zuweisung einer SVM zu Anwendungen ermöglicht die Delegation von Berechtigungen und die Anwendung bewährter Verfahren zur Begrenzung des Ressourcenverbrauchs.

Für die Verwaltung der SVM stehen mehrere Optionen zur Verfügung:

- Stellen Sie in der Backend-Konfiguration die Cluster-Management-Schnittstelle zusammen mit den entsprechenden Anmeldeinformationen bereit und geben Sie den SVM-Namen an.
- Erstellen Sie eine dedizierte Verwaltungsschnittstelle für die SVM mithilfe des ONTAP System Manager oder der CLI.
- Teilen Sie die Verwaltungsrolle mit einer NFS-Datenschnittstelle.

In jedem Fall sollte die Schnittstelle im DNS hinterlegt sein, und der DNS-Name sollte bei der Konfiguration von Trident verwendet werden. Dies erleichtert bestimmte DR-Szenarien, beispielsweise SVM-DR ohne Verwendung der Netzwerkidentitätsbeibehaltung.

Es gibt keine Präferenz zwischen einem dedizierten oder einem gemeinsam genutzten Management-LIF für die SVM. Sie sollten jedoch sicherstellen, dass Ihre Netzwerksicherheitsrichtlinien mit dem von Ihnen gewählten Ansatz übereinstimmen. Ungeachtet dessen sollte die Management-LIF über DNS zugänglich sein, um maximale Flexibilität zu gewährleisten. "SVM-DR" wird in Verbindung mit Trident verwendet.

Begrenzen Sie die maximale Anzahl

ONTAP Speichersysteme haben eine maximale Anzahl an Volumes, die je nach Softwareversion und Hardwareplattform variiert. Siehe "NetApp Hardware Universe" Die genauen Grenzwerte hängen von Ihrer spezifischen Plattform und ONTAP Version ab. Wenn die maximale Speicherkapazität erreicht ist, schlagen Bereitstellungsvorgänge nicht nur für Trident, sondern für alle Speicheranforderungen fehl.

Tridents `ontap-nas` Und `ontap-san` Treiber stellen für jedes erstellte Kubernetes Persistent Volume (PV) ein FlexVolume bereit. Der `ontap-nas-economy` Der Treiber erzeugt ungefähr ein FlexVolume pro 200 PVs (konfigurierbar zwischen 50 und 300). Der `ontap-san-economy` Der Treiber erzeugt ungefähr ein FlexVolume pro 100 PVs (konfigurierbar zwischen 50 und 200). Um zu verhindern, dass Trident alle verfügbaren Volumes auf dem Speichersystem verbraucht, sollten Sie ein Limit für die SVM festlegen. Sie können dies über die Befehlszeile tun:

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

Der Wert für `max-volumes` variiert je nach verschiedenen Kriterien, die für Ihre Umgebung spezifisch sind:

- Die Anzahl der vorhandenen Volumes im ONTAP Cluster

- Die Anzahl der Volumes, die Sie voraussichtlich außerhalb von Trident für andere Anwendungen bereitstellen werden.
- Die Anzahl der persistenten Volumes, die voraussichtlich von Kubernetes-Anwendungen belegt werden.

Der `max-volumes` Der Wert bezieht sich auf die Gesamtmenge der auf allen Knoten im ONTAP Cluster bereitgestellten Daten und nicht auf einen einzelnen ONTAP Knoten. Infolgedessen können Bedingungen auftreten, bei denen ein ONTAP Clusterknoten über weitaus mehr oder weniger von Trident bereitgestellte Volumes verfügt als ein anderer Knoten.

Ein ONTAP -Cluster mit zwei Knoten kann beispielsweise maximal 2000 FlexVol Volumes hosten. Die Festlegung der maximalen Lautstärkeanzahl auf 1250 erscheint sehr sinnvoll. Wenn jedoch nur "Aggregate" Wenn von einem Knoten Daten dem SVM zugewiesen werden oder die von einem Knoten zugewiesenen Aggregate nicht bereitgestellt werden können (z. B. aufgrund von Kapazitätsengpässen), wird der andere Knoten zum Ziel für alle von Trident bereitgestellten Volumes. Dies bedeutet, dass die Volumenbegrenzung für diesen Knoten möglicherweise erreicht wird, bevor `max-volumes` Dieser Wert wird erreicht, was sich sowohl auf Trident als auch auf andere Volumenoperationen auswirkt, die diesen Knoten verwenden. **Diese Situation lässt sich vermeiden, indem sichergestellt wird, dass die Aggregate von jedem Knoten im Cluster dem von Trident verwendeten SVM in gleicher Anzahl zugewiesen werden.**

Klonen eines Volumes

NetApp Trident unterstützt das Klonen von Volumes bei Verwendung von `ontap-nas` , `ontap-san` , `solidfire-san` , Und `gcp-cvs` Speichertreiber. Bei der Verwendung des `ontap-nas-flexgroup` oder `ontap-nas-economy` Treiber, Klonen wird nicht unterstützt. Wenn aus einem bestehenden Volume ein neues Volume erstellt wird, wird ein neuer Snapshot erstellt.

> Vermeiden Sie das Klonen eines PVC, das einer anderen StorageClass zugeordnet ist. Um Kompatibilität zu gewährleisten und unerwartetes Verhalten zu vermeiden, sollten Klonvorgänge innerhalb derselben StorageClass durchgeführt werden.

Begrenzen Sie die maximale Größe der von Trident erstellten Volumen.

Um die maximale Größe für von Trident erstellbare Volumes zu konfigurieren, verwenden Sie die `limitVolumeSize` Parameter in Ihrem `backend.json` Definition.

Zusätzlich zur Steuerung der Volumegröße im Speicherarray sollten Sie auch die Kubernetes-Funktionen nutzen.

Die maximale Größe von FlexVols, die von Trident erstellt werden, begrenzen.

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

Konfigurieren Sie Trident für die Verwendung von bidirektionalem CHAP.

Sie können die Benutzernamen und Passwörter für CHAP-Initiator und -Ziel in Ihrer Backend-Definition angeben und Trident veranlassen, CHAP auf der SVM zu aktivieren. Verwenden des `useCHAP` Parameter in Ihrer Backend-Konfiguration, Trident authentifiziert iSCSI-Verbindungen für ONTAP -Backends mit CHAP.

Erstellen und Verwenden einer SVM-QoS-Richtlinie

Durch die Nutzung einer ONTAP QoS-Richtlinie, die auf die SVM angewendet wird, wird die Anzahl der von den bereitgestellten Trident -Volumes verbrauchbaren IOPS begrenzt. Dies hilft dabei "Mobbing verhindern" oder dass ein außer Kontrolle geratener Container Arbeitslasten außerhalb der Trident SVM beeinträchtigt.

Sie können in wenigen Schritten eine QoS-Richtlinie für die SVM erstellen. Die genauesten Informationen finden Sie in der Dokumentation zu Ihrer ONTAP -Version. Das folgende Beispiel erstellt eine QoS-Richtlinie, die die insgesamt für die 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>
```

Zusätzlich können Sie, sofern Ihre ONTAP -Version dies unterstützt, die Verwendung eines QoS-Minimums in Betracht ziehen, um einen gewissen Durchsatz für containerisierte Workloads zu garantieren. Adaptives QoS ist nicht mit einer SVM-Richtlinie kompatibel.

Die Anzahl der für die containerisierten Workloads reservierten IOPS hängt von vielen Aspekten ab. Dazu gehören unter anderem:

- Andere Arbeitslasten, die das Speichersystem nutzen. Falls andere Arbeitslasten, die nicht mit der Kubernetes-Bereitstellung zusammenhängen, die Speicherressourcen nutzen, ist darauf zu achten, dass diese Arbeitslasten nicht versehentlich beeinträchtigt werden.
- Erwartete Workloads, die in Containern ausgeführt werden. Wenn Workloads mit hohen IOPS-Anforderungen in Containern ausgeführt werden, führt eine niedrige QoS-Richtlinie zu einer schlechten Benutzererfahrung.

Wichtig ist zu beachten, dass eine auf SVM-Ebene zugewiesene QoS-Richtlinie dazu führt, dass alle der SVM bereitgestellten Volumes denselben IOPS-Pool nutzen. Wenn eine oder wenige der containerisierten Anwendungen einen hohen IOPS-Bedarf haben, könnte dies zu einer Belastung für die anderen containerisierten Workloads führen. In diesem Fall sollten Sie erwägen, externe Automatisierung zur Zuweisung von QoS-Richtlinien pro Volume zu verwenden.

Sie sollten die QoS-Richtliniengruppe der SVM **nur** dann zuweisen, wenn Ihre ONTAP Version älter als 9.8 ist.

Erstellen Sie QoS-Richtliniengruppen für Trident.

Die Dienstgüte (QoS) gewährleistet, dass die Leistung kritischer Arbeitslasten nicht durch konkurrierende Arbeitslasten beeinträchtigt wird. ONTAP QoS-Richtliniengruppen bieten QoS-Optionen für Volumes und ermöglichen es Benutzern, die Durchsatzobergrenze für eine oder mehrere Workloads zu definieren. Weitere Informationen zu QoS finden Sie unter "Gewährleistung des Durchsatzes mit QoS" . Sie können QoS-Richtliniengruppen im Backend oder in einem Speicherpool festlegen, und diese werden auf jedes in diesem Pool oder Backend erstellte Volume angewendet.

ONTAP kennt zwei Arten von QoS-Richtliniengruppen: traditionelle und adaptive. Traditionelle

Richtliniengruppen bieten einen festen maximalen (bzw. minimalen, in späteren Versionen) Durchsatz in IOPS. Adaptive QoS skaliert den Durchsatz automatisch an die Workload-Größe und hält dabei das Verhältnis von IOPS zu TBs|GBs aufrecht, während sich die Größe der Workload ändert. Dies bietet einen erheblichen Vorteil, wenn Sie Hunderte oder Tausende von Workloads in einer großen Bereitstellung verwalten.

Beachten Sie Folgendes beim Erstellen von QoS-Richtliniengruppen:

- Du solltest die `qosPolicy` Schlüssel im `defaults` Block der Backend-Konfiguration. Siehe das folgende Beispiel für eine Backend-Konfiguration:

```
---
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, durch die Richtliniengruppe festgelegten Durchsatz erhält. Gemeinsame Richtliniengruppen werden nicht unterstützt.

