Bewährte Verfahren und Empfehlungen

Trident

NetApp
July 01, 2026

Inhalt

Bewährte Verfahren und Empfehlungen

Bereitstellung

Verwenden Sie die hier aufgeführten Empfehlungen, wenn Sie Trident bereitstellen.

In einem dedizierten Namensraum bereitstellen

"Namensräume"Sie sorgen für eine administrative Trennung zwischen verschiedenen Anwendungen und stellen eine Barriere für die gemeinsame Nutzung von Ressourcen dar. Beispielsweise kann ein PVC aus einem Namespace nicht von einem anderen verwendet werden. Trident stellt PV-Ressourcen allen Namespaces im Kubernetes-Cluster zur Verfügung und nutzt daher ein Servicekonto mit erweiterten 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 nicht die Möglichkeit haben, auf die Trident-Objektdefinitionen oder die Pods selbst zuzugreifen.

Verwenden 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 es dem Administrator, globale sowie speicherklassenspezifische Kapazitäts- und Objektanzahlbeschränkungen pro Namespace zu implementieren. Darüber hinaus stellt die Verwendung eines "Bereichslimit" sicher, dass die PVC-Anfragen sowohl einen minimalen als auch einen maximalen Wert einhalten, bevor die Anfrage an den Provisioner weitergeleitet wird.

Diese Werte werden pro Namensraum definiert, was bedeutet, dass für jeden Namensraum Werte definiert sein sollten, die seinen Ressourcenanforderungen entsprechen. Siehe hier für Informationen über "wie man Quoten nutzt".

Storage-Konfiguration

Jede Speicherplattform im NetApp Portfolio verfügt über einzigartige Funktionen, die Anwendungen zugutekommen, ob containerisiert 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, jedoch sollten bei der Auswahl einer Plattform die Anforderungen der Anwendung und des Teams, das das Gerät verwaltet, berücksichtigt werden.

Sie sollten die grundlegenden Best Practices für das Host-Betriebssystem mit dem Protokoll, das Sie verwenden, beachten. Optional können Sie in Erwägung ziehen, sofern verfügbar, die Best Practices für die Anwendung zusammen mit Backend-, Speicherklassen- und PVC-Einstellungen zu integrieren, um den Speicher für spezifische Anwendungen zu optimieren.

ONTAP und Cloud Volumes ONTAP Best Practices

Lernen Sie die Best Practices für die Konfiguration von ONTAP und Cloud Volumes ONTAP für Trident.

Die folgenden Empfehlungen sind Richtlinien für die Konfiguration von ONTAP für containerisierte Workloads, die Volumes nutzen, die von Trident dynamisch bereitgestellt werden. Jede sollte hinsichtlich ihrer Eignung für Ihre Umgebung geprüft und bewertet werden.

Verwenden Sie SVM(s), 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 von Best Practices zur Begrenzung des Ressourcenverbrauchs.

Für die Verwaltung der SVM stehen mehrere Optionen zur Verfügung:

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

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

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

Begrenzen Sie die maximale Volume-Anzahl

ONTAP-Speichersysteme haben eine maximale Volume-Anzahl, die je nach Softwareversion und Hardwareplattform variiert. Siehe "NetApp Hardware Universe" für Ihre spezifische Plattform und ONTAP-Version, um die genauen Grenzwerte zu bestimmen. Wenn die Volume-Anzahl erschöpft ist, schlagen Bereitstellungsvorgänge nicht nur für Trident, sondern für alle Speicheranforderungen fehl.

Tridents `ontap-nas` und `ontap-san` Treiber stellen ein FlexVolume für jedes erstellte Kubernetes Persistent Volume (PV) bereit. Der `ontap-nas-economy` Treiber erstellt etwa ein FlexVolume für alle 200 PVs (konfigurierbar zwischen 50 und 300). Der `ontap-san-economy` Treiber erstellt etwa ein FlexVolume für alle 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 mehreren 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 verwendet werden

Der `max-volumes` Wert ist die Gesamtanzahl der über alle Nodes im ONTAP Cluster bereitgestellten Volumes und nicht auf einem einzelnen ONTAP Node. Daher kann es vorkommen, dass ein ONTAP Cluster-Node deutlich mehr oder weniger von Trident bereitgestellte Volumes hat als ein anderer Node.

Ein ONTAP-Cluster mit zwei Knoten kann beispielsweise maximal 2000 FlexVol Volumes hosten. Die Festlegung der maximalen Volume-Anzahl auf 1250 erscheint sehr sinnvoll. Wenn jedoch nur "Aggregate" von einem Knoten dem SVM zugewiesen sind oder die Aggregate, die von einem Knoten zugewiesen wurden, nicht bereitgestellt werden können (zum Beispiel aufgrund von Kapazität), wird der andere Knoten zum Ziel für alle von Trident bereitgestellten Volumes. Das bedeutet, dass das Volume-Limit für diesen Knoten möglicherweise erreicht wird, bevor der `max-volumes` Wert erreicht ist, was sowohl Trident als auch andere Volume-Operationen, die diesen Knoten nutzen, beeinträchtigt. **Sie können diese Situation vermeiden, indem Sie sicherstellen, dass Aggregate von jedem Knoten im Cluster dem von Trident verwendeten SVM in gleicher Anzahl zugewiesen werden.**

Ein Volume klonen

NetApp Trident unterstützt das Klonen von Volumes bei Verwendung der `ontap-nas`, `ontap-san` und `solidfire-san` Speichertreiber. Bei Verwendung der `ontap-nas-flexgroup` oder `ontap-nas-economy` Treiber wird das Klonen nicht unterstützt. Das Erstellen eines neuen Volumes aus einem vorhandenen Volume führt zur Erstellung eines neuen Snapshots.

> Vermeiden Sie das Klonen einer PVC, die mit einer anderen StorageClass verknüpft ist. Führen Sie Klonvorgänge innerhalb derselben StorageClass durch, um Kompatibilität zu gewährleisten und unerwartetes Verhalten zu verhindern.

Begrenzen Sie die maximale Größe von Volumes, die von Trident erstellt werden

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

Neben der Kontrolle der Volume-Größe am Speicherarray sollten Sie auch die Kubernetes-Funktionen nutzen.

Begrenzen Sie die maximale Größe der FlexVols, die von Trident erstellt werden

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

Konfigurieren Sie Trident für die Verwendung von bidirektionalem CHAP

Sie können die CHAP-Initiator- und Ziel-Benutzernamen sowie Passwörter in Ihrer Backend-Definition angeben und Trident CHAP auf der SVM aktivieren lassen. Mit dem `useCHAP`-Parameter in Ihrer Backend-Konfiguration authentifiziert Trident 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 durch Trident bereitgestellten Volumes verbrauchbaren IOPS begrenzt. Dies hilft, "einen Tyrannen verhindern"dass ein außer Kontrolle geratener Container keine Workloads außerhalb der Trident SVM

beeinträchtigt.

Sie können in wenigen Schritten eine QoS-Richtlinie für die SVM erstellen. Siehe die Dokumentation für Ihre Version von ONTAP für die genauesten Informationen. 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, wenn Ihre Version von ONTAP dies unterstützt, können Sie die Verwendung eines QoS-Minimums in Betracht ziehen, um einen bestimmten Durchsatz für containerisierte Workloads zu garantieren. Adaptives QoS ist nicht mit einer SVM-Level-Richtlinie kompatibel.

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

- Andere Workloads, die das Speichersystem nutzen. Falls andere Workloads, die nicht mit der Kubernetes-Bereitstellung zusammenhängen, die Speicherressourcen nutzen, ist darauf zu achten, dass diese Workloads nicht versehentlich negativ beeinflusst 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.

Es ist wichtig zu beachten, dass eine auf SVM-Ebene zugewiesene QoS-Richtlinie dazu führt, dass alle für die SVM bereitgestellten Volumes denselben IOPS-Pool nutzen. Wenn eine oder wenige der containerisierten Anwendungen einen hohen IOPS-Bedarf haben, könnten sie zu einem „Bully“ für die anderen containerisierten Workloads werden. Wenn dies der Fall ist, sollten Sie in Erwägung ziehen, externe Automatisierung zu verwenden, um QoS-Richtlinien pro Volume zuzuweisen.

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

QoS-Policy-Gruppen für Trident erstellen

Quality of Service (QoS) gewährleistet, dass die Leistung kritischer Workloads nicht durch konkurrierende Workloads beeinträchtigt wird. ONTAP QoS-Richtliniengruppen bieten QoS-Optionen für Volumes und ermöglichen Benutzern, die Durchsatzobergrenze für einen oder mehrere Workloads festzulegen. Weitere Informationen zu QoS finden Sie unter "Gewährleistung des Durchsatzes mit QoS". Sie können QoS-Richtliniengruppen im Backend oder in einem Speicherpool angeben, und sie werden auf jedes in diesem Pool oder Backend erstellte Volume angewendet.

