Erste Schritte

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/de-de/netapp-solutions-cloud/openshift/os-solutions-overview.html on August 18, 2025. Always check docs.netapp.com for the latest.

Inhalt

Erste Schritte . . . 1
NetApp Hybrid Multicloud-Lösungen für Red Hat OpenShift Container-Workloads . . . 1
Überblick . . . 1
Wertversprechen der NetApp Hybrid Multicloud-Lösungen für Red Hat OpenShift Container-Workloads . . . 3
Unterstützte Lösungen von NetApp Hybrid Multicloud für Red Hat OpenShift Container-Workloads . . . 4
Szenario 1: Datenschutz und Migration innerhalb der lokalen Umgebung mit Trident Protect . . . 5
Szenario 2: Datenschutz und Migration von der lokalen Umgebung in die AWS-Umgebung mit Trident Protect . . . 5
Szenario 3: Datenschutz und Migration von der lokalen Umgebung in die AWS-Umgebung . . . 6
Versionen verschiedener Komponenten, die bei der Lösungsvalidierung verwendet werden . . . 8
Unterstützte NetApp Storage-Integrationen mit Red Hat OpenShift Containers . . . 9
Optionen für die Container Storage Interface (CSI) . . . 11
Zusätzliche Dokumentation . . . 13

Erste Schritte

NetApp Hybrid Multicloud-Lösungen für Red Hat OpenShift Container-Workloads

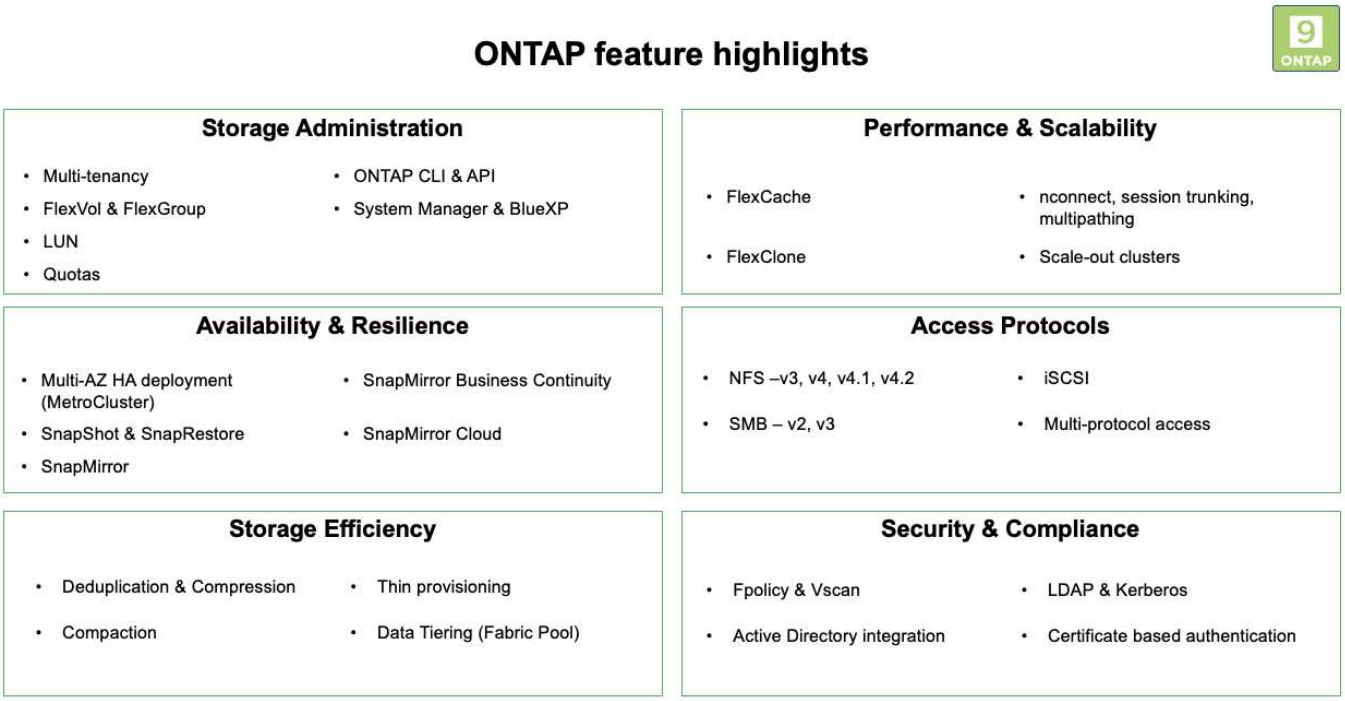
NetApp verzeichnet einen deutlichen Anstieg der Zahl der Kunden, die ihre alten Unternehmensanwendungen modernisieren und mithilfe von Containern und Orchestrierungsplattformen, die auf Kubernetes basieren, neue Anwendungen erstellen. Die Red Hat OpenShift Container Platform ist ein Beispiel, das unserer Erfahrung nach von vielen unserer Kunden übernommen wird.