Weitere Informationen zu QoS-Richtliniengruppen finden Sie unter "ONTAP Befehlsreferenz" .

Beschränken Sie den Zugriff auf Speicherressourcen für Kubernetes-Cluster-Mitglieder.

Die Beschränkung des Zugriffs auf die von Trident erstellten NFS-Volumes, iSCSI-LUNs und FC-LUNs ist ein entscheidender Bestandteil der Sicherheitsarchitektur Ihrer Kubernetes-Bereitstellung. Dadurch wird verhindert, dass Hosts, die nicht Teil des Kubernetes-Clusters sind, auf die Volumes zugreifen und möglicherweise Daten unerwartet ändern.

Es ist wichtig zu verstehen, dass Namespaces die logische Grenze für Ressourcen in Kubernetes sind. Die Annahme ist, dass Ressourcen im selben Namensraum gemeinsam genutzt werden können; wichtig ist jedoch, dass es keine Möglichkeit zur Nutzung über verschiedene Namensräume hinweg gibt. Dies bedeutet, dass PVs zwar globale Objekte sind, aber wenn sie an ein PVC gebunden sind, nur von Pods im selben Namespace zugänglich sind. Es ist von entscheidender Bedeutung, sicherzustellen, dass Namensräume gegebenenfalls zur Trennung verwendet werden.

Die größte Sorge der meisten Organisationen hinsichtlich der Datensicherheit im Kubernetes-Kontext besteht

darin, dass ein Prozess in einem Container auf Speicher zugreifen kann, der auf dem Host eingebunden ist, aber nicht für den Container bestimmt ist. "Namensräume" sind so konzipiert, dass diese Art von Kompromiss verhindert wird. Es gibt jedoch eine Ausnahme: privilegierte Container.

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

Bei Volumes, auf die sowohl von Kubernetes als auch von externen Hosts zugegriffen werden soll, sollte der Speicher auf traditionelle Weise verwaltet werden, wobei das PV vom Administrator eingeführt und nicht von Trident verwaltet wird. Dadurch wird sichergestellt, dass das Speichervolume erst dann zerstört wird, wenn sowohl Kubernetes als auch externe Hosts die Verbindung getrennt haben und das Volume nicht mehr verwenden. Zusätzlich kann eine benutzerdefinierte Exportrichtlinie angewendet werden, die den Zugriff von den Kubernetes-Clusterknoten und von Zielservern außerhalb des Kubernetes-Clusters ermöglicht.

Bei Bereitstellungen mit dedizierten Infrastrukturknoten (z. B. OpenShift) oder anderen Knoten, die keine Benutzeranwendungen einplanen können, sollten separate Exportrichtlinien verwendet werden, um den Zugriff auf Speicherressourcen weiter einzuschränken. Dazu gehört das Erstellen einer Exportrichtlinie für Dienste, die auf diesen Infrastrukturknoten bereitgestellt werden (z. B. die OpenShift-Dienste „Metrics“ und „Logging“), und für Standardanwendungen, die auf Nicht-Infrastrukturknoten bereitgestellt werden.

Nutzen Sie eine spezielle Exportrichtlinie

Sie sollten sicherstellen, dass für jedes Backend eine Exportrichtlinie existiert, die nur den Zugriff auf die im Kubernetes-Cluster vorhandenen Knoten erlaubt. Trident kann Exportrichtlinien automatisch erstellen und verwalten. Auf diese Weise beschränkt Trident den Zugriff auf die Volumes, die es den Knoten im Kubernetes-Cluster bereitstellt, und vereinfacht das Hinzufügen/Löschen von Knoten.

Alternativ können Sie auch manuell eine Exportrichtlinie erstellen und diese mit einer oder mehreren Exportregeln füllen, die jede Knotenzugriffsanfrage verarbeiten:

- Verwenden Sie die `vserver export-policy create` ONTAP CLI-Befehl zum Erstellen der Exportrichtlinie.
- Fügen Sie der Exportrichtlinie Regeln hinzu, indem Sie die `vserver export-policy rule create` ONTAP CLI-Befehl.

Durch Ausführen dieser Befehle können Sie einschränken, welche Kubernetes-Knoten Zugriff auf die Daten haben.

Deaktivieren `showmount` für die Anwendung SVM

Der `showmount` Diese Funktion ermöglicht es einem NFS-Client, die SVM nach einer Liste der verfügbaren NFS-Exporte abzufragen. Ein im Kubernetes-Cluster bereitgestellter Pod kann die folgende Aktion ausführen: `showmount -e` Mit dem Befehl `get` erhalten Sie eine Liste der verfügbaren Mounts, einschließlich derer, auf die es keinen Zugriff hat. Dies stellt zwar für sich genommen keine Sicherheitslücke dar, liefert aber unnötige Informationen, die einem nicht autorisierten Benutzer möglicherweise dabei helfen, eine Verbindung zu einem NFS-Export herzustellen.

Sie sollten deaktivieren `showmount` durch Verwendung des ONTAP CLI-Befehls auf SVM-Ebene:

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

SolidFire – bewährte Verfahren

Lernen Sie die besten Vorgehensweisen für die Konfiguration von SolidFire -Speicher für Trident kennen.

Solidfire-Konto erstellen

Jedes SolidFire -Konto repräsentiert einen eindeutigen Volume-Inhaber und erhält seine eigenen CHAP-Anmeldeinformationen (Challenge-Handshake Authentication Protocol). Sie können auf einem Konto zugewiesene Datenträger entweder über den Kontonamen und die zugehörigen CHAP-Anmeldeinformationen oder über eine Datenträgerzugriffsgruppe zugreifen. Einem Konto können bis zu zweitausend Volumes zugeordnet werden, aber ein Volume kann nur zu einem Konto gehören.

Erstellen Sie eine QoS-Richtlinie

Verwenden Sie SolidFire Quality of Service (QoS)-Richtlinien, wenn Sie eine standardisierte Servicequalitätseinstellung erstellen und speichern möchten, die auf viele Volumes angewendet werden kann.

Sie können QoS-Parameter pro Volume festlegen. Die Leistungsfähigkeit jedes Volumes kann durch die Festlegung von drei konfigurierbaren Parametern, die die QoS definieren, sichergestellt werden: Min IOPS, Max IOPS und Burst IOPS.

Hier sind die möglichen Minimal-, Maximal- und Burst-IOPS-Werte für die 4-Kb-Blockgröße.

IOPS-Parameter	Definition	Minimalwert	Standardwert	Maximalwert (4 KB)
Min IOPS	Das garantierte Leistungsniveau für ein bestimmtes Volumen.	50	50	15000
Maximale IOPS	Die Leistung wird dieses Limit nicht überschreiten.	50	15000	200.000
Burst IOPS	Maximal zulässige IOPS in einem Kurzzeit-Burst-Szenario.	50	15000	200.000

Obwohl die Werte für Max IOPS und Burst IOPS auf bis zu 200.000 eingestellt werden können, ist die tatsächliche maximale Leistung eines Volumes durch die Clusternutzung und die Leistung pro Knoten begrenzt.

Blockgröße und Bandbreite haben einen direkten Einfluss auf die Anzahl der IOPS. Mit zunehmender Blockgröße erhöht das System die Bandbreite auf ein Niveau, das zur Verarbeitung der größeren Blockgrößen erforderlich ist. Mit zunehmender Bandbreite sinkt die Anzahl der IOPS, die das System erreichen kann. Siehe "SolidFire Servicequalität" Für weitere Informationen zu QoS und Leistung.

SolidFire Authentifizierung

Element unterstützt zwei Authentifizierungsmethoden: CHAP und Volume Access Groups (VAG). CHAP verwendet das CHAP-Protokoll zur Authentifizierung des Hosts gegenüber dem Backend. Volume Access

Groups steuert den Zugriff auf die von ihnen bereitgestellten Volumes. NetApp empfiehlt die Verwendung von CHAP zur Authentifizierung, da es einfacher ist und keine Skalierungsbeschränkungen aufweist.

> Trident mit dem erweiterten CSI-Provisioner unterstützt die Verwendung der CHAP-Authentifizierung. VAGs sollten nur im herkömmlichen Nicht-CSI-Betriebsmodus verwendet werden.

Die CHAP-Authentifizierung (Überprüfung, ob der Initiator der beabsichtigte Volumennutzer ist) wird nur bei kontobasierter Zugriffskontrolle unterstützt. Wenn Sie CHAP zur Authentifizierung verwenden, stehen Ihnen zwei Optionen zur Verfügung: unidirektionales CHAP und bidirektionales CHAP. Unidirektionales CHAP authentifiziert den Zugriff auf das Volume mithilfe des SolidFire -Kontonamens und des Initiator-Geheimnisses. Die bidirektionale CHAP-Option bietet die sicherste Methode zur Authentifizierung des Volumes, da das Volume den Host über den Kontonamen und das Initiator-Geheimnis authentifiziert und der Host anschließend das Volume über den Kontonamen und das Ziel-Geheimnis 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 eine kontobasierte Zugriffskontrolle verwendet. Wenn der iSCSI-Initiator nicht für die Verwendung der CHAP-Authentifizierung konfiguriert ist, wird die Zugriffskontrolle über Volume Access Groups (VAG) verwendet.

Wo finde ich weitere Informationen?

Nachfolgend sind einige der Best-Practice-Dokumentationen aufgeführt. Suchen Sie nach "NetApp Bibliothek" für die aktuellsten Versionen.

- ONTAP*
- "NFS-Leitfaden für bewährte Verfahren und Implementierung"
- "SAN-Verwaltung"(für iSCSI)
- "iSCSI Express-Konfiguration für RHEL"

Element Software

- "SolidFire für Linux konfigurieren"
- NetApp HCI*
- "Voraussetzungen für die NetApp HCI Bereitstellung"
- "Greifen Sie auf die NetApp Bereitstellungs-Engine zu."