ONTAP bietet zwei Arten von QoS-Richtliniengruppen: traditionelle und adaptive. Traditionelle Richtliniengruppen bieten einen festen maximalen (oder in späteren Versionen minimalen) Durchsatz in IOPS. Adaptives QoS skaliert den Durchsatz automatisch mit der Workload-Größe und hält das Verhältnis von IOPS zu TB/GB aufrecht, wenn sich die Größe der Workload ändert. Dies bietet einen erheblichen Vorteil, wenn Sie Hunderte oder Tausende von Workloads in einer großen Umgebung verwalten.

Beachten Sie Folgendes, wenn Sie QoS-Richtliniengruppen erstellen:

- Sie sollten den `qosPolicy` Schlüssel im `defaults` Block der Backend-Konfiguration festlegen. 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, sodass jedes Volume den gesamten Durchsatz erhält, wie von der Richtliniengruppe festgelegt. Gemeinsam genutzte Richtliniengruppen werden nicht unterstützt.

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

Beschränken Sie den Zugriff auf Speicherressourcen auf Mitglieder des Kubernetes-Clusters

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 verändern.

Es ist wichtig zu verstehen, dass Namespaces die logische Grenze für Ressourcen in Kubernetes darstellen. Die Annahme ist, dass Ressourcen im selben Namespace gemeinsam genutzt werden können, jedoch gibt es, was wichtig ist, keine Namespace-übergreifende Fähigkeit. Das bedeutet, dass selbst wenn PVs globale Objekte sind, sie, wenn sie an ein PVC gebunden sind, nur von Pods im selben Namespace zugänglich sind. **Es ist entscheidend sicherzustellen, dass Namespaces verwendet werden, um bei Bedarf eine Trennung bereitzustellen.**

Die größte Sorge der meisten Organisationen hinsichtlich 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 darauf ausgelegt, diese Art von Kompromittierung zu verhindern. Es gibt jedoch eine Ausnahme: privilegierte Container.

Ein privilegierter Container ist ein Container, der mit deutlich mehr Host-Berechtigungen als üblich ausgeführt wird. Diese werden nicht standardmäßig verweigert, daher stellen Sie sicher, dass Sie die Fähigkeit mit "Sicherheitsrichtlinien für Pods" deaktivieren.

Für 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. Dies stellt sicher, dass das Speichervolume nur dann zerstört wird, wenn sowohl Kubernetes als auch die externen 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.

Für Bereitstellungen mit dedizierten Infrastrukturknoten (zum Beispiel OpenShift) oder anderen Knoten, die keine Benutzeranwendungen planen können, sollten separate Exportrichtlinien verwendet werden, um den Zugriff auf Speicherressourcen weiter einzuschränken. Dies umfasst die Erstellung einer Exportrichtlinie für Dienste, die auf diesen Infrastrukturknoten bereitgestellt werden (zum Beispiel die OpenShift Metrics- und Logging-Dienste), sowie für Standardanwendungen, die auf Nicht-Infrastrukturknoten bereitgestellt werden.

Verwenden Sie eine dedizierte Exportrichtlinie

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

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

- Verwenden Sie den `vserver export-policy create` ONTAP CLI-Befehl, um die Export-Policy zu erstellen.
- Fügen Sie der Exportrichtlinie Regeln mithilfe des `vserver export-policy rule create` ONTAP CLI-Befehls hinzu.

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

Deaktivieren `showmount` für die Anwendung SVM

Die `showmount` Funktion ermöglicht es einem NFS-Client, die SVM nach einer Liste verfügbarer NFS-Exporte abzufragen. Ein im Kubernetes-Cluster bereitgestellter Pod kann den `showmount -e` Befehl gegen die SVM ausführen und eine Liste der verfügbaren Mounts erhalten, einschließlich solcher, auf die er keinen Zugriff hat. Auch wenn dies für sich genommen kein Sicherheitsrisiko darstellt, liefert es dennoch unnötige Informationen, die einem unbefugten Benutzer potenziell helfen können, eine Verbindung zu einem NFS-Export herzustellen.

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

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

SolidFire Best Practices

Lernen Sie die Best Practices für die Konfiguration von SolidFire-Speicher für Trident.

SolidFire-Konto erstellen

Jedes SolidFire Konto repräsentiert einen eindeutigen Volume-Inhaber und erhält einen eigenen Satz von Challenge-Handshake Authentication Protocol (CHAP)-Anmeldeinformationen. Sie können auf die einem Konto zugewiesenen Volumes entweder mit dem Kontonamen und den entsprechenden CHAP-Anmeldeinformationen oder über eine Volume-Zugriffsgruppe zugreifen. Einem Konto können bis zu zweitausend Volumes zugewiesen 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 Quality of Service-Einstellung erstellen und speichern möchten, die auf viele Volumes angewendet werden kann.

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

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

IOPS-Parameter	Definition	Min. Wert	Standardwert	Max. value (4 KB)
Min. IOPS	Das garantierte Leistungsniveau für ein Volume.	50	50	15000
Max. 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 Node 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 notwendig ist, um die größeren Blockgrößen zu verarbeiten. Mit zunehmender Bandbreite sinkt die Anzahl der IOPS, die das System erreichen kann. Weitere Informationen zu QoS und Leistung finden Sie unter "SolidFire Quality of Service".

SolidFire Authentifizierung

Element unterstützt zwei Methoden für die Authentifizierung: CHAP und Volume Access Groups (VAG). CHAP verwendet das CHAP-Protokoll, um den Host gegenüber dem Backend zu authentifizieren. Volume Access Groups steuern den Zugriff auf die Volumes, die sie bereitstellen. NetApp empfiehlt die Verwendung von CHAP zur Authentifizierung, da es einfacher ist und keine Skalierungsbeschränkungen hat.

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

CHAP-Authentifizierung (Überprüfung, ob der Initiator der beabsichtigte Volume-Benutzer ist) wird nur bei kontobasierter Zugriffskontrolle unterstützt. Wenn Sie CHAP zur Authentifizierung verwenden, stehen zwei Optionen zur Verfügung: unidirektionales CHAP und bidirektionales CHAP. Unidirektionales CHAP authentifiziert den Volume-Zugriff mithilfe des SolidFire-Kontonamens und des 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 anschließend der Host das Volume über den Kontonamen und das Ziel-Geheimnis authentifiziert.

Wenn CHAP nicht aktiviert werden kann und VAGs erforderlich sind, erstellen Sie die Zugriffsgruppe und fügen Sie die Host-Initiatoren und Volumes zur Zugriffsgruppe hinzu. Jeder IQN, den Sie einer Zugriffsgruppe hinzufügen, kann auf jedes Volume in der Gruppe mit oder ohne CHAP-Authentifizierung zugreifen. Wenn der iSCSI-Initiator für die Verwendung von CHAP-Authentifizierung konfiguriert ist, wird die kontobasierte Zugriffskontrolle verwendet. Wenn der iSCSI-Initiator nicht für die Verwendung von CHAP-Authentifizierung konfiguriert ist, wird die Zugriffskontrolle über Volume Access Group verwendet.

Wo finde ich weitere Informationen?

Einige der Best-Practice-Dokumentationen sind unten aufgeführt. Suchen Sie im "NetApp Bibliothek" nach den aktuellsten Versionen.

ONTAP

- "NFS Best Practice and Implementation Guide"
- "SAN-Verwaltung" (für iSCSI)
- "iSCSI Express-Konfiguration für RHEL"

Element Software

- "Konfiguration von SolidFire für Linux"

NetApp HCI

- "NetApp HCI-Bereitstellungsvoraussetzungen"
- "Zugriff auf die NetApp Deployment Engine"

Informationen zu bewährten Anwendungspraktiken

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

Nicht alle Anwendungen verfügen über spezifische Richtlinien, es ist wichtig, mit Ihrem NetApp Team zusammenzuarbeiten und die "NetApp Bibliothek" zu nutzen, um die aktuellste Dokumentation zu finden.

Trident integrieren

Um Trident zu integrieren, müssen die folgenden Design- und Architekturelemente integriert werden: 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 -bereitstellung

Wählen und implementieren Sie einen Backend-Treiber für Ihr Speichersystem.

ONTAP-Backend-Treiber

ONTAP-Backend-Treiber unterscheiden sich durch das verwendete Protokoll und die Art, wie die Volumes auf dem Speichersystem bereitgestellt werden. Daher sollten Sie sorgfältig überlegen, welchen Treiber Sie einsetzen.