Überblick

Da immer mehr Kunden Container in ihren Unternehmen einsetzen, ist NetApp optimal aufgestellt, um die persistenten Speicheranforderungen ihrer Stateful-Anwendungen und die klassischen Datenverwaltungsanforderungen wie Datenschutz, Datensicherheit und Datenmigration zu erfüllen. Diese Anforderungen werden jedoch mithilfe unterschiedlicher Strategien, Tools und Methoden erfüllt.

Die unten aufgeführten Speicheroptionen auf Basis von **NetApp ONTAP** bieten Sicherheit, Datenschutz, Zuverlässigkeit und Flexibilität für Container- und Kubernetes-Bereitstellungen.

- Selbstverwalteter Speicher vor Ort:
  - NetApp Fabric Attached Storage (FAS), NetApp All Flash FAS Arrays (AFF), NetApp All SAN Array (ASA) und ONTAP Select
- Vom Anbieter verwalteter Speicher vor Ort:
  - NetApp Keystone bietet Storage as a Service (STaaS)
- Selbstverwalteter Speicher in der Cloud:
  - NetApp Cloud Volumes ONTAP(CVO) bietet selbstverwalteten Speicher in den Hyperscalern
- Vom Anbieter verwalteter Speicher in der Cloud:
  - Amazon FSx for NetApp ONTAP, Azure NetApp Files und Google Cloud NetApp Volumes bieten dateibasierten Speicher in der Cloud.



- NetApp BlueXP** ermöglicht Ihnen die Verwaltung Ihres gesamten Speicher- und Datenbestands über eine einzige Steuerebene/Schnittstelle.

Sie können BlueXP verwenden, um Cloud-Speicher (z. B. Cloud Volumes ONTAP und Azure NetApp Files) zu erstellen und zu verwalten, Daten zu verschieben, zu schützen und zu analysieren und viele lokale und Edge-Speichergeräte zu steuern.

- NetApp Trident** ist ein CSI-konformer Speicher-Orchestrator, der eine schnelle und einfache Nutzung von persistentem Speicher ermöglicht, der durch eine Vielzahl der oben genannten NetApp -Speicheroptionen unterstützt wird. Es handelt sich um eine Open-Source-Software, die von NetApp gepflegt und unterstützt wird.

Astra Trident CSI feature highlights

CSI specific

- CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies
- CSI topology
- Volume expansion

Security

- Dynamic-export policy management
- iSCSI initiator-groups dynamic management
- iSCSI bidirectional CHAP

Control

- Storage and performance consumption
- Monitoring
- Volume Import
- Cross Namespace Volume Access

Installation methods

- Binary
- Helm chart
- Operator
- GitOps

Choose your access mode

- RWO (ReadWriteOnce, i.e 1⇔1)
- RWX (*ReadWriteMany*, i.e 1⇔n)
- ROX (*ReadOnlyMany*)
- RWOP (ReadWriteOnce POD)

Choose your protocol

- NFS
- SMB
- iSCSI

Geschäftskritische Container-Workloads erfordern mehr als nur persistente Volumes. Ihre Datenverwaltungsanforderungen erfordern auch den Schutz und die Migration der Kubernetes-Anwendungsobjekte.