Informationen zu bewährten Anwendungspraktiken

- "Bewährte Verfahren für MySQL auf ONTAP"
- "Bewährte Vorgehensweisen für MySQL auf SolidFire"
- "NetApp SolidFire und Cassandra"
- "Oracle Best Practices für SolidFire"
- "PostgreSQL-Best Practices auf SolidFire"

Nicht für alle Anwendungen gibt es spezifische Richtlinien. Es ist wichtig, mit Ihrem NetApp -Team zusammenzuarbeiten und die "NetApp Bibliothek" um die aktuellste Dokumentation zu finden.

Integriere Trident

Für die Integration von Trident ist die Integration der folgenden Design- und Architekturelemente erforderlich: Treiberauswahl und -bereitstellung, Speicherklassendesign, Design virtueller Pools, Auswirkungen von Persistent Volume Claims (PVC) auf die Speicherbereitstellung, Volumenoperationen und die Bereitstellung von OpenShift-Diensten mit Trident.

Fahrerauswahl und -einsatz

Wählen Sie einen Backend-Treiber für Ihr Speichersystem aus und stellen Sie ihn bereit.

ONTAP Backend-Treiber

ONTAP Backend-Treiber unterscheiden sich durch das verwendete Protokoll und die Art und Weise, wie die Volumes auf dem Speichersystem bereitgestellt werden. Überlegen Sie sich daher gut, welchen Treiber Sie einsetzen möchten.

Auf einer höheren Ebene, wenn Ihre Anwendung Komponenten enthält, die gemeinsam genutzten Speicher benötigen (mehrere Pods greifen auf denselben PVC zu), sind NAS-basierte Treiber die Standardwahl, während die blockbasierten iSCSI-Treiber die Anforderungen von nicht gemeinsam genutztem Speicher erfüllen. Wählen Sie das Protokoll basierend auf den Anforderungen der Anwendung und dem Komfortniveau der Speicher- und Infrastrukturteams. Im Allgemeinen gibt es für die meisten Anwendungen kaum einen Unterschied zwischen ihnen, daher basiert die Entscheidung oft darauf, ob gemeinsam genutzter Speicher (auf den mehr als ein Pod gleichzeitig zugreifen muss) benötigt wird oder nicht.

Folgende ONTAP Backend-Treiber stehen zur Verfügung:

- `ontap-nas`Jedes bereitgestellte PV ist ein vollständiges ONTAP FlexVolume.
- `ontap-nas-economy`: Jedes bereitgestellte PV ist ein Qtree, wobei die Anzahl der Qtrees pro FlexVolume konfigurierbar ist (Standardwert ist 200).
- `ontap-nas-flexgroup`: Jeder PV wird als vollständige ONTAP FlexGroup bereitgestellt, und alle einem SVM zugewiesenen Aggregate werden verwendet.
- `ontap-san`Jedes bereitgestellte PV ist eine LUN innerhalb eines eigenen FlexVolumes.
- `ontap-san-economy`Jedes bereitgestellte PV ist eine LUN, wobei die Anzahl der LUNs pro FlexVolume konfigurierbar ist (Standardwert ist 100).

Die Wahl zwischen den drei NAS-Treibern hat Auswirkungen auf die Funktionen, die der Anwendung zur Verfügung stehen.

Beachten Sie, dass in den folgenden Tabellen nicht alle Funktionen über Trident zugänglich sind. Einige dieser Einstellungen müssen vom Speicheradministrator nach der Bereitstellung vorgenommen werden, wenn die gewünschte Funktionalität gewünscht ist. Die hochgestellten Fußnoten unterscheiden die Funktionalität pro Feature und Treiber.

ONTAP NAS-Treiber	Snapshots	Klone	Dynamische Exportrichtlinien	Mehrfachbefestigung	QoS	Größe ändern	Replikation
`ontap-nas`	Ja	Ja	Fußnote Ja:5[]	Ja	Fußnote:1[]	Ja	Fußnote:1[]
`ontap-nas-economy`	NO [3]	NO [3]	Fußnote Ja:5[]	Ja	NO [3]	Ja	NO [3]
`ontap-nas-flexgroup`	Fußnote:1[]	NEIN	Fußnote Ja:5[]	Ja	Fußnote:1[]	Ja	Fußnote:1[]

Trident bietet 2 SAN-Treiber für ONTAP an, deren Funktionen im Folgenden dargestellt werden.

ONTAP SAN-Treiber	Snapshots	Klone	Mehrfachbefestigung	Bidirektionales CHAP	QoS	Größe ändern	Replikation
`ontap-san`	Ja	Ja	Fußnote Ja:4[]	Ja	Fußnote:1[]	Ja	Fußnote:1[]
`ontap-san-economy`	Ja	Ja	Fußnote Ja:4[]	Ja	NO [3]	Ja	NO [3]

> Fußnoten zu den obigen Tabellen: Yes [1]: Nicht von Trident verwaltet Yes [2]: Von Trident verwaltet, aber nicht PV-granular No [3]: Nicht von Trident verwaltet und nicht PV-granular Yes [4]: Für Raw-Block-Volumes unterstützt Yes [5]: Von Trident unterstützt

Die Features, die nicht PV-granular sind, werden auf das gesamte FlexVolume angewendet, und alle PVs (d. h. Qtrees oder LUNs in gemeinsam genutzten FlexVols) teilen sich einen gemeinsamen Zeitplan.

Wie wir aus den obigen Tabellen ersehen können, besteht ein Großteil der Funktionalität zwischen den `ontap-nas` Und `ontap-nas-economy` ist dasselbe. Da jedoch `ontap-nas-economy` Der Treiber schränkt die Möglichkeit ein, den Zeitplan auf Ebene einzelner PVs zu steuern; dies kann sich insbesondere auf Ihre Notfallwiederherstellungs- und Datensicherungsplanung auswirken. Für Entwicklungsteams, die die PVC-Klonfunktion auf ONTAP -Speicher nutzen möchten, ist dies nur möglich, wenn sie Folgendes verwenden: `ontap-nas` , `ontap-san` oder `ontap-san-economy` Fahrer.

Der `solidfire-san` Der Treiber ist auch in der Lage, PVCs zu klonen.

Cloud Volumes ONTAP Backend-Treiber

Cloud Volumes ONTAP bietet Datenkontrolle sowie Speicherfunktionen der Enterprise-Klasse für verschiedene Anwendungsfälle, darunter Dateifreigaben und Blockspeicher, die NAS- und SAN-Protokolle (NFS, SMB / CIFS und iSCSI) unterstützen. 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 und Cloud Volume ONTAP für GCP.

Amazon FSx für ONTAP Backend-Treiber

Mit Amazon FSx for NetApp ONTAP können Sie die Ihnen vertrauten Funktionen, die Leistung und die administrativen Möglichkeiten von NetApp nutzen und gleichzeitig die Einfachheit, Agilität, Sicherheit und Skalierbarkeit der Datenspeicherung auf AWS in Anspruch nehmen. 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` .

NetApp HCI/ SolidFire Backend-Treiber

Der `solidfire-san` Der Treiber, der mit den NetApp HCI/ SolidFire Plattformen verwendet wird, hilft dem Administrator, ein Element-Backend für Trident auf Basis von QoS-Grenzwerten zu konfigurieren. Wenn Sie Ihr Backend so konfigurieren möchten, dass die spezifischen QoS-Grenzwerte für die von Trident bereitgestellten Volumes festgelegt werden, verwenden Sie die `type` Parameter in der Backend-Datei. Der Administrator kann außerdem die Größe des auf dem Speicher erstellten Volumes mithilfe der `limitVolumeSize` Parameter. Aktuell werden Element-Speicherfunktionen wie die Größenänderung von Datenträgern und die Replikation von Datenträgern nicht unterstützt. `solidfire-san` Treiber. Diese Vorgänge sollten manuell über die Web-Benutzeroberfläche von Element Software durchgeführt werden.

SolidFire -Treiber	Snapshots	Klone	Mehrfachbefestigung	KERL	QoS	Größe ändern	Replikation
`solidfire-san`	Ja	Ja	Fußnote Ja:2[]	Ja	Ja	Ja	Fußnote:1[]

> Fußnote: Yes [1]: Wird nicht von Trident verwaltet Yes [2]: Wird für Raw-Block-Volumes unterstützt

Azure NetApp Files -Backend-Treiber

Trident verwendet die `azure-netapp-files` Fahrer zur Verwaltung des"Azure NetApp Files" Service.

Weitere Informationen zu diesem Treiber und dessen Konfiguration finden Sie in"Trident Backend-Konfiguration für Azure NetApp Files" .

Azure NetApp Files Treiber	Snapshots	Klone	Mehrfachbefestigung	QoS	Expandieren	Replikation
`azure-netapp-files`	Ja	Ja	Ja	Ja	Ja	Fußnote:1[]

> Fußnote: Yes [1]: Nicht von Trident verwaltet

Cloud Volumes Service auf Google Cloud Backend-Treiber

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

Der `gcp-cvs` Der Treiber verwendet virtuelle Pools, um das Backend zu abstrahieren und Trident die Bestimmung der Volume-Platzierung zu ermöglichen. Der Administrator definiert die virtuellen Pools im `backend.json` Dateien. Speicherklassen verwenden Selektoren, um virtuelle Pools anhand ihrer Bezeichnung zu identifizieren.

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

Um das Google Cloud-Backend auf Trident zu konfigurieren, müssen Sie Folgendes angeben: `projectNumber` , `apiRegion` , Und `apiKey` in der Backend-Datei. Die Projektnummer finden Sie in der Google Cloud Console. Der API-Schlüssel stammt aus der privaten Schlüsseldatei des Dienstkontos, die Sie beim Einrichten des API-Zugriffs für den Cloud Volumes Service auf Google Cloud erstellt haben.

Für Details zum Cloud Volumes Service auf Google Cloud (Diensttypen und Servicelevel) siehe"Erfahren Sie mehr über die Trident Unterstützung für CVS für GCP." .