Auf einer höheren Ebene gilt: Wenn Ihre Anwendung Komponenten enthält, die gemeinsam genutzten Speicher benötigen (mehrere Pods greifen auf dieselbe PVC zu), sind NAS-basierte Treiber die Standardwahl, während die blockbasierten iSCSI-Treiber den Bedarf an nicht gemeinsam genutztem Speicher abdecken. Wählen Sie das Protokoll basierend auf den Anforderungen der Anwendung und dem Erfahrungsstand der Speicher- und Infrastrukturteams. Allgemein gesprochen gibt es für die meisten Anwendungen kaum Unterschiede zwischen ihnen, sodass die Entscheidung oft davon abhängt, ob gemeinsam genutzter Speicher (bei dem mehr als ein Pod gleichzeitig Zugriff benötigt) erforderlich ist oder nicht.

Die verfügbaren ONTAP Backend-Treiber sind:

- `ontap-nas`: Jeder bereitgestellte PV ist ein vollständiger ONTAP FlexVolume.
- `ontap-nas-economy`: Jeder bereitgestellte PV ist ein Qtree, mit einer konfigurierbaren Anzahl von Qtrees pro FlexVolume (Standard ist 200).
- `ontap-nas-flexgroup`: Jeder PV wird als vollständiger ONTAP FlexGroup bereitgestellt, und alle einem SVM zugewiesenen Aggregate werden verwendet.
- `ontap-san`: Jeder bereitgestellte PV ist eine LUN innerhalb seines eigenen FlexVolume.
- `ontap-san-economy`: Jedes bereitgestellte PV ist eine LUN, mit einer konfigurierbaren Anzahl von LUNs pro FlexVolume (Standardwert ist 100).

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

Beachten Sie, dass in den folgenden Tabellen nicht alle Funktionen über Trident verfügbar sind. Einige müssen vom Speicheradministrator nach der Bereitstellung angewendet werden, falls diese Funktionalität gewünscht ist. Die hochgestellten Fußnoten kennzeichnen die Funktionalität pro Feature und Treiber.

ONTAP NAS-Treiber	Snapshots	Klone	Dynamische Exportrichtlinien	Multi-Attach	QoS	Größe ändern	Replication
`ontap-nas`	Ja	Ja	JaFußnote:5[]	Ja	JaFußnote:1[]	Ja	JaFußnote:1[]
`ontap-nas-economy`	NO [3]	NO [3]	JaFußnote:5[]	Ja	NO [3]	Ja	NO [3]
`ontap-nas-flexgroup`	JaFußnote:1[]	NEIN	JaFußnote:5[]	Ja	JaFußnote:1[]	Ja	JaFußnote:1[]

Trident bietet 2 SAN-Treiber für ONTAP, deren Fähigkeiten unten gezeigt werden.

ONTAP SAN-Treiber	Snapshots	Klone	Multi-Attach	Bidirektionales CHAP	QoS	Größe ändern	Replication
`ontap-san`	Ja	Ja	JaFußnote:4[]	Ja	JaFußnote:1[]	Ja	JaFußnote:1[]
`ontap-san-economy`	Ja	Ja	JaFußnote:4[]	Ja	NO [3]	Ja	NO [3]

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

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

Wie wir in den obigen Tabellen sehen können, ist vieles der Funktionalität zwischen dem `ontap-nas` und dem `ontap-nas-economy` gleich. Da jedoch der `ontap-nas-economy` Treiber die Möglichkeit einschränkt, den Zeitplan auf PV-Granularität zu steuern, kann dies insbesondere Ihre Notfallwiederherstellungs- und Backup-Planung beeinflussen. Für Entwicklungsteams, die die PVC-Klonfunktionalität auf ONTAP-Speicher nutzen möchten, ist dies nur möglich, wenn sie die `ontap-nas`, `ontap-san` oder `ontap-san-economy` Treiber verwenden.

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

Cloud Volumes ONTAP Backend-Treiber

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

Amazon FSx for ONTAP Backend-Treiber

Amazon FSx for NetApp ONTAP ermöglicht es Ihnen, NetApp-Funktionen, Leistung und Verwaltungsfunktionen zu nutzen, mit denen Sie vertraut sind, während Sie gleichzeitig von der Einfachheit, Agilität, Sicherheit und Skalierbarkeit der Datenspeicherung auf AWS profitieren. FSx for ONTAP unterstützt viele ONTAP-Dateisystemfunktionen und Verwaltungs-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` 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 gestalten möchten, dass spezifische QoS-Grenzwerte für die von Trident bereitgestellten Volumes festgelegt werden, verwenden Sie den `type` Parameter in der Backend-Datei. Der Administrator kann außerdem die Volume-Größe, die auf dem Speicher erstellt werden kann, mit dem `limitVolumeSize` Parameter beschränken. Derzeit werden Element-Speicherfunktionen wie Volume-Resize und Volume-Replikation nicht über den `solidfire-san` Treiber unterstützt. Diese Vorgänge sollten manuell über die Element Software Web-Oberfläche durchgeführt werden.

SolidFire Treiber	Snapshots	Klone	Multi-Attach	CHAP	QoS	Größe ändern	Replication
`solidfire-san`	Ja	Ja	JaFußnote:2[]	Ja	Ja	Ja	JaFußnote:1[]

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

Azure NetApp Files-Backend-Treiber

Trident verwendet den `azure-netapp-files`-Treiber, um den "Azure NetApp Files"-Dienst zu verwalten.

Weitere Informationen zu diesem Treiber und wie Sie ihn konfigurieren können, finden Sie in "Trident Backend-Konfiguration für Azure NetApp Files".

Azure NetApp Files-Treiber	Snapshots	Klone	Multi-Attach	QoS	Erweitern	Replication
`azure-netapp-files`	Ja	Ja	Ja	Ja	Ja	JaFußnote:1[]

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

Speicherklassendesign

Einzelne Speicherklassen 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

Innerhalb eines bestimmten Speicherklassenobjekts kann mithilfe von Filtern festgelegt werden, welcher Speicherpool oder welche Speicherpools für diese bestimmte Speicherklasse verwendet werden sollen. Drei

Filtergruppen können in der Speicherklasse festgelegt werden: `storagePools`, `additionalStoragePools`, und/oder `excludeStoragePools`.

Der `storagePools` Parameter hilft, den Speicher auf die Menge der Pools zu beschränken, die mit beliebigen angegebenen Attributen übereinstimmen. Der `additionalStoragePools` Parameter wird verwendet, um die Menge der Pools, die Trident für die Bereitstellung verwendet, zusammen mit der durch die Attribute und `storagePools` Parameter ausgewählten Menge von Pools zu erweitern. Sie können entweder einen der beiden Parameter allein oder beide zusammen verwenden, um sicherzustellen, dass die geeignete Menge an Speicherpools ausgewählt wird.

Der `excludeStoragePools`Parameter wird verwendet, um die aufgelistete Gruppe von Pools, die den Attributen entsprechen, gezielt auszuschließen.

QoS-Richtlinien emulieren

Wenn Sie Storage Classes entwerfen möchten, um Quality of Service-Richtlinien zu emulieren, erstellen Sie eine Storage Class mit dem `media` Attribut als `hdd` oder `ssd`. Basierend auf dem `media` Attribut, das in der Storage Class angegeben ist, wählt Trident das passende Backend aus, das `hdd` oder `ssd` Aggregate bereitstellt, um das Media-Attribut abzugleichen, und leitet dann die Bereitstellung der Volumes auf das spezifische Aggregat weiter. Daher können wir eine Storage Class PREMIUM erstellen, bei der das `media` Attribut als `ssd` gesetzt ist, was als PREMIUM QoS-Richtlinie klassifiziert werden kann. Wir können eine weitere Storage Class STANDARD erstellen, bei der das Media-Attribut auf `hdd` gesetzt ist, was als STANDARD QoS-Richtlinie klassifiziert werden kann. Wir könnten auch das ``IOPS'' Attribut in der Storage Class verwenden, um die Bereitstellung auf ein Element Appliance umzuleiten, das als QoS-Richtlinie definiert werden kann.

Backend basierend auf spezifischen Funktionen nutzen

Speicherklassen können so konzipiert werden, dass sie die Volume-Bereitstellung auf einem bestimmten Backend steuern, 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 der erforderlichen aktivierten Funktion angeben.

Virtuelle Pools

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

Virtuelle Pools ermöglichen es einem Administrator, eine Abstraktionsebene über Backends zu erstellen, die über Storage Classes referenziert werden können, um mehr Flexibilität und eine effiziente Platzierung von Volumes auf den Backends zu erreichen. Verschiedene Backends können mit derselben Serviceklasse definiert werden. Außerdem können mehrere Speicherpools auf demselben Backend, aber mit unterschiedlichen Eigenschaften erstellt werden. Wenn eine Storage Class mit einem Selektor mit den spezifischen Labels konfiguriert wird, wählt Trident ein Backend aus, das allen Selektor-Labels entspricht, um das Volume zu platzieren. Wenn die Selektor-Labels der Storage Class mit mehreren Speicherpools übereinstimmen, wählt Trident einen davon aus, um das Volume bereitzustellen.