> Anwendungsdaten umfassen neben den Benutzerdaten auch Kubernetes-Objekte: Einige Beispiele sind: - Kubernetes-Objekte wie Pods-Spezifikationen, PVCs, Bereitstellungen, Dienste - benutzerdefinierte Konfigurationsobjekte wie Konfigurationszuordnungen und Geheimnisse - persistente Daten wie Snapshot-Kopien, Backups, Klone - benutzerdefinierte Ressourcen wie CRs und CRDs

- NetApp Trident Protect**, verfügbar als kostenlose Open-Source-Software, die von NetApp gepflegt wird, bietet erweiterte Funktionen zur Anwendungsdatenverwaltung, die die Funktionalität und Verfügbarkeit von Stateful-Kubernetes-Anwendungen verbessern, die von NetApp ONTAP Speichersystemen und dem NetApp Trident CSI-Speicherbereitsteller unterstützt werden. Trident Protect vereinfacht die Verwaltung, den Schutz und die Verschiebung von Container-Workloads über öffentliche Clouds und lokale Umgebungen hinweg. Es bietet außerdem Automatisierungsfunktionen über seine API und CLI.

Diese Referenzdokumentation bietet eine Validierung des Datenschutzes von containerbasierten Anwendungen, die auf der RedHat OpenShift-Plattform mit Trident Protect bereitgestellt werden. Darüber hinaus bietet die Lösung detaillierte Informationen zur Bereitstellung und Verwendung von Red Hat Advanced Cluster Management (ACM) zur Verwaltung der Containerplattformen. Das Dokument hebt auch die Details zur Integration von NetApp -Speicher mit Red Hat OpenShift-Containerplattformen mithilfe des Trident CSI Provisioner hervor.

Wertversprechen der NetApp Hybrid Multicloud-Lösungen für Red Hat OpenShift Container-Workloads

Die meisten Kunden beginnen nicht einfach mit dem Aufbau von Kubernetes-basierten Umgebungen ohne vorhandene Infrastruktur. Vielleicht handelt es sich um einen traditionellen IT-Shop, der die meisten seiner Unternehmensanwendungen auf virtuellen

Maschinen ausführt (beispielsweise in großen VMware-Umgebungen). Dann beginnen sie mit dem Aufbau kleiner containerbasierter Umgebungen, um die Anforderungen ihrer modernen Anwendungsentwicklungsteams zu erfüllen. Diese Initiativen beginnen normalerweise im Kleinen und breiten sich immer weiter aus, wenn die Teams diese neuen Technologien und Fähigkeiten erlernen und die vielen Vorteile erkennen, die sich aus ihrer Einführung ergeben. Die gute Nachricht für Kunden ist, dass NetApp die Anforderungen beider Umgebungen erfüllen kann. Dieses Lösungspaket für Hybrid-Multicloud mit Red Hat OpenShift ermöglicht es NetApp -Kunden, moderne Cloud-Technologien und -Dienste zu übernehmen, ohne ihre gesamte Infrastruktur und Organisation umbauen zu müssen. Unabhängig davon, ob Kundenanwendungen und -daten vor Ort, in der Cloud, auf virtuellen Maschinen oder in Containern gehostet werden, kann NetApp konsistentes Datenmanagement, Schutz, Sicherheit und Portabilität bieten. Mit diesen neuen Lösungen steht derselbe Mehrwert, den NetApp seit Jahrzehnten in lokalen Rechenzentrumsumgebungen bietet, für den gesamten Datenhorizont des Unternehmens zur Verfügung, ohne dass erhebliche Investitionen in die Umrüstung, den Erwerb neuer Fähigkeiten oder den Aufbau neuer Teams erforderlich sind. NetApp ist gut aufgestellt, um Kunden bei der Lösung dieser geschäftlichen Herausforderungen zu unterstützen, unabhängig davon, in welcher Phase ihrer Cloud-Reise sie sich befinden.

NetApp Hybrid Multi-Cloud mit Red Hat Openshift:

- Bietet Kunden validierte Designs und Vorgehensweisen, die ihnen die besten Möglichkeiten zum Verwalten, Schützen, Sichern und Migrieren ihrer Daten und Anwendungen bei der Verwendung von Red Hat OpenShift mit NetApp basierten Speicherlösungen aufzeigen.
- Präsentieren Sie Best Practices für Kunden, die Red Hat OpenShift mit NetApp -Speicher in VMware-Umgebungen, Bare-Metal-Infrastruktur oder einer Kombination aus beidem ausführen.
- Demonstrieren Sie Strategien und Optionen sowohl für lokale als auch für Cloud-Umgebungen sowie für Hybridumgebungen, in denen beide verwendet werden.

Unterstützte Lösungen von