Cloud Volumes Service für Google Cloud Driver	Snapshots	Klone	Mehrfachbefestigung	QoS	Expandieren	Replikation
`gcp-cvs`	Ja	Ja	Ja	Ja	Ja	Nur verfügbar beim Servicetyp CVS-Performance.

Replikationsnotizen

- Die Replikation wird nicht von Trident verwaltet.
- Der Klon wird im selben Speicherpool wie das Quellvolume erstellt.

Speicherklassendesign

Einzelne Storage-Klassen müssen konfiguriert und angewendet werden, um ein Kubernetes-Storage-Class-Objekt zu erstellen. In diesem Abschnitt wird erläutert, wie Sie eine Speicherklasse für Ihre Anwendung entwerfen.

Spezifische Backend-Nutzung

Mithilfe von Filtern kann innerhalb eines bestimmten Speicherklassenobjekts ermittelt werden, welcher Speicherpool oder welche Gruppe von Speicherpools mit dieser bestimmten Speicherklasse verwendet werden soll. In der Speicherklasse können drei Filtersätze festgelegt werden: `storagePools` , `additionalStoragePools` und/oder `excludeStoragePools` .

Der `storagePools` Mit diesem Parameter kann der Speicher auf die Pools beschränkt werden, die den angegebenen Attributen entsprechen. Der `additionalStoragePools` Der Parameter dient dazu, die Menge der Pools, die Trident für die Bereitstellung verwendet, zusammen mit der Menge der durch die Attribute ausgewählten Pools zu erweitern. `storagePools` Parameter. Sie können entweder den einen oder den anderen Parameter einzeln oder beide zusammen verwenden, um sicherzustellen, dass die richtigen Speicherpools ausgewählt werden.

Der `excludeStoragePools` Der Parameter dient dazu, die aufgelisteten Pools, die den Attributen entsprechen, gezielt auszuschließen.

Emulieren von QoS-Richtlinien

Wenn Sie Speicherklassen entwerfen möchten, um QoS-Richtlinien zu emulieren, erstellen Sie eine Speicherklasse mit der `media` Attribut als `hdd` oder `ssd` . Basierend auf der `media` Trident wählt für jedes in der Speicherklasse angegebene Attribut das passende Backend aus. `hdd` oder `ssd` Aggregate werden erstellt, um das Medienattribut abzugleichen und anschließend die Bereitstellung der Volumes auf das jeweilige Aggregat zu steuern. Daher können wir eine Speicherklasse PREMIUM erstellen, die Folgendes hätte: `media` Attribut festgelegt als `ssd` was als PREMIUM QoS-Richtlinie eingestuft werden könnte. Wir können eine weitere Speicherklasse STANDARD erstellen, deren Medienattribut auf `hdd` gesetzt wäre, die als STANDARD QoS-Richtlinie klassifiziert werden könnte. Wir könnten auch das Attribut „IOPS“ in der Speicherklasse verwenden, um die Bereitstellung auf ein Element-Gerät umzuleiten, das als QoS-Richtlinie definiert werden kann.

Nutzen Sie das Backend basierend auf spezifischen Funktionen

Speicherklassen können so konzipiert werden, dass die Volumenbereitstellung auf einem bestimmten Backend gesteuert wird, auf dem Funktionen wie Thin und Thick Provisioning, Snapshots, Klone und Verschlüsselung aktiviert sind. Um festzulegen, welcher Speicher verwendet werden soll, erstellen Sie Speicherklassen, die das entsprechende Backend mit den erforderlichen aktivierten Funktionen angeben.

Virtuelle Pools

Virtuelle Pools sind für alle Trident -Backends verfügbar. Sie können virtuelle Pools für jedes Backend definieren und dabei jeden von Trident bereitgestellten Treiber verwenden.

Virtuelle Pools ermöglichen es einem Administrator, eine Abstraktionsebene über Backends zu erstellen, auf die über Storage Classes verwiesen werden kann, um eine größere Flexibilität und effizientere Platzierung von Volumes auf Backends zu gewährleisten. Verschiedene Backends können mit derselben Serviceklasse definiert werden. Darüber hinaus können auf demselben Backend mehrere Speicherpools mit unterschiedlichen Eigenschaften erstellt werden. Wenn eine Speicherklasse mit einem Selektor mit den spezifischen Bezeichnungen konfiguriert ist, wählt Trident ein Backend aus, das allen Selektorbezeichnungen entspricht, um das Volume dort zu platzieren. Wenn die Bezeichnungen des Speicherklassenselektors mit mehreren Speicherpools übereinstimmen, wählt Trident einen davon aus, um das Volume bereitzustellen.

Virtuelles Pool-Design

Beim Erstellen eines Backends können Sie im Allgemeinen einen Satz von Parametern angeben. Es war für den Administrator unmöglich, ein anderes Backend mit denselben Speicheranmeldeinformationen und einem anderen Satz von Parametern zu erstellen. Mit der Einführung virtueller Pools wurde dieses Problem behoben. Ein virtueller Pool ist eine Ebenenabstraktion zwischen dem Backend und der Kubernetes-Speicherklasse, sodass der Administrator Parameter zusammen mit Bezeichnungen definieren kann, auf die über Kubernetes-Speicherklassen als Selektor Backend-unabhängig verwiesen werden kann. Virtuelle Pools können mit Trident für alle unterstützten NetApp Backends definiert werden. Diese Liste umfasst SolidFire/ NetApp HCI, ONTAP, Cloud Volumes Service auf GCP sowie Azure NetApp Files.

> Bei der Definition virtueller Pools wird empfohlen, die Reihenfolge bestehender virtueller Pools in einer Backend-Definition nicht zu ändern. Es empfiehlt sich außerdem, die Attribute eines bestehenden virtuellen Pools nicht zu bearbeiten/zu ändern, sondern stattdessen einen neuen virtuellen Pool zu definieren.

Emulation verschiedener Servicelevel/QoS

Es ist möglich, virtuelle Pools zur Emulation von Serviceklassen zu entwerfen. Anhand der virtuellen Pool-Implementierung für Cloud Volume Service für Azure NetApp Files wollen wir untersuchen, wie wir

verschiedene Dienstklassen einrichten können. Konfigurieren Sie das Azure NetApp Files -Backend mit mehreren Bezeichnungen, die unterschiedliche Leistungsstufen darstellen. Satz `servicelevel` den jeweiligen Aspekt dem entsprechenden Leistungsniveau zuordnen und unter jeder Bezeichnung weitere erforderliche Aspekte hinzufügen. Erstellen Sie nun verschiedene Kubernetes-Speicherklassen, die unterschiedlichen virtuellen Pools zugeordnet werden. Verwenden des `parameters.selector` Im Feld „StorageClass“ wird für jede StorageClass angegeben, welche virtuellen Pools zum Hosten eines Volumes verwendet werden können.

Zuweisung eines bestimmten Satzes von Aspekten

Ausgehend von einem einzigen Speicher-Backend können mehrere virtuelle Pools mit jeweils spezifischen Eigenschaften entworfen werden. Konfigurieren Sie dazu das Backend mit mehreren Labels und legen Sie unter jedem Label die erforderlichen Aspekte fest. Erstellen Sie nun verschiedene Kubernetes-Speicherklassen mithilfe der `parameters.selector` Feld, das verschiedenen virtuellen Pools zugeordnet werden würde. Die im Backend bereitgestellten Volumes weisen die im gewählten virtuellen Pool definierten Eigenschaften auf.

PVC-Eigenschaften, die die Speicherkapazität beeinflussen

Bei der Erstellung eines PVC können neben den angeforderten Speicherklassen auch andere Parameter den Trident -Bereitstellungsprozess beeinflussen.

Zugriffsmodus

Bei der Anforderung von Speicherplatz über eine PVC ist eines der Pflichtfelder der Zugriffsmodus. Der gewünschte Modus kann Einfluss darauf haben, welches Backend für die Verarbeitung der Speicheranfrage ausgewählt wird.

Trident wird versuchen, das verwendete Speicherprotokoll mit der angegebenen Zugriffsmethode gemäß der folgenden Matrix abzugleichen. Dies ist unabhängig von der zugrunde liegenden Speicherplattform.

	Einmal lesen und schreiben	ReadOnlyMany	ReadWriteMany
iSCSI	Ja	Ja	Ja (Rohblock)
NFS	Ja	Ja	Ja

Eine Anfrage für ein ReadWriteMany PVC, die an eine Trident Bereitstellung ohne konfiguriertes NFS-Backend gesendet wird, führt dazu, dass kein Volume bereitgestellt wird. Aus diesem Grund sollte der Anfragende den für seine Anwendung geeigneten Zugriffsmodus verwenden.

Volumenoperationen

Persistente Volumes ändern

Persistente Volumes sind, mit zwei Ausnahmen, unveränderliche Objekte in Kubernetes. Nach der Erstellung können die Rückforderungsrichtlinie und die Größe angepasst werden. Dies verhindert jedoch nicht, dass bestimmte Aspekte des Volumes außerhalb von Kubernetes modifiziert werden. Dies kann wünschenswert sein, um das Volume für bestimmte Anwendungen anzupassen, um sicherzustellen, dass die Kapazität nicht versehentlich verbraucht wird, oder um das Volume aus beliebigen Gründen auf einen anderen Speichercontroller zu verschieben.

Die In-Tree-Provisioner von Kubernetes unterstützen derzeit keine Volume-Resize-Operationen 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 mehr geändert werden.

Erstellen Sie bedarfsgesteuerte Volume-Snapshots

Trident unterstützt die Erstellung von Volume-Snapshots bei Bedarf sowie die Erstellung von PVCs aus Snapshots mithilfe des CSI-Frameworks. Snapshots bieten eine komfortable Methode zur Aufbewahrung von zeitpunktbezogenen Kopien der Daten und haben einen vom Quell-PV in Kubernetes unabhängigen Lebenszyklus. Mithilfe dieser Snapshots können PVCs geklont werden.