Design des virtuellen Pools

Beim Erstellen eines Backends können Sie üblicherweise eine Reihe von Parametern festlegen. Es war dem Administrator nicht möglich, ein weiteres Backend mit denselben Speicherzugangsdaten und einem anderen Parametersatz zu erstellen. Mit der Einführung virtueller Pools wurde dieses Problem behoben. Ein virtueller Pool ist eine Abstraktionsebene, die zwischen dem Backend und der Kubernetes Storage Class eingeführt wurde, sodass der Administrator Parameter zusammen mit Labels definieren kann, die über Kubernetes

Storage Classes als Selektor backendunabhängig referenziert werden können. Virtuelle Pools können für alle unterstützten NetApp Backends mit Trident definiert werden. Diese Liste umfasst SolidFire/NetApp HCI, ONTAP sowie Azure NetApp Files.

Bei der Definition virtueller Pools wird empfohlen, die Reihenfolge bestehender virtueller Pools in einer Backend-Definition nicht zu ändern. Es ist außerdem ratsam, Attribute eines bestehenden virtuellen Pools nicht zu bearbeiten oder zu ändern und stattdessen einen neuen virtuellen Pool zu definieren.

Emulieren verschiedener Servicelevel/QoS

Es ist möglich, virtuelle Pools zur Emulation von Dienstklassen zu entwerfen. Anhand der Implementierung virtueller Pools für Cloud Volume Service für Azure NetApp Files untersuchen wir, wie wir verschiedene Dienstklassen einrichten können. Konfigurieren Sie das Azure NetApp Files-Backend mit mehreren Labels, die unterschiedliche Leistungsstufen repräsentieren. Setzen Sie den `servicelevel` Aspekt auf die entsprechende Leistungsstufe und fügen Sie unter jedem Label weitere erforderliche Aspekte hinzu. Erstellen Sie nun verschiedene Kubernetes Storage Classes, die jeweils unterschiedlichen virtuellen Pools zugeordnet werden. Mit dem `parameters.selector` Feld gibt jede StorageClass an, welche virtuellen Pools zum Hosten eines Volumes verwendet werden können.

Zuweisung eines bestimmten Satzes von Aspekten

Aus einem einzigen Storage-Backend lassen sich mehrere virtuelle Pools mit jeweils spezifischen Aspekten erstellen. Konfigurieren Sie dazu das Backend mit mehreren Labels und legen Sie unter jedem Label die benötigten Aspekte fest. Erstellen Sie anschließend verschiedene Kubernetes Storage Classes, indem Sie das `parameters.selector` Feld verwenden, das den verschiedenen virtuellen Pools zugeordnet wird. Die auf dem Backend bereitgestellten Volumes enthalten dann die im jeweiligen virtuellen Pool definierten Aspekte.

PVC-Eigenschaften, die die Speicherbereitstellung beeinflussen

Einige Parameter außerhalb der angeforderten Speicherklasse können den Trident-Bereitstellungsentscheidungsprozess bei der Erstellung eines PVC beeinflussen.

Zugriffsmodus

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

Trident versucht, das verwendete Speicherprotokoll der angegebenen Zugriffsmethode gemäß der folgenden Matrix zuzuordnen. Dies ist unabhängig von der zugrunde liegenden Speicherplattform.

	ReadWriteOnce	ReadOnlyMany	ReadWriteMany
iSCSI	Ja	Ja	Ja (Rohblock)
NFS	Ja	Ja	Ja

Eine Anfrage für eine 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 Zugriffsmodus verwenden, der für seine Anwendung geeignet ist.

Volumenoperationen

Persistente Volumes ändern

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

Kubernetes in-tree Provisioner unterstützen derzeit keine Größenänderung von 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 bedarfsgesteuerte Erstellung von Volume-Snapshots und die Erstellung von PVCs aus Snapshots mithilfe des CSI-Frameworks. Snapshots bieten eine komfortable Methode zur Verwaltung zeitpunktgenauer Kopien der Daten und haben einen vom Quell-PV in Kubernetes unabhängigen Lebenszyklus. Diese Snapshots können zum Klonen von PVCs verwendet werden.

Volumes aus Snapshots erstellen

Trident unterstützt auch die Erstellung von PersistentVolumes aus Volume-Snapshots. Dazu erstellen Sie einfach eine PersistentVolumeClaim und geben den `datasource` gewünschten Snapshot an, aus dem das Volume erstellt werden soll. Trident wird diese PVC verarbeiten, indem ein Volume mit den auf dem Snapshot vorhandenen Daten erstellt wird. Mit dieser Funktion ist es möglich, Daten regionsübergreifend zu duplizieren, Testumgebungen zu erstellen, ein beschädigtes oder beschädigtes Produktionsvolume vollständig zu ersetzen oder bestimmte Dateien und Verzeichnisse abzurufen und auf ein anderes angeschlossenes Volume zu übertragen.

Verschieben Sie Volumes im Cluster

Speicheradministratoren haben die Möglichkeit, Volumes zwischen Aggregaten und Controllern im ONTAP Cluster unterbrechungsfrei für den Speicherkonsumenten zu verschieben. Dieser Vorgang hat keine Auswirkungen auf Trident oder den Kubernetes-Cluster, solange das Zielaggregat eines ist, auf das die von Trident verwendete SVM Zugriff hat. Wichtig ist, dass, wenn das Aggregat neu zur SVM hinzugefügt wurde, das Backend durch erneutes Hinzufügen zu Trident aktualisiert werden muss. Dadurch wird Trident veranlasst, die SVM neu zu inventarisieren, sodass das neue Aggregat erkannt wird.

Das Verschieben von Volumes zwischen Backends wird von Trident nicht automatisch unterstützt. Dies gilt für Verschiebungen zwischen SVMs im selben Cluster, zwischen Clustern oder auf eine andere 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. Dadurch können Benutzer ihre Volumes direkt über die Kubernetes-Schicht anpassen. Die Volume-Erweiterung ist für alle gängigen NetApp Speicherplattformen möglich, einschließlich ONTAP und SolidFire/NetApp HCI-Backends. Um eine spätere

Erweiterung zu ermöglichen, setzen Sie `allowVolumeExpansion` auf `true` in Ihrer StorageClass, die dem Volume zugeordnet ist. Wann immer das Persistent Volume vergrößert werden muss, bearbeiten Sie die `spec.resources.requests.storage` Annotation im Persistent Volume Claim auf die gewünschte Volume-Größe. Trident kümmert sich dann automatisch um die Größenänderung des Volumes im Speichercluster.

Ein vorhandenes Volume in Kubernetes importieren

Der Volume-Import ermöglicht das Importieren eines vorhandenen Speichervolumes in eine Kubernetes-Umgebung. Dies wird derzeit von den `ontap-nas`, `ontap-nas-flexgroup`, `solidfire-san` und `azure-netapp-files` Treibern unterstützt. Diese Funktion ist nützlich beim Portieren einer bestehenden Anwendung nach Kubernetes oder während Notfallwiederherstellungsszenarien.

Bei Verwendung der ONTAP- und `solidfire-san` Treiber verwenden Sie den Befehl `tridentctl import volume <backend-name> <volume-name> -f /path/pvc.yaml`, um ein vorhandenes Volume in Kubernetes zu importieren, damit es von Trident verwaltet wird. Die im Import-Volume-Befehl verwendete PVC-YAML- oder JSON-Datei verweist auf eine Storage-Class, die Trident als Provisioner identifiziert. Bei Verwendung eines NetApp HCI/SolidFire Backends stellen Sie sicher, dass die Volume-Namen eindeutig sind. Wenn die Volume-Namen doppelt vorhanden sind, klonen Sie das Volume unter einem eindeutigen Namen, damit die Volume-Importfunktion zwischen ihnen unterscheiden kann.

Wenn der `azure-netapp-files` Treiber verwendet wird, verwenden Sie den Befehl `tridentctl import volume <backend-name> <volume path> -f /path/pvc.yaml`, um das Volume in Kubernetes zu importieren, damit es von Trident verwaltet wird. Dadurch wird eine eindeutige Volume-Referenz sichergestellt.

Wenn der oben stehende Befehl ausgeführt wird, findet Trident das Volume im Backend und liest dessen Größe aus. Es wird automatisch die konfigurierte Größe des PVC-Volumes hinzugefügt (und bei Bedarf überschrieben). Anschließend erstellt Trident das neue PV und Kubernetes bindet das PVC an das PV.

Wenn ein Container so bereitgestellt wurde, dass er die spezifische importierte PVC benötigt, bleibt er im Status „Ausstehend“, bis das PVC/PV-Paar über den Volume-Importprozess gebunden ist. Nachdem das PVC/PV-Paar gebunden ist, sollte der Container starten, sofern keine weiteren Probleme auftreten.