Volumes aus Snapshots erstellen

Trident unterstützt auch die Erstellung von PersistentVolumes aus Volume-Snapshots. Um dies zu erreichen, erstellen Sie einfach einen PersistentVolumeClaim und geben Sie den entsprechenden Eintrag an. `datasource` als der erforderliche Snapshot, aus dem das Volume erstellt werden muss. Trident wird dieses PVC verarbeiten, indem ein Volume mit den im Snapshot vorhandenen Daten erstellt wird. Mit dieser Funktion können Daten regionsübergreifend dupliziert, Testumgebungen erstellt, ein beschädigtes oder fehlerhaftes Produktionsvolume vollständig ersetzt oder bestimmte Dateien und Verzeichnisse abgerufen und auf ein anderes angeschlossenes Volume übertragen werden.

Verschieben Sie die Volumes im Cluster

Speicheradministratoren haben die Möglichkeit, Datenträger zwischen Aggregaten und Controllern im ONTAP Cluster zu verschieben, ohne den Speicherkonsumenten zu beeinträchtigen. Dieser Vorgang hat keine Auswirkungen auf Trident oder den Kubernetes-Cluster, sofern es sich bei dem Zielaggregat um ein solches handelt, auf das die von Trident verwendete SVM Zugriff hat. Wichtig ist, dass, wenn das Aggregat neu zum SVM hinzugefügt wurde, das Backend aktualisiert werden muss, indem es erneut zu Trident hinzugefügt wird. Dies veranlasst Trident, das SVM neu zu inventarisieren, damit das neue Aggregat erkannt wird.

Das Verschieben von Datenvolumen zwischen verschiedenen Backends wird von Trident jedoch nicht automatisch unterstützt. Dies umfasst SVMs innerhalb desselben Clusters, SVMs zwischen Clustern oder SVMs auf einer anderen Speicherplattform (selbst wenn dieses Speichersystem mit Trident verbunden ist).

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

Volumen erweitern

Trident unterstützt die Größenänderung von NFS-, iSCSI- und FC-PVs. Dies ermöglicht es Benutzern, ihre Volumes direkt über die Kubernetes-Schicht zu vergrößern oder zu verkleinern. Die Speichererweiterung ist für alle wichtigen NetApp Speicherplattformen möglich, einschließlich ONTAP, SolidFire/ NetApp HCI und Cloud Volumes Service Backends. Um eine spätere Erweiterung zu ermöglichen, setzen Sie `allowVolumeExpansion` Zu `true` in Ihrer StorageClass, die dem Volume zugeordnet ist. Immer wenn die Größe des persistenten Volumes geändert werden muss, bearbeiten Sie die `spec.resources.requests.storage` Anmerkung im Persistent Volume Claim zur erforderlichen Volumengröße. Trident kümmert sich automatisch um die Größenanpassung des Volumes im Speichercluster.

Ein vorhandenes Volume in Kubernetes importieren

Der Volume-Import ermöglicht es, ein vorhandenes Speichervolume in eine Kubernetes-Umgebung zu importieren. Dies wird derzeit unterstützt durch `ontap-nas` , `ontap-nas-flexgroup` , `solidfire-san` ,

`azure-netapp-files` , Und `gcp-cvs` Fahrer. Diese Funktion ist nützlich beim Portieren einer bestehenden Anwendung nach Kubernetes oder in Notfallwiederherstellungsszenarien.

Bei der Verwendung von ONTAP und `solidfire-san` Fahrer, verwenden Sie den Befehl `tridentctl import volume <backend-name> <volume-name> -f /path/pvc.yaml` Ein vorhandenes Volume in Kubernetes importieren, das von Trident verwaltet werden soll. Die im Import-Volume-Befehl verwendete PVC-YAML- oder JSON-Datei verweist auf eine Speicherklasse, die Trident als Provisionierer identifiziert. Bei Verwendung eines NetApp HCI/ SolidFire Backends muss sichergestellt werden, dass die Volume-Namen eindeutig sind. Falls die Volumennamen doppelt vorkommen, klonen Sie das Volumen unter einem eindeutigen Namen, damit die Volumenimportfunktion sie unterscheiden kann.

Wenn die `azure-netapp-files` oder `gcp-cvs` Wenn der Treiber verwendet wird, verwenden Sie den Befehl `tridentctl import volume <backend-name> <volume path> -f /path/pvc.yaml` Das Volume soll in Kubernetes importiert und von Trident verwaltet werden. Dies gewährleistet eine eindeutige Volumenreferenz.

Wenn der obige Befehl ausgeführt wird, findet Trident das Volume im Backend und liest dessen Größe aus. Die konfigurierte PVC-Volumengröße wird automatisch hinzugefügt (und gegebenenfalls überschrieben). Trident erstellt dann das neue PV und Kubernetes bindet das PVC an das PV.

Wenn ein Container so eingesetzt wird, dass er die spezifische importierte PVC benötigt, bleibt er im Status "ausstehend", bis das PVC/PV-Paar über den Volumenimportprozess gebunden wird. Nach dem Verbinden der PVC/PV-Leitungen sollte sich der Behälter hochziehen lassen, sofern keine anderen Probleme auftreten.

Registrierungsdienst

Die Bereitstellung und Verwaltung des Speichers für die Registry wurde dokumentiert auf"netapp.io" im"Blog" .

Protokollierungsdienst

Wie andere OpenShift-Dienste wird auch der Protokollierungsdienst mithilfe von Ansible bereitgestellt, wobei die Konfigurationsparameter aus der Inventardatei (auch Hosts genannt) stammen, die dem Playbook übergeben wird. Es werden zwei Installationsmethoden behandelt: die Bereitstellung der Protokollierung während der Erstinstallation von OpenShift und die Bereitstellung der Protokollierung nach der Installation von OpenShift.

> Ab Red Hat OpenShift Version 3.9 rät die offizielle Dokumentation aufgrund von Bedenken hinsichtlich Datenbeschädigung von NFS für den Protokollierungsdienst ab. Dies basiert auf Tests, die Red Hat mit ihren Produkten durchgeführt hat. Der ONTAP NFS-Server hat diese Probleme nicht und kann problemlos eine Protokollierungsbereitstellung unterstützen. Letztendlich liegt die Wahl des Protokolls für den Protokollierungsdienst bei Ihnen. Sie sollten jedoch wissen, dass beide Protokolle auf NetApp -Plattformen hervorragend funktionieren und es keinen Grund gibt, NFS zu vermeiden, wenn Sie diese Option bevorzugen.

Wenn Sie NFS mit dem Protokollierungsdienst verwenden möchten, müssen Sie die Ansible-Variable festlegen. `openshift_enable_unsupported_configurations` Zu `true` um zu verhindern, dass das Installationsprogramm fehlschlägt.

Erste Schritte

Der Protokollierungsdienst kann optional sowohl für Anwendungen als auch für den Kernbetrieb des OpenShift-Clusters selbst bereitgestellt werden. Wenn Sie die Protokollierung von Vorgängen aktivieren möchten, geben Sie dazu die Variable an. `openshift_logging_use_ops` als `true` Es werden zwei Instanzen des Dienstes erstellt. Die Variablen, die die Protokollierungsinstanz für Operationen steuern,

enthalten "ops" in sich, während dies bei der Instanz für Anwendungen nicht der Fall ist.

Die Konfiguration der Ansible-Variablen entsprechend der Bereitstellungsmethode ist wichtig, um sicherzustellen, dass die zugrunde liegenden Dienste den richtigen Speicher nutzen. Schauen wir uns die Optionen für jede der Bereitstellungsmethoden an.

> Die nachfolgenden Tabellen enthalten nur die Variablen, die für die Speicherkonfiguration im Zusammenhang mit dem Protokollierungsdienst relevant sind. Weitere Optionen finden Sie in"Red Hat OpenShift-Protokollierungsdokumentation" Diese sollten entsprechend Ihrer Bereitstellung geprüft, konfiguriert und verwendet werden.

Die Variablen in der folgenden Tabelle führen dazu, dass das Ansible-Playbook anhand der angegebenen Details ein PV und ein PVC für den Logging-Service erstellt. Diese Methode ist deutlich weniger flexibel als die Verwendung des Komponenteninstallations-Playbooks nach der OpenShift-Installation. Wenn Sie jedoch bereits Volumes zur Verfügung haben, ist sie eine Option.

Variable	Details
`openshift_logging_storage_kind`	Auf einstellen `nfs` Der Installer soll ein NFS PV für den Protokollierungsdienst erstellen.
`openshift_logging_storage_host`	Der Hostname oder die IP-Adresse des NFS-Hosts. Dies sollte auf die dataLIF Ihrer virtuellen Maschine eingestellt werden.
`openshift_logging_storage_nfs_directory`	Der Mount-Pfad für den NFS-Export. Wenn beispielsweise das Volumen als verbunden wird `/openshift_logging` Diesen Pfad würden Sie für diese Variable verwenden.
`openshift_logging_storage_volume_name`	Der Name, z.B. `pv_ose_logs` , der PV zu erzeugen.
`openshift_logging_storage_volume_size`	Die Größe des NFS-Exports, zum Beispiel `100Gi` .

Wenn Ihr OpenShift-Cluster bereits läuft und Trident daher bereitgestellt und konfiguriert wurde, kann das Installationsprogramm die Volumes mithilfe der dynamischen Bereitstellung erstellen. Folgende Variablen müssen konfiguriert werden.

Variable	Details
`openshift_logging_es_pvc_dynamic`	Auf „true“ setzen, um dynamisch bereitgestellte Volumes zu verwenden.
`openshift_logging_es_pvc_storage_class_name`	Die Bezeichnung der Speicherklasse, die im PVC verwendet wird.
`openshift_logging_es_pvc_size`	Die im PVC angeforderte Volumengröße.
`openshift_logging_es_pvc_prefix`	Ein Präfix für die vom Protokollierungsdienst verwendeten PVCs.
`openshift_logging_es_ops_pvc_dynamic`	Auf einstellen `true` Um dynamisch bereitgestellte Volumes für die Ops-Protokollierungsinstanz zu verwenden.
`openshift_logging_es_ops_pvc_storage_class_name`	Der Name der Speicherklasse für die Operationsprotokollierungsinstanz.

Variable	Details
`openshift_logging_es_ops_pvc_size`	Die Größe der Volumenanforderung für die Ops-Instanz.
`openshift_logging_es_ops_pvc_prefix`	Ein Präfix für die PVCs der Operationsinstanz.