Registrierungsdienst

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

Protokollierungsdienst

Wie andere OpenShift-Dienste wird der Protokollierungsdienst mithilfe von Ansible mit den in der Inventardatei, auch Hosts genannt, bereitgestellten Konfigurationsparametern bereitgestellt, die dem Playbook übergeben wird. Es gibt zwei Installationsmethoden, die behandelt werden: die Bereitstellung der Protokollierung während der anfänglichen OpenShift-Installation und die Bereitstellung der Protokollierung, nachdem OpenShift installiert wurde.

> Ab Red Hat OpenShift Version 3.9 empfiehlt die offizielle Dokumentation NFS für den Protokollierungsdienst nicht zu verwenden, aufgrund von Bedenken hinsichtlich Datenbeschädigung. Dies basiert auf Red Hat Tests ihrer Produkte. 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, aber beide funktionieren hervorragend mit NetApp Plattformen und es gibt keinen Grund, NFS zu vermeiden, wenn dies Ihre Präferenz ist.

Wenn Sie NFS mit dem Protokollierungsdienst verwenden, müssen Sie die Ansible-Variable

`openshift_enable_unsupported_configurations` auf `true` setzen, um zu verhindern, dass die Installation fehlschlägt.

Los geht's

Der Protokollierungsdienst kann optional sowohl für Anwendungen als auch für die Kernoperationen des OpenShift-Clusters bereitgestellt werden. Wenn Sie sich entscheiden, die Protokollierung für den Betrieb bereitzustellen, indem Sie die Variable `openshift_logging_use_ops` als `true` angeben, werden zwei Instanzen des Dienstes erstellt. Die Variablen, die die Protokollierungsinstanz für den Betrieb steuern, enthalten „ops“, während die Instanz für Anwendungen dies nicht tut.

Die Konfiguration der Ansible-Variablen entsprechend der Bereitstellungsmethode ist wichtig, um sicherzustellen, dass der korrekte Speicher von den zugrunde liegenden Diensten genutzt wird. Sehen wir uns die Optionen für jede der Bereitstellungsmethoden an.

> ⓘ Die folgenden Tabellen enthalten ausschließlich die für die Speicherkonfiguration im Zusammenhang mit dem Protokollierungsdienst relevanten Variablen. Weitere Optionen finden Sie in "Red Hat OpenShift Protokollierungsdokumentation", die Sie prüfen, konfigurieren und entsprechend Ihrer Bereitstellung verwenden sollten.

Die Variablen in der folgenden Tabelle führen dazu, dass das Ansible-Playbook ein PV und ein PVC für den Protokollierungsdienst anhand der angegebenen Details erstellt. Diese Methode ist deutlich weniger flexibel als die Verwendung des Playbooks zur Komponenteninstallation nach der OpenShift-Installation, jedoch ist sie eine Option, wenn bereits Volumes verfügbar sind.

Variable	Details
`openshift_logging_storage_kind`	Setzen Sie `nfs` , damit das Installationsprogramm ein NFS-PV für den Protokollierungsdienst erstellt.
`openshift_logging_storage_host`	Der Hostname oder die IP-Adresse des NFS-Hosts. Dies sollte auf die dataLIF für Ihre virtuelle Maschine eingestellt werden.
`openshift_logging_storage_nfs_directory`	Der Mount-Pfad für den NFS-Export. Wenn das Volume beispielsweise als `/openshift_logging` eingebunden ist, verwenden Sie diesen Pfad für diese Variable.
`openshift_logging_storage_volume_name`	Der Name, z. B. `pv_ose_logs`, des zu erstellenden PV.
`openshift_logging_storage_volume_size`	Die Größe des NFS-Exports, zum Beispiel `100Gi`.

Wenn Ihr OpenShift-Cluster bereits läuft und somit Trident bereitgestellt und konfiguriert wurde, kann das Installationsprogramm die Volumes mithilfe der dynamischen Bereitstellung erstellen. Die folgenden 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`	Der Name der Speicherklasse, die im PVC verwendet wird.

Variable	Details
`openshift_logging_es_pvc_size`	Die im PVC angeforderte Größe des Volumens.
`openshift_logging_es_pvc_prefix`	Ein Präfix für die von dem Protokollierungsdienst verwendeten PVCs.
`openshift_logging_es_ops_pvc_dynamic`	Auf `true` setzen, um dynamisch bereitgestellte Volumes für die Ops-Protokollierungsinstanz zu verwenden.
`openshift_logging_es_ops_pvc_storage_class_name`	Der Name der Speicherklasse für die Protokollierungsinstanz.
`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 ops-Instanz.

Stellen Sie den Protokollierungs-Stack bereit

Wenn Sie die Protokollierung als Teil 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 abgeschlossen ist.

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

Metrikdienst

Der Metrikdienst liefert dem Administrator wertvolle Informationen über Status, Ressourcenauslastung und Verfügbarkeit des OpenShift Clusters. Er ist außerdem für die automatische Pod-Skalierung erforderlich und viele Organisationen nutzen die Daten des Metrikdienstes für ihre Kostenverrechnungs- und/oder Kostenanzeigeanwendungen.

Wie beim Protokollierungsdienst und bei OpenShift insgesamt wird Ansible verwendet, um den Metrikdienst bereitzustellen. Ebenso wie der Protokollierungsdienst kann der Metrikdienst entweder 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 folgenden Tabellen enthalten nur die Variablen, die für die Speicherkonfiguration im Zusammenhang mit dem Metrics Service relevant sind. In der Dokumentation finden Sie viele weitere Optionen, die geprüft, konfiguriert und entsprechend Ihrer Implementierung verwendet werden sollten.

Variable	Details
`openshift_metrics_storage_kind`	Setzen Sie `nfs` , damit das Installationsprogramm ein NFS-PV für den Protokollierungsdienst erstellt.
`openshift_metrics_storage_host`	Der Hostname oder die IP-Adresse des NFS-Hosts. Dieser Wert sollte auf die dataLIF für Ihre SVM eingestellt werden.

Variable	Details
`openshift_metrics_storage_nfs_directory`	Der Mount-Pfad für den NFS-Export. Wenn das Volume beispielsweise als `/openshift_metrics` eingebunden ist, verwenden Sie diesen Pfad für diese Variable.
`openshift_metrics_storage_volume_name`	Der Name, z. B. `pv_ose_metrics`, des zu erstellenden PV.
`openshift_metrics_storage_volume_size`	Die Größe des NFS-Exports, zum Beispiel `100Gi`.

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

Variable	Details
`openshift_metrics_cassandra_pvc_prefix`	Ein Präfix, das für die Metrik-PVCs verwendet werden soll.
`openshift_metrics_cassandra_pvc_size`	Die Größe der anzufordernden Volumes.
`openshift_metrics_cassandra_storage_type`	Der Typ des Speichers, der für Metriken verwendet werden soll, muss auf dynamisch gesetzt werden, damit Ansible PVCs mit der entsprechenden Speicherklasse erstellt.
`openshift_metrics_cassanda_pvc_storage_class_name`	Der Name der zu verwendenden Speicherklasse.

Stellen Sie den Metrikdienst bereit

Mit den entsprechenden Ansible-Variablen, die in Ihrer Hosts/Inventory-Datei definiert sind, stellen Sie den Dienst mit Ansible bereit. Wenn Sie während der OpenShift-Installation bereitstellen, wird das PV automatisch erstellt und verwendet. Wenn Sie mit den Komponenten-Playbooks nach der OpenShift-Installation bereitstellen, erstellt Ansible alle benötigten PVCs und nachdem Trident Speicher dafür bereitgestellt hat, wird der Dienst bereitgestellt.

Die oben genannten Variablen und der Bereitstellungsprozess können sich mit jeder Version von OpenShift ändern. Stellen Sie sicher, dass Sie "Red Hat's OpenShift Implementierungs-Leitfaden" für Ihre Version überprüfen und befolgen, damit diese für Ihre Umgebung konfiguriert ist.

Datenschutz und Notfallwiederherstellung

Informieren Sie sich über die Schutz- und Wiederherstellungsoptionen für Trident und Volumes, die mit Trident erstellt wurden. Sie sollten für jede Anwendung mit Persistenzanforderung eine Strategie zur Datensicherung und Wiederherstellung 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 das etcd des Kubernetes-Clusters mit "Kubernetes: Sichern eines etcd-Clusters".
2. Platzieren Sie die Sicherungsdateien auf einem FlexVol volume

> NetApp empfiehlt, die SVM, in der sich die FlexVol befindet, mit einer SnapMirror Beziehung zu einer anderen SVM zu schützen.

Trident Wiederherstellung

Mithilfe von Kubernetes-CRDs und dem etcd-Snapshot des Kubernetes-Clusters können Sie Trident wiederherstellen.

Schritte

1. Vom Ziel-SVM aus binden Sie das Volume, das die Kubernetes etcd-Datendateien und Zertifikate enthält, auf dem Host ein, 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 mithilfe von "Kubernetes: Wiederherstellen eines etcd-Clusters" wieder her.
4. Führen Sie `kubectl get crd` aus, um zu überprüfen, ob alle Trident benutzerdefinierten Ressourcen geladen wurden, und rufen Sie die Trident Objekte ab, um zu prüfen, ob alle Daten verfügbar sind.

SVM-Replikation und -Wiederherstellung

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

Im Katastrophenfall können Sie die SnapMirror Ziel-SVM aktivieren, um die Datenbereitstellung aufzunehmen. Sie können wieder auf die primäre SVM umschalten, wenn die Systeme wiederhergestellt sind.

Über diese Aufgabe

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

- Sie sollten für jede SVM mit aktiviertem SVM-DR ein eigenes 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 die zusätzlichen Kosten und die Komplexität verstehen, die mit der Replikation verbunden sind, und ihren Wiederherstellungsplan sorgfältig prüfen, bevor sie mit diesem Prozess beginnen.

SVM-Replikation

Sie können "ONTAP: SnapMirror SVM-Replikation" verwenden, um die SVM-Replikationsbeziehung zu erstellen.

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

- "-identity-preserve true" repliziert die gesamte SVM-Konfiguration.
- "-discard-configs Netzwerk" schließt LIFs und zugehörige Netzwerkeinstellungen aus.
- "-identity-preserve false" Repliziert werden nur die Volumes und die Sicherheitskonfiguration.

SVM-Wiederherstellung mit Trident

Trident erkennt SVM-Ausfälle nicht automatisch. Im Katastrophenfall kann der Administrator das Trident Failover auf die neue SVM manuell 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 `-identity-preserve false` oder `-discard-config network` bei der Konfiguration Ihrer SVM-Replikation angegeben haben, aktualisieren Sie 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. Das Weglassen von `storagePrefix` führt dazu, 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 `-identity-preserve false` oder `discard-config network` angegeben haben, müssen Sie alle Anwendungspods neu starten.

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

Volumenreplikation und Wiederherstellung

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

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

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

Snapshot-Datenschutz

Sie können Daten mit folgenden Methoden schützen und wiederherstellen:

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

  "Volume Snapshots"

- ONTAP Snapshots, um den gesamten Inhalt eines Volumes wiederherzustellen oder einzelne Dateien oder LUNs wiederherzustellen.

  "ONTAP Snapshots"

Automatisierung des Failovers von zustandsbehafteten Anwendungen mit Trident

Die Force-Detach-Funktion von Trident ermöglicht es Ihnen, Volumes automatisch von fehlerhaften Knoten in einem Kubernetes-Cluster zu trennen, wodurch Datenbeschädigung verhindert und die Anwendungsverfügbarkeit sichergestellt wird. Diese Funktion ist besonders nützlich in Szenarien, in denen Knoten nicht mehr reagieren oder für Wartungsarbeiten offline genommen werden.

Details zum erzwungenen Abtrennen

Die erzwungene Trennung ist für `ontap-san`, `ontap-san-economy`, `ontap-nas` und `ontap-nas-economy` verfügbar. Bevor Sie die erzwungene Trennung aktivieren, muss das nicht-graceful node shutdown (NGNS) im Kubernetes-Cluster aktiviert sein. NGNS ist standardmäßig für Kubernetes 1.28 und höher aktiviert. Weitere Informationen finden sich unter "Kubernetes: Nicht ordnungsgemäßes Herunterfahren eines Knotens".

> Bei Verwendung des `ontap-nas` oder `ontap-nas-economy`-Treibers müssen Sie den `autoExportPolicy`-Parameter in der Backend-Konfiguration auf `true` setzen, damit Trident den Zugriff vom Kubernetes-Knoten mit dem angewendeten Taint mithilfe verwalteter Exportrichtlinien einschränken kann.

> Da Trident auf Kubernetes NGNS basiert, sollten Sie `out-of-service`Taints von einem fehlerhaften Knoten erst dann entfernen, wenn alle nicht tolerierbaren Workloads neu geplant wurden. Das unbedachte Anwenden oder Entfernen von Taints kann den Schutz der Backend-Daten gefährden.

Wenn der Kubernetes-Clusteradministrator den `node.kubernetes.io/out-of-service=nodeshutdown:NoExecute` Taint auf den Knoten angewendet hat und `enableForceDetach` auf `true` gesetzt ist, ermittelt Trident den Knotenstatus und:

1. Stoppen Sie den Backend-I/O-Zugriff für Volumes, die an diesem Node gemountet sind.
2. Markieren Sie das Trident node object als `dirty` (nicht sicher für neue Veröffentlichungen).

> Der Trident-Controller lehnt neue Veröffentlichungsanforderungen für Volumes ab, bis der Knoten als `dirty`vom Trident-Knotenpod erneut qualifiziert wurde. Alle Workloads, die mit einem eingebundenen PVC geplant sind (auch nachdem der Clusterknoten fehlerfrei und bereit ist), werden nicht akzeptiert, bis Trident den Knoten `clean` (sicher für neue Veröffentlichungen) verifizieren kann.

Wenn die Knotenintegrität wiederhergestellt ist und die Taint entfernt wurde, wird Trident:

1. Identifizieren und bereinigen Sie veraltete veröffentlichte Pfade auf dem Node.
2. Wenn sich der Knoten in einem `cleanable` Zustand befindet (die Außerbetriebnahme-Warnung wurde entfernt und der Knoten befindet sich im `Ready` Zustand) und alle veralteten, veröffentlichten Pfade sauber sind, wird Trident den Knoten als `clean` wieder zulassen und neue veröffentlichte Volumes auf dem Knoten erlauben.

Details zum automatischen Failover

Sie können den Prozess der erzwungenen Trennung durch die Integration mit "Node Health Check (NHC) Operator" automatisieren. Wenn ein Knotenausfall auftritt, löst NHC die Trident-Knotenbehebung (TNR) und die erzwungene Trennung automatisch aus, indem ein TridentNodeRemediation CR im Trident-Namensraum erstellt wird, der den ausgefallenen Knoten definiert. TNR wird nur bei einem Knotenausfall erstellt und von NHC entfernt, sobald der Knoten wieder online ist oder gelöscht wurde.

Fehlgeschlagener Node-Pod-Entfernungsprozess

Automated-failover wählt die Workloads aus, die vom ausgefallenen Knoten entfernt werden sollen. Wenn ein TNR erstellt wird, markiert der TNR-Controller den Knoten als dirty, verhindert die Veröffentlichung neuer Volumes und beginnt mit dem Entfernen von Force-Detach-unterstützten Pods und deren Volume-Anhängen.

Alle von Force-Detach unterstützten Volumes/PVCs werden auch von Automated-Failover unterstützt:

- NAS- und NAS-economy-Volumes unter Verwendung von Auto-Export-Richtlinien (SMB wird noch nicht unterstützt).
- SAN- und SAN-economy-Volumes.

Siehe Details zum erzwungenen Abtrennen.

Standardverhalten:

- Pods, die von force-detach unterstützte Volumes verwenden, werden vom ausgefallenen Knoten entfernt. Kubernetes wird diese auf einem fehlerfreien Knoten neu einplanen.
- Pods, die ein von force-detach nicht unterstütztes Volume verwenden, einschließlich nicht-Trident-Volumes, werden nicht vom ausgefallenen Knoten entfernt.
- Stateless Pods (nicht PVCs) werden nicht vom ausgefallenen Knoten entfernt, es sei denn, die Pod-Annotation `trident.netapp.io/podRemediationPolicy: delete` gesetzt ist.

Überschreiben des Pod-Entfernungsverhaltens:

Das Verhalten bei der Pod-Entfernung kann mithilfe einer Pod-Annotation angepasst werden: `trident.netapp.io/podRemediationPolicy[retain, delete]`. Diese Annotationen werden geprüft und verwendet, wenn ein Failover auftritt. Wenden Sie Annotationen auf die Kubernetes Deployment/ReplicaSet Pod-Spezifikation an, um zu verhindern, dass die Annotation nach einem Failover verschwindet:

- `retain` - Der Pod wird während eines automatischen Failovers NICHT vom ausgefallenen Knoten entfernt.
- `delete` - Der Pod wird bei einem automatischen Failover vom ausgefallenen Knoten entfernt.

Diese Annotationen können auf jeden Pod angewendet werden.

- E/A-Operationen werden nur auf ausgefallenen Knoten für Volumes blockiert, die force-detach unterstützen.
- Für Volumes, die das erzwungene Trennen nicht unterstützen, besteht das Risiko von Datenbeschädigung und Multi-Attach-Problemen.

TridentNodeRemediation CR

Der TridentNodeRemediation (TNR) CR definiert einen ausgefallenen Knoten. Der Name des TNR ist der Name des ausgefallenen Knotens.