Stellen Sie den Logging-Stack bereit.

Wenn Sie die Protokollierung im Rahmen des anfänglichen OpenShift-Installationsprozesses bereitstellen, müssen Sie lediglich dem Standard-Bereitstellungsprozess folgen. Ansible konfiguriert und stellt die benötigten Dienste und OpenShift-Objekte bereit, sodass der Dienst verfügbar ist, sobald Ansible den Vorgang abgeschlossen hat.

Wenn Sie jedoch nach der Erstinstallation eine Bereitstellung durchführen, muss das Komponenten-Playbook von Ansible verwendet werden. Dieser Prozess kann sich je nach OpenShift-Version geringfügig unterscheiden. Lesen und befolgen Sie daher unbedingt die Anweisungen."Red Hat OpenShift Container Platform 3.11 Dokumentation" für Ihre Version.

Metrikdienst

Der Metrikdienst liefert dem Administrator wertvolle Informationen über den Status, die Ressourcennutzung und die Verfügbarkeit des OpenShift-Clusters. Es ist außerdem für die automatische Skalierungsfunktion der Pods erforderlich, und viele Organisationen nutzen Daten aus dem Metrikdienst für ihre Kostenverrechnungs- und/oder Anzeigeanwendungen.

Wie beim Logging-Service und OpenShift insgesamt wird auch beim Metrik-Service Ansible verwendet. Ebenso wie der Protokollierungsdienst kann auch der Metrikendienst während der Ersteinrichtung des Clusters oder nach dessen Inbetriebnahme mithilfe der Komponenteninstallationsmethode bereitgestellt werden. Die folgenden Tabellen enthalten die Variablen, die bei der Konfiguration des persistenten Speichers für den Metrikdienst wichtig sind.

> Die nachfolgenden Tabellen enthalten nur die Variablen, die für die Speicherkonfiguration im Zusammenhang mit dem Metrikdienst relevant sind. Es gibt viele weitere Optionen in der Dokumentation, die geprüft, konfiguriert und entsprechend Ihrer Bereitstellung verwendet werden sollten.

Variable	Details
`openshift_metrics_storage_kind`	Auf einstellen `nfs` Der Installer soll ein NFS PV für den Protokollierungsdienst erstellen.
`openshift_metrics_storage_host`	Der Hostname oder die IP-Adresse des NFS-Hosts. Dies sollte auf den dataLIF für Ihre SVM eingestellt werden.
`openshift_metrics_storage_nfs_directory`	Der Mount-Pfad für den NFS-Export. Wenn beispielsweise das Volumen als verbunden wird `/openshift_metrics` Diesen Pfad würden Sie für diese Variable verwenden.
`openshift_metrics_storage_volume_name`	Der Name, z.B. `pv_ose_metrics` , der PV zu erzeugen.
`openshift_metrics_storage_volume_size`	Die Größe des NFS-Exports, zum Beispiel `100Gi` .

Wenn Ihr OpenShift-Cluster bereits läuft und Trident daher bereitgestellt und konfiguriert wurde, kann das Installationsprogramm die Volumes mithilfe der dynamischen Bereitstellung erstellen. Folgende Variablen müssen konfiguriert werden.

Variable	Details
`openshift_metrics_cassandra_pvc_prefix`	Ein Präfix für die Metrik-PVCs.
`openshift_metrics_cassandra_pvc_size`	Die Größe der anzufordernden Volumina.
`openshift_metrics_cassandra_storage_type`	Der Speichertyp für Metriken muss auf dynamisch eingestellt sein, damit Ansible PVCs mit der entsprechenden Speicherklasse erstellen kann.
`openshift_metrics_cassanda_pvc_storage_class_name`	Der Name der zu verwendenden Speicherklasse.

Stellen Sie den Metrikdienst bereit.

Nachdem die entsprechenden Ansible-Variablen in Ihrer hosts/inventory-Datei definiert wurden, können Sie den Dienst mithilfe von Ansible bereitstellen. Wenn Sie die Bereitstellung zum Zeitpunkt der OpenShift-Installation durchführen, wird das PV automatisch erstellt und verwendet. Wenn Sie die Bereitstellung mithilfe der Komponenten-Playbooks durchführen, erstellt Ansible nach der OpenShift-Installation alle benötigten PVCs und stellt den Dienst bereit, nachdem Trident Speicherplatz dafür bereitgestellt hat.

Die oben genannten Variablen und der Bereitstellungsprozess können sich mit jeder Version von OpenShift ändern. Bitte überprüfen und befolgen Sie die Anweisungen."Red Hats OpenShift-Bereitstellungsleitfaden" für Ihre Version, damit sie für Ihre Umgebung konfiguriert ist.

Datenschutz und Notfallwiederherstellung

Erfahren Sie mehr über Schutz- und Wiederherstellungsoptionen für Trident und mit Trident erstellte Volumes. Sie sollten für jede Anwendung mit Persistenzanforderungen eine Datensicherungs- und -wiederherstellungsstrategie haben.

Trident -Replikation und -Wiederherstellung

Sie können eine Sicherungskopie erstellen, um Trident im Katastrophenfall wiederherzustellen.

Trident -Replikation

Trident verwendet Kubernetes CRDs, um seinen eigenen Zustand zu speichern und zu verwalten, und das Kubernetes-Cluster-etcd, um seine Metadaten zu speichern.

Schritte

1. Sichern Sie den etcd-Speicher des Kubernetes-Clusters mit"Kubernetes: Sichern eines etcd-Clusters" .
2. Platzieren Sie die Sicherungsdateien auf einem FlexVol volume.

> NetApp empfiehlt, die SVM, auf der sich FlexVol befindet, durch eine SnapMirror -Beziehung zu einer anderen SVM zu schützen.

Trident Wiederherstellung

Mithilfe von Kubernetes CRDs und dem etcd-Snapshot des Kubernetes-Clusters lässt sich Trident wiederherstellen.

Schritte

1. Vom Ziel-SVM wird das Volume, das die Kubernetes etcd-Datendateien und Zertifikate enthält, auf dem Host eingebunden, der als Master-Knoten eingerichtet werden soll.
2. Kopieren Sie alle erforderlichen Zertifikate, die sich auf den Kubernetes-Cluster beziehen, unter `/etc/kubernetes/pki` und die etcd-Mitgliedsdateien unter `/var/lib/etcd` .
3. Stellen Sie den Kubernetes-Cluster aus dem etcd-Backup wieder her, indem Sie"Kubernetes: Wiederherstellen eines etcd-Clusters" .
4. Laufen `kubectl get crd` um zu überprüfen, ob alle Trident Benutzerressourcen geladen wurden, und um die Trident -Objekte abzurufen, um zu überprüfen, ob alle Daten verfügbar sind.

SVM-Replikation und -Wiederherstellung

Trident kann keine Replikationsbeziehungen konfigurieren, der Speicheradministrator kann dies jedoch tun. "ONTAP SnapMirror" um eine SVM zu replizieren.

Im Katastrophenfall können Sie die SnapMirror Ziel-SVM aktivieren, um mit der Datenbereitstellung zu beginnen. Sie können wieder auf das primäre System umschalten, sobald die Systeme wiederhergestellt sind.

Informationen zu diesem Vorgang

Beachten Sie Folgendes bei der Verwendung der SnapMirror SVM-Replikationsfunktion:

- Sie sollten für jede SVM mit aktiviertem SVM-DR ein separates Backend erstellen.
- Konfigurieren Sie die Speicherklassen so, dass die replizierten Backends nur bei Bedarf ausgewählt werden, um zu vermeiden, dass Volumes, die keine Replikation benötigen, auf den Backends bereitgestellt werden, die SVM-DR unterstützen.
- Anwendungsadministratoren sollten sich der zusätzlichen Kosten und der Komplexität bewusst sein, die mit der Replikation verbunden sind, und ihren Wiederherstellungsplan sorgfältig prüfen, bevor sie mit diesem Prozess beginnen.

SVM-Replikation

Sie können verwenden"ONTAP: SnapMirror SVM-Replikation" um die SVM-Replikationsbeziehung herzustellen.

SnapMirror ermöglicht es Ihnen, Optionen festzulegen, um zu steuern, was repliziert werden soll. Sie müssen wissen, welche Optionen Sie bei der Durchführung ausgewählt haben.SVM-Wiederherstellung mit Trident .

- "-identity-reserve true"repliziert die gesamte SVM-Konfiguration.
- "-discard-configs Netzwerk"Ausgenommen sind LIFs und zugehörige Netzwerkeinstellungen.
- "-identity-reserve false"Es werden lediglich die Volumes und die Sicherheitskonfiguration repliziert.

SVM-Wiederherstellung mit Trident

Trident erkennt SVM-Fehler nicht automatisch. Im Katastrophenfall kann der Administrator manuell ein Trident Failover auf die neue SVM einleiten.

Schritte

1. Brechen Sie geplante und laufende SnapMirror Übertragungen ab, trennen Sie die Replikationsbeziehung, stoppen Sie die Quell-SVM und aktivieren Sie anschließend die SnapMirror Ziel-SVM.
2. Wenn Sie angegeben haben `-identity-preserve false` oder `-discard-config network` Aktualisieren Sie bei der Konfiguration Ihrer SVM-Replikation die `managementLIF` Und `dataLIF` in der Trident Backend-Definitionsdatei.
3. Bestätigen `storagePrefix` ist in der Trident Backend-Definitionsdatei vorhanden. Dieser Parameter kann nicht geändert werden. Auslassen `storagePrefix` wird dazu führen, dass das Backend-Update fehlschlägt.
4. Aktualisieren Sie alle erforderlichen Backends, um den neuen Ziel-SVM-Namen widerzuspiegeln, indem Sie Folgendes verwenden:

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

5. Wenn Sie angegeben haben `-identity-preserve false` oder `discard-config network` Sie müssen alle Anwendungs-Pods neu starten.

> Wenn Sie angegeben haben `-identity-preserve true` Alle von Trident bereitgestellten Volumes beginnen mit der Datenbereitstellung, sobald die Ziel-SVM aktiviert ist.