Beispiel TNR:

```
apiVersion: trident.netapp.io/v1
kind: TridentNodeRemediation
metadata:
  name: <K8s-node-name>
spec: {}
```

TNR states: Verwenden Sie die folgenden Befehle, um den Status der TNRs anzuzeigen:
`kubectl get tnr <name> -n <trident-namespace>`

TNRs können sich in einem der folgenden Zustände befinden:

- *Behebung*:
  - Den Backend-E/A-Zugriff für Volumes, die von force-detach unterstützt und an diesen Knoten angehängt wurden, einstellen.
  - Das Trident-Knotenobjekt ist als „dirty“ markiert (nicht sicher für neue Veröffentlichungen).
  - Entfernen Sie Pods und Volume-Anhänge vom Knoten
- *NodeRecoveryPending*:
  - Der Controller wartet darauf, dass der Knoten wieder online geht.
  - Sobald der Knoten online ist, stellt publish-enforcement sicher, dass der Knoten sauber und bereit für neue Volume-Veröffentlichungen ist.
- Wenn der Knoten aus K8s gelöscht wird, entfernt der TNR-Controller den TNR und stellt die Abstimmung ein.
- *Erfolgreich*:
  - Alle Sanierungs- und Wiederherstellungsmaßnahmen wurden erfolgreich abgeschlossen. Der Knoten ist bereinigt und bereit für neue Volume-Veröffentlichungen.
- *Fehlgeschlagen*:
  - Nicht behebbarer Fehler. Fehlergründe sind im Feld status.message des CR festgelegt.

Automatisches Failover aktivieren

Voraussetzungen:

- Stellen Sie sicher, dass die erzwungene Trennung aktiviert ist, bevor Sie das automatische Failover aktivieren. Weitere Informationen finden sich unter Details zum erzwungenen Abtrennen.

- Installieren Sie Node Health Check (NHC) im Kubernetes-Cluster.
  - "Installiere operator-sdk".
  - Installieren Sie Operator Lifecycle Manager (OLM) im Cluster, falls noch nicht installiert: `operator-sdk olm install`.
  - Installieren Sie den Node Health check Operator: `kubectl create -f https://operatorhub.io/install/node-healthcheck-operator.yaml`.

Sie können auch alternative Methoden zur Erkennung von Knotenausfällen verwenden, wie im [Integrating Custom Node Health Check Solutions] Abschnitt unten angegeben.

Weitere Informationen finden Sie unter "Node Health Check Operator".

Schritte

1. Erstellen Sie einen NodeHealthCheck (NHC) CR im Trident-Namespace, um die Worker-Knoten im Cluster zu überwachen. Beispiel:

```
apiVersion: remediation.medik8s.io/v1alpha1
kind: NodeHealthCheck
metadata:
  name: <CR name>
spec:
  selector:
    matchExpressions:
      - key: node-role.kubernetes.io/control-plane
        operator: DoesNotExist
      - key: node-role.kubernetes.io/master
        operator: DoesNotExist
  remediationTemplate:
    apiVersion: trident.netapp.io/v1
    kind: TridentNodeRemediationTemplate
    namespace: <Trident installation namespace>
    name: trident-node-remediation-template
  minHealthy: 0 # Trigger force-detach upon one or more node failures
  unhealthyConditions:
    - type: Ready
      status: "False"
      duration: 0s
    - type: Ready
      status: Unknown
      duration: 0s
```

2. Wenden Sie die Knoten-Integritätsprüfung CR im `trident` Namespace an.

```
kubectl apply -f <nhc-cr-file>.yaml -n <trident-namespace>
```

Der oben genannte CR ist so konfiguriert, dass er die K8s-Worker-Knoten auf die Knotenzustände Ready: false und Unknown überwacht. Automated-Failover wird ausgelöst, sobald ein Knoten in den Zustand Ready: false oder Ready: Unknown wechselt.

The `unhealthyConditions` in the CR verwendet eine Karenzzeit von 0 Sekunden. Dies führt dazu, dass das automatisierte Failover sofort ausgelöst wird, sobald K8s den Knotenstatus auf Ready: false setzt, was erfolgt, nachdem K8s den Heartbeat eines Knotens verloren hat. K8s hat standardmäßig eine Wartezeit von 40 Sekunden nach dem letzten Heartbeat, bevor Ready: false gesetzt wird. Diese Karenzzeit kann in den K8s-Bereitstellungsoptionen angepasst werden.

Weitere Konfigurationsoptionen finden Sie unter "Node-Healthcheck-Operator Dokumentation".

Zusätzliche Setup-Informationen

Wenn Trident mit aktiviertem Force-Detach installiert wird, werden automatisch zwei zusätzliche Ressourcen im Trident-Namensraum erstellt, um die Integration mit NHC zu erleichtern: TridentNodeRemediationTemplate (TNRT) und ClusterRole.

TridentNodeRemediationTemplate (TNRT):

Das TNRT dient als Vorlage für den NHC Controller, der TNRT verwendet, um bei Bedarf TNR-Ressourcen zu generieren.

```
apiVersion: trident.netapp.io/v1
kind: TridentNodeRemediationTemplate
metadata:
  name: trident-node-remediation-template
  namespace: trident
spec:
  template:
    spec: {}
```

ClusterRole:

Eine Clusterrolle wird während der Installation ebenfalls hinzugefügt, wenn die erzwungene Trennung aktiviert ist. Dadurch erhält NHC Berechtigungen für TNRs im Trident-Namespace.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  labels:
    rbac.ext-remediation/aggregate-to-ext-remediation: "true"
  name: tridentnoderemediation-access
rules:
- apiGroups:
  - trident.netapp.io
  resources:
  - tridentnoderemediationtemplates
  - tridentnoderemediations
  verbs:
  - get
  - list
  - watch
  - create
  - update
  - patch
  - delete
```

K8s-Cluster-Upgrades und Wartung

Um Failover zu verhindern, pausieren Sie das automatisierte Failover während K8s-Wartungsarbeiten oder -Upgrades, bei denen die Nodes voraussichtlich ausfallen oder neu starten. Sie können das NHC CR (siehe oben) pausieren, indem Sie dessen CR patchen:

```
kubectl patch NodeHealthCheck <cr-name> --patch
'{"spec":{"pauseRequests":["<description-for-reason-of-pause>"]}}' --type=merge
```

Dadurch wird das automatische Failover pausiert. Um das automatische Failover wieder zu aktivieren, entfernen Sie die pauseRequests aus der Spezifikation, nachdem die Wartung abgeschlossen ist.

Einschränkungen

- E/A-Operationen werden nur auf den ausgefallenen Knoten für Volumes verhindert, die von force-detach unterstützt werden. Nur Pods, die Volumes/PVCs verwenden, die von force-detach unterstützt werden, werden automatisch entfernt.
- Automatisches Failover und erzwungenes Trennen werden innerhalb des trident-controller-Pods ausgeführt. Fällt der Knoten, auf dem der trident-controller ausgeführt wird, aus, verzögert sich das automatische Failover, bis K8s den Pod auf einen fehlerfreien Knoten verschoben hat.

Integration kundenspezifischer Lösungen zur Überprüfung des Knotenzustands

Sie können den Node Healthcheck Operator durch alternative Tools zur Erkennung von Knotenausfällen ersetzen, um automatisches Failover auszulösen. Um die Kompatibilität mit dem automatisierten Failover-Mechanismus zu gewährleisten, sollte Ihre individuelle Lösung:

- Erstelle einen TNR, wenn ein Knotenausfall erkannt wird, wobei der Name des ausgefallenen Knotens als TNR-CR-Name verwendet wird.
- Löschen Sie den TNR, wenn der Knoten wiederhergestellt ist und sich der TNR im Status „Succeeded“ befindet.

Sicherheit

Sicherheit

Verwenden Sie die hier aufgeführten Empfehlungen, um sicherzustellen, dass Ihre Trident-Installation sicher ist.

Trident in einem eigenen Namensraum ausführen

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

Um andere Anwendungen und Benutzer von Trident zu trennen, installieren Sie Trident immer in einem eigenen Kubernetes-Namespace (`trident`). Wenn Trident in einem eigenen Namespace installiert wird, wird sichergestellt, dass nur das Kubernetes-Administrationspersonal Zugriff auf den Trident-Pod und die in den Namespaced-CRD-Objekten gespeicherten Artefakte (wie Backend- und CHAP-Secrets, falls zutreffend) hat. Sie sollten sicherstellen, dass nur Administratoren Zugriff auf den Trident-Namespace und damit auf die `tridentctl` Anwendung haben.

CHAP Authentifizierung mit ONTAP SAN-Backends verwenden

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

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

Verwenden Sie die CHAP-Authentifizierung mit NetApp HCI und SolidFire Backends

NetApp empfiehlt die Bereitstellung von bidirektionalem CHAP, um die Authentifizierung zwischen einem Host und den NetApp HCI- und SolidFire-Backends sicherzustellen. Trident verwendet ein Secret-Objekt, das zwei CHAP-Passwörter pro Mandant enthält. Wenn Trident installiert ist, verwaltet es die CHAP-Secrets 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 Volumes, die von Trident erstellt werden, sind keiner Volume-Zugriffsgruppe zugeordnet.

Verwenden Sie Trident mit NVE und NAE

NetApp ONTAP bietet Verschlüsselung ruhender Daten, um sensible Daten im Falle von Diebstahl, Rückgabe oder anderweitiger Verwendung einer Festplatte zu schützen. Weitere Informationen finden Sie unter "Konfigurieren Sie die Übersicht zur NetApp Volume Encryption".

- 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 auf dem Backend nicht aktiviert ist, wird jedes in Trident bereitgestellte Volume NVE-fähig sein, es sei denn, das NVE-Verschlüsselungsflag ist auf `false` (den Standardwert) in der Backend-Konfiguration gesetzt.

> Volumes, die in Trident auf einem NAE-fähigen Backend erstellt wurden, müssen NVE- oder NAE-verschlüsselt sein.
>
> - Sie können das NVE-Verschlüsselungsflag auf `true` in der Trident-Backend-Konfiguration setzen, um die NAE-Verschlüsselung zu überschreiben und einen spezifischen Verschlüsselungsschlüssel pro Volume zu verwenden.
> - Das Setzen des NVE-Verschlüsselungsflags auf `false` einem NAE-fähigen Backend erstellt ein NAE-fähiges Volume. Sie können die NAE-Verschlüsselung nicht deaktivieren, indem Sie das NVE-Verschlüsselungsflag auf `false` setzen.

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

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 Volume-Erweiterung für LUKS-verschlüsselte Volumes.

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

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

Bevor Sie beginnen

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

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

Wird keine Antwort zurückgegeben, unterstützt Ihr Prozessor kein AES-NI. 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 Sie `parameters.selector` zur Definition der Speicherpools mit LUKS-Verschlüsselung. Beispiel:

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

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

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

Einschränkungen

LUKS-verschlüsselte 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 `luksEncryption` auf (`true` im Backend setzen. Die `luksEncryption` Option teilt Trident mit, ob das Volume LUKS-kompatibel (`true` ist oder nicht LUKS-kompatibel (`false`, wie im folgenden Beispiel gezeigt.

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

PVC-Konfiguration für den Import von LUKS-Volumes

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

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

Eine LUKS-Passphrase rotieren

Sie können die LUKS-Passphrase rotieren und die Rotation bestätigen.

> Vergessen Sie eine Passphrase erst, nachdem Sie überprüft haben, dass sie von keinem Volume, Snapshot oder Secret mehr referenziert wird. Geht eine referenzierte Passphrase verloren, können Sie das Volume möglicherweise nicht einbinden und die Daten bleiben verschlüsselt und unzugänglich.

Über diese Aufgabe

Die Rotation der LUKS-Passphrase erfolgt, wenn ein Pod, der das Volume einbindet, erstellt wird, nachdem eine neue LUKS-Passphrase festgelegt wurde. Wenn ein neuer Pod erstellt wird, vergleicht Trident die LUKS-Passphrase auf dem Volume mit der aktiven Passphrase im Secret.

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

Schritte

1. Fügen Sie die `node-publish-secret-name` und `node-publish-secret-namespace` StorageClass-Parameter hinzu. 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. Stellen Sie sicher, dass `previous-luke-passphrase-name` und `previous-luks-passphrase` mit der vorherigen Passphrase 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. Erstellen Sie einen neuen Pod, der das Volume einbindet. Dies ist erforderlich, um die Rotation zu initiieren.

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 die neue Passphrase zurückgegeben wird.

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

Volumenerweiterung aktivieren

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

Schritte

1. Aktivieren Sie das `CSINodeExpandSecret` Feature-Gate (Beta 1.25+). Siehe "Kubernetes 1.25: Verwendung von Secrets für die knotengesteuerte Erweiterung von CSI-Volumes" für Details.
2. Fügen Sie die `node-expand-secret-name` und `node-expand-secret-namespace` StorageClass-Parameter hinzu. Beispiel:

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

Ergebnisse

Wenn Sie die Online-Speichererweiterung initiieren, übergibt das kubelet die entsprechenden Anmeldeinformationen an den Treiber.

Kerberos-In-Flight-Verschlüsselung

Durch die Verwendung der Kerberos-In-Flight-Verschlüsselung können Sie die Sicherheit des Datenzugriffs verbessern, indem Sie die Verschlüsselung für den Datenverkehr zwischen Ihrem verwalteten Cluster und dem Storage-Backend aktivieren.

Trident unterstützt Kerberos-Verschlüsselung für ONTAP als Storage-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 Sie die 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 Storage-Backend aktivieren.

> ⓘ Die Kerberos-Verschlüsselung für NFS-Datenverkehr mit On-Premise ONTAP-Speicher-Backends wird nur mit dem `ontap-nas` storage driver unterstützt.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie Zugriff auf das `tridentctl` Dienstprogramm haben.
- 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 Storage-Backend freigeben werden.
- Stellen Sie sicher, dass Sie die ONTAP Storage-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 den Abschnitt NetApp NFSv4-Domänenkonfiguration (Seite 13) des "NetApp NFSv4-Verbesserungen 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 ONTAP Storage-VM-Root-Volume sowie für alle ONTAP-Volumes, die mit dem Upstream-Kubernetes-Cluster gemeinsam genutzt werden, unterstützen. Die Exportrichtlinienregeln, die Sie hinzufügen, oder neuen Exportrichtlinien, die Sie erstellen, 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 Privatsphärenschutz)

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	Aktiviert	Aktiviert	Aktiviert
Kerberos 5i	Aktiviert	Aktiviert	Aktiviert
Kerberos 5p	Aktiviert	Aktiviert	Aktiviert

Siehe die folgende Dokumentation, um zu erfahren, wie Sie ONTAP Exportrichtlinien und Exportrichtlinienregeln erstellen:

- "Erstellen Sie eine Exportrichtlinie"
- "Fügen Sie einer Exportrichtlinie eine Regel hinzu"

Erstellen Sie ein Storage-Backend

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

Über diese Aufgabe

Wenn Sie eine Storage-Backend-Konfigurationsdatei erstellen, die die Kerberos-Verschlüsselung konfiguriert, können Sie mit dem `spec.nfsMountOptions`-Parameter eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung angeben:

- `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-Verschlüsselungsstufe 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 Werte in Klammern <> mit Informationen aus Ihrer Umgebung:

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

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

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

Schlägt die Backend-Erstellung fehl, liegt ein Fehler in der Backend-Konfiguration vor. Sie können die Protokolle einsehen, um die Ursache zu ermitteln, indem Sie den folgenden Befehl ausführen:

```
tridentctl logs
```

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

Erstellen Sie eine Speicherklasse

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

Über diese Aufgabe

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

- `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-Verschlüsselungsstufe an. Wenn Sie in der Parameterliste mehr als eine Kerberos-Verschlüsselungsstufe angeben, wird nur die erste Option verwendet. Wenn die von Ihnen in der Speicher-Backend-Konfiguration angegebene Verschlüsselungsstufe von der Stufe abweicht, die Sie im Speicherklassenobjekt angeben, 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
```

Sie sollten eine Ausgabe ähnlich der folgenden sehen:

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

Volumes bereitstellen

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

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 das `tridentctl` Dienstprogramm haben.
- Stellen Sie sicher, dass Sie das Azure NetApp Files Storage-Backend für die Kerberos-Verschlüsselung vorbereitet haben, indem Sie die Anforderungen beachten und den Anweisungen in "Azure NetApp Files-Dokumentation"folgen.
- Stellen Sie sicher, dass alle NFSv4-Volumes, die Sie mit Kerberos-Verschlüsselung verwenden, korrekt konfiguriert sind. Siehe den Abschnitt NetApp NFSv4-Domänenkonfiguration (Seite 13) des "NetApp NFSv4-Verbesserungen und Best Practices-Leitfaden".

Erstellen Sie ein Storage-Backend

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

Über diese Aufgabe

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

- Die **Speicher-Backend-Ebene** unter Verwendung des `spec.kerberos` Felds
- Der **virtuelle Poolpegel** unter Verwendung des `spec.storage.kerberos` Feldes

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 virtuelle Pool-Ebene). Ersetzen Sie Werte in Klammern <> mit Informationen aus Ihrer Umgebung:

Beispiel auf Storage-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 auf virtueller Pool-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
  storage:
    - labels:
        type: encryption
      kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-secret
```

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

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

Schlägt die Backend-Erstellung fehl, liegt ein Fehler in der Backend-Konfiguration vor. Sie können die Protokolle einsehen, um die Ursache zu ermitteln, indem Sie den folgenden Befehl ausführen:

```
tridentctl logs
```

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

Erstellen Sie eine 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
```

Sie sollten eine Ausgabe ähnlich der folgenden sehen:

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

Volumes bereitstellen

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