Volumenreplikation und Wiederherstellung

Trident kann keine SnapMirror Replikationsbeziehungen konfigurieren, der Speicheradministrator kann jedoch Folgendes verwenden:"ONTAP SnapMirror Replikation und -Wiederherstellung" um von Trident erstellte Volumes zu replizieren.

Anschließend können Sie die wiederhergestellten Volumes in Trident importieren."tridentctl volume import" .

> Der Import wird nicht unterstützt auf `ontap-nas-economy` , `ontap-san-economy` , oder `ontap-flexgroup-economy` Fahrer.

Snapshot-Datenschutz

Sie können Daten schützen und wiederherstellen mit:

- Ein externer Snapshot-Controller und CRDs zur Erstellung von Kubernetes-Volume-Snapshots von Persistent Volumes (PVs).

  "Volumen-Snapshots"

- ONTAP Snapshots dienen zur Wiederherstellung des gesamten Inhalts eines Volumes oder zur Wiederherstellung einzelner Dateien oder LUNs.

  "ONTAP Schnappschüsse"

Sicherheit

Sicherheit

Befolgen Sie die hier aufgeführten Empfehlungen, um eine sichere Installation Ihres Trident zu gewährleisten.

Trident in einem eigenen Namensraum ausführen

Um eine zuverlässige Speicherung zu gewährleisten und potenziell schädliche Aktivitäten zu verhindern, ist es wichtig, Anwendungen, Anwendungsadministratoren, Benutzer und Verwaltungsanwendungen den Zugriff auf Trident -Objektdefinitionen oder die Pods zu verwehren.

Um andere Anwendungen und Benutzer von Trident zu trennen, installieren Sie Trident immer in einem eigenen Kubernetes-Namespace.(`trident`). Durch die Platzierung von Trident in einem eigenen Namespace wird sichergestellt, dass nur das Kubernetes-Administratorpersonal Zugriff auf den Trident -Pod und die in den Namespace-CRD-Objekten gespeicherten Artefakte (wie z. B. Backend- und CHAP-Secrets, falls zutreffend) hat. Sie sollten sicherstellen, dass nur Administratoren Zugriff auf den Trident -Namensraum und somit auf die entsprechenden Funktionen haben. `tridentctl` Anwendung.

CHAP-Authentifizierung mit ONTAP SAN-Backends verwenden

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

Für ONTAP Backends, die SAN-Speichertreiber verwenden, kann Trident bidirektionales CHAP einrichten und CHAP-Benutzernamen und -Geheimnisse verwalten. `tridentctl` . Siehe"Bereiten Sie die Konfiguration des Backends mit ONTAP SAN-Treibern vor." um zu verstehen, wie Trident CHAP auf ONTAP Backends konfiguriert.

CHAP-Authentifizierung mit NetApp HCI und SolidFire -Backends verwenden

NetApp empfiehlt den Einsatz von bidirektionalem CHAP, um die Authentifizierung zwischen einem Host und den NetApp HCI und SolidFire -Backends sicherzustellen. Trident verwendet ein geheimes Objekt, das zwei CHAP-Passwörter pro Mandant enthält. Nach der Installation von Trident verwaltet es die CHAP-Geheimnisse und speichert sie in einem `tridentvolume` CR-Objekt für das jeweilige PV. Wenn Sie ein PV erstellen, verwendet Trident die CHAP-Secrets, um eine iSCSI-Sitzung zu initiieren und über CHAP mit dem NetApp HCI und SolidFire -System zu kommunizieren.

Die von Trident erstellten Volumes sind keiner Volume-Zugriffsgruppe zugeordnet.

Verwenden Sie Trident mit NVE und NAE

NetApp ONTAP bietet Datenverschlüsselung im Ruhezustand, um sensible Daten für den Fall zu schützen, dass eine Festplatte gestohlen, zurückgegeben oder anderweitig verwendet wird. Weitere Einzelheiten finden Sie unter"Übersicht über die Konfiguration der NetApp Volume-Verschlüsselung" .

- Wenn NAE im Backend aktiviert ist, wird jedes in Trident bereitgestellte Volume NAE-fähig sein.
  - Sie können das NVE-Verschlüsselungsflag auf „“ setzen. `""` um NAE-fähige Volumes zu erstellen.
- Wenn NAE im Backend nicht aktiviert ist, wird jedes in Trident bereitgestellte Volume NVE-fähig sein, es

sei denn, das NVE-Verschlüsselungsflag ist auf „true“ gesetzt. `false` (der Standardwert) in der Backend-Konfiguration.

> In Trident auf einem NAE-fähigen Backend erstellte Volumes müssen NVE- oder NAE-verschlüsselt sein.
>
> - Sie können das NVE-Verschlüsselungsflag auf „“ setzen. `true` in der Trident -Backend -Konfiguration, um die NAE-Verschlüsselung zu überschreiben und einen spezifischen Verschlüsselungsschlüssel pro Volume zu verwenden.
> - Setzen des NVE-Verschlüsselungsflags auf `false` Auf einem NAE-fähigen Backend wird ein NAE-fähiges Volume erstellt. Die NAE-Verschlüsselung kann nicht durch Setzen des NVE-Verschlüsselungsflags deaktiviert werden. `false` .

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

Weitere Informationen zu den Backend-Konfigurationsoptionen finden Sie unter:

- "ONTAP SAN-Konfigurationsoptionen"
- "ONTAP NAS-Konfigurationsoptionen"

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 von Passphrasen und die Volumenerweiterung für LUKS-verschlüsselte Volumes.

In Trident verwenden LUKS-verschlüsselte Volumes die aes-xts-plain64-Verschlüsselung und den entsprechenden Modus, wie von empfohlen."NIST" .

> LUKS-Verschlüsselung wird für ASA r2-Systeme nicht unterstützt. Informationen zu ASA r2-Systemen finden Sie unter"Erfahren Sie mehr über ASA R2-Speichersysteme" .

Bevor Sie beginnen

- Auf den Worker-Knoten muss cryptsetup 2.1 oder höher (aber niedriger als 3.0) installiert sein. Weitere Informationen finden Sie unter"GitLab: cryptsetup" .
- Aus Performancegründen empfiehlt NetApp , dass Worker-Knoten den Advanced Encryption Standard New Instructions (AES-NI) unterstützen. Um die AES-NI-Unterstützung zu überprüfen, führen Sie folgenden Befehl aus:

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

Wenn keine Antwort zurückgegeben wird, unterstützt Ihr Prozessor AES-NI nicht. Weitere Informationen zu AES-NI finden Sie unter:"Intel: Advanced Encryption Standard Instructions (AES-NI)" .

LUKS-Verschlüsselung aktivieren

Sie können die volumenbezogene, hostseitige Verschlüsselung mithilfe von Linux Unified Key Setup (LUKS) für ONTAP SAN- und ONTAP SAN ECONOMY-Volumes aktivieren.

Schritte

1. Definieren Sie die LUKS-Verschlüsselungsattribute in der Backend-Konfiguration. Weitere Informationen zu den Backend-Konfigurationsoptionen für ONTAP SAN finden Sie unter"ONTAP SAN-Konfigurationsoptionen" .

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

2. Verwenden `parameters.selector` Die Speicherpools werden mithilfe der LUKS-Verschlüsselung definiert. 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 Datenträger können die Deduplizierung und Komprimierung von ONTAP nicht nutzen.

Backend-Konfiguration für den Import von LUKS-Volumes

Um ein LUKS-Volume zu importieren, müssen Sie Folgendes einstellen: `luksEncryption` Zu(`true` im Backend. Der `luksEncryption` Diese Option teilt Trident mit, ob das Volume LUKS-kompatibel 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, legen Sie die Annotation fest. `trident.netapp.io/luksEncryption` Zu `true` und eine LUKS-fähige Speicherklasse in die PVC einbinden, 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
```

LUKS-Passphrase rotieren

Sie können die LUKS-Passphrase ändern und die Änderung bestätigen.

> Vergessen Sie eine Passphrase erst dann, wenn Sie sichergestellt haben, dass sie von keinem Volume, Snapshot oder Geheimnis mehr referenziert wird. Geht die angegebene Passphrase verloren, kann das Volume möglicherweise nicht eingebunden werden und die Daten bleiben verschlüsselt und unzugänglich.

Informationen zu diesem Vorgang

Eine LUKS-Passphrase-Rotation tritt auf, wenn ein Pod, der das Volume einbindet, erstellt wird, nachdem eine neue LUKS-Passphrase angegeben wurde. Wenn ein neuer Pod erstellt wird, vergleicht Trident die LUKS-Passphrase des Volumes mit der aktiven Passphrase im Secret.

- Stimmt die Passphrase des Volumes nicht mit der aktiven Passphrase im Geheimnis überein, findet eine Rotation statt.
- Wenn die Passphrase des Volumes mit der aktiven Passphrase im Geheimnis übereinstimmt, `previous-luks-passphrase` Der Parameter wird ignoriert.

Schritte

1. Füge die `node-publish-secret-name` Und `node-publish-secret-namespace` StorageClass-Parameter. 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 Passphrasen auf dem Volume oder Snapshot.

Volumen

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

...luksPassphraseNames:["A"]
```

Schnappschuss

```
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 neue und die vorherige Passphrase anzugeben. Sicherstellen `previous-luke-passphrase-name` Und `previous-luks-passphrase` Die vorherige Passphrase muss übereinstimmen.

```
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. Erstelle einen neuen Pod, der das Volume einbindet. Dies ist erforderlich, um die Rotation einzuleiten.
5. Überprüfen Sie, ob die Passphrase geändert wurde.

Volumen

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

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

Schnappschuss

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

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

Ergebnisse

Die Passphrase wurde geändert, wenn auf dem Volume und im Snapshot nur noch die neue Passphrase angezeigt wird.

> Wenn zwei Passphrasen zurückgegeben werden, zum Beispiel `luksPassphraseNames: ["B", "A"]` Die Rotation ist unvollständig. Sie können eine neue Kapsel auslösen, um zu versuchen, die Rotation abzuschließen.

Volumenerweiterung aktivieren

Sie können die Volumenerweiterung auf einem LUKS-verschlüsselten Volumen aktivieren.

Schritte

1. Aktivieren Sie die `CSINodeExpandSecret` Feature Gate (Beta 1,25+). Siehe "Kubernetes 1.25: Verwendung von Secrets zur knotengesteuerten Erweiterung von CSI-Volumes" für Details.
2. Füge die `node-expand-secret-name` Und `node-expand-secret-namespace` StorageClass-Parameter. 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 starten, übergibt das Kubelet die entsprechenden Anmeldeinformationen an den Treiber.

Kerberos-Verschlüsselung während des Fluges

Durch die Verwendung von Kerberos-Verschlüsselung während der Datenübertragung können Sie die Datensicherheit verbessern, indem Sie die Verschlüsselung für den Datenverkehr zwischen Ihrem verwalteten Cluster und dem Speicher-Backend aktivieren.

Trident unterstützt Kerberos-Verschlüsselung für ONTAP als Speicher-Backend:

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

Sie können Volumes erstellen, löschen, ihre Größe ändern, Snapshots erstellen, klonen, schreibgeschützte Klone erstellen und importieren, die NFS-Verschlüsselung verwenden.

Konfigurieren der Kerberos-Verschlüsselung während der Übertragung mit lokalen ONTAP -Volumes

Sie können die Kerberos-Verschlüsselung für den Speicherdatenverkehr zwischen Ihrem verwalteten Cluster und einem lokalen ONTAP -Speicher-Backend aktivieren.

> Die Kerberos-Verschlüsselung für NFS-Datenverkehr mit lokalen ONTAP -Speicher-Backends wird nur mit folgender Konfiguration unterstützt: `ontap-nas` Speichertreiber.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie Zugriff auf die `tridentctl` Dienstprogramm.
- Stellen Sie sicher, dass Sie über Administratorzugriff auf das ONTAP -Speicher-Backend verfügen.
- Stellen Sie sicher, dass Sie den Namen des oder der Volumes kennen, die Sie vom ONTAP -Speicher -Backend freigeben werden.
- Stellen Sie sicher, dass Sie die ONTAP -Speicher-VM für die Unterstützung der Kerberos-Verschlüsselung für NFS-Volumes vorbereitet haben. Siehe "Kerberos auf einem dataLIF aktivieren" für Anweisungen.
- Stellen Sie sicher, dass alle NFSv4-Volumes, die Sie mit Kerberos-Verschlüsselung verwenden, korrekt konfiguriert sind. Siehe Abschnitt „NetApp NFSv4-Domänenkonfiguration“ (Seite 13) des "NetApp NFSv4-Erweiterungen und Best Practices-Leitfaden" .

ONTAP Exportrichtlinien hinzufügen oder ändern

Sie müssen bestehenden ONTAP Exportrichtlinien Regeln hinzufügen oder neue Exportrichtlinien erstellen, die die Kerberos-Verschlüsselung für das Root-Volume der ONTAP Speicher-VM sowie für alle ONTAP -Volumes unterstützen, die mit dem Upstream-Kubernetes-Cluster geteilt werden. Die von Ihnen hinzugefügten Exportrichtlinienregeln oder die von Ihnen erstellten neuen Exportrichtlinien müssen die folgenden Zugriffsprotokolle und Zugriffsberechtigungen unterstützen:

Zugriffsprotokolle

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

Zugangsdaten

Je nach Ihren Anforderungen an das Volume können Sie eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung konfigurieren:

- **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 Exportrichtlinienregel mit den entsprechenden Zugriffsberechtigungen. Wenn Cluster beispielsweise die NFS-Volumes mit einer Mischung aus Kerberos 5i- und Kerberos 5p-Verschlüsselung einbinden, verwenden Sie die folgenden Zugriffseinstellungen:

Typ	Nur-Lese-Zugriff	Lese-/Schreibzugriff	Superuser-Zugriff
UNIX	Ermöglicht	Ermöglicht	Ermöglicht
Kerberos 5i	Ermöglicht	Ermöglicht	Ermöglicht
Kerberos 5p	Ermöglicht	Ermöglicht	Ermöglicht

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

- "Erstellen einer Exportrichtlinie"
- "Hinzufügen einer Regel zu einer Exportrichtlinie"

Erstellen Sie ein Speicher-Backend

Sie können eine Trident -Speicher-Backend-Konfiguration erstellen, die die Kerberos-Verschlüsselungsfunktion beinhaltet.

Informationen zu diesem Vorgang

Wenn Sie eine Konfigurationsdatei für das Speicher-Backend erstellen, die die Kerberos-Verschlüsselung konfiguriert, können Sie mithilfe der folgenden Optionen eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung angeben: `spec.nfsMountOptions` Parameter:

- `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-Verschlüsselungsstufe angeben, wird nur die erste Option verwendet.

Schritte

1. Erstellen Sie auf dem verwalteten Cluster eine Speicher-Backend-Konfigurationsdatei anhand des folgenden Beispiels. Ersetzen Sie die Werte in eckigen 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 im vorherigen Schritt erstellte Konfigurationsdatei, um das Backend zu erstellen:

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

Wenn die Backend-Erstellung fehlschlägt, stimmt etwas mit der Backend-Konfiguration nicht. Sie können die Protokolle einsehen, um die Ursache zu ermitteln, indem Sie folgenden Befehl ausführen:

```
tridentctl logs
```

Nachdem Sie das Problem mit der Konfigurationsdatei identifiziert und behoben haben, können Sie den Befehl zum Erstellen erneut ausführen.

Erstellen einer Speicherklasse

Sie können eine Speicherklasse erstellen, um Volumes mit Kerberos-Verschlüsselung bereitzustellen.

Informationen zu diesem Vorgang

Beim Erstellen eines Speicherklassenobjekts können Sie mithilfe der Kerberos-Verschlüsselungsmethode eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung angeben. `mountOptions` Parameter:

- `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-Verschlüsselungsstufe angeben, wird nur die erste Option verwendet. Wenn der in der Speicher-Backend-Konfiguration angegebene Verschlüsselungsgrad von dem im Speicherklassenobjekt angegebenen Grad abweicht, hat das Speicherklassenobjekt Vorrang.

Schritte

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

```
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. Erstellen Sie die Speicherklasse:

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

3. Stellen Sie sicher, dass die Speicherklasse erstellt wurde:

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

   Die Ausgabe sollte in etwa wie folgt aussehen:

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

Bereitstellungsmengen

Nachdem Sie ein Speicher-Backend und eine Speicherklasse erstellt haben, können Sie nun ein Volume bereitstellen. Anweisungen hierzu finden Sie unter "Bereitstellung eines Volumens" .

Konfigurieren der Kerberos-Verschlüsselung während der Übertragung mit Azure NetApp Files -Volumes

Sie können die Kerberos-Verschlüsselung für den Speicherdatenverkehr zwischen Ihrem verwalteten Cluster und einem einzelnen Azure NetApp Files -Speicher-Backend oder einem virtuellen Pool von Azure NetApp Files -Speicher-Backends 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 die `tridentctl` Dienstprogramm.
- Stellen Sie sicher, dass Sie das Azure NetApp Files -Speicher-Backend für die Kerberos-Verschlüsselung vorbereitet haben, indem Sie die Anforderungen beachten und die Anweisungen in [Link einfügen] befolgen. "Azure NetApp Files Dokumentation" .
- Stellen Sie sicher, dass alle NFSv4-Volumes, die Sie mit Kerberos-Verschlüsselung verwenden, korrekt konfiguriert sind. Siehe Abschnitt „NetApp NFSv4-Domänenkonfiguration“ (Seite 13) des "NetApp NFSv4-Erweiterungen und Best Practices-Leitfaden" .

Erstellen Sie ein Speicher-Backend

Sie können eine Azure NetApp Files -Speicher-Backend-Konfiguration erstellen, die die Kerberos-Verschlüsselungsfunktion beinhaltet.

Informationen zu diesem Vorgang

Wenn Sie eine Konfigurationsdatei für das Speicher-Backend erstellen, die die Kerberos-Verschlüsselung konfiguriert, können Sie festlegen, dass diese auf einer von zwei möglichen Ebenen angewendet werden soll:

- Die **Speicher-Backend-Ebene** unter Verwendung der `spec.kerberos` Feld
- Die **virtuelle Poolebene** unter Verwendung der `spec.storage.kerberos` Feld

Wenn Sie die Konfiguration auf Ebene des virtuellen Pools definieren, wird der Pool anhand der Bezeichnung 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 Storage-Backend-Konfigurationsdatei anhand eines der folgenden Beispiele, je nachdem, wo Sie das Storage-Backend definieren müssen (Storage-Backend-Ebene oder Virtual-Pool-Ebene). Ersetzen Sie die Werte in eckigen Klammern <> durch Informationen aus Ihrer Umgebung:

Beispiel auf Speicher-Backend-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 für ein virtuelles Schwimmbecken

```
---
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 im vorherigen Schritt erstellte Konfigurationsdatei, um das Backend zu erstellen:

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

Wenn die Backend-Erstellung fehlschlägt, stimmt etwas mit der Backend-Konfiguration nicht. Sie können die Protokolle einsehen, um die Ursache zu ermitteln, indem Sie folgenden Befehl ausführen:

```
tridentctl logs
```

Nachdem Sie das Problem mit der Konfigurationsdatei identifiziert und behoben haben, können Sie den Befehl zum Erstellen erneut ausführen.

Erstellen einer Speicherklasse

Sie können eine Speicherklasse erstellen, um Volumes mit Kerberos-Verschlüsselung bereitzustellen.

Schritte

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

```
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. Erstellen Sie die Speicherklasse:

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

3. Stellen Sie sicher, dass die Speicherklasse erstellt wurde:

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

Die Ausgabe sollte in etwa wie folgt aussehen:

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

Bereitstellungsmengen

Nachdem Sie ein Speicher-Backend und eine Speicherklasse erstellt haben, können Sie nun ein Volume bereitstellen. Anweisungen hierzu finden Sie unter "Bereitstellung eines Volumens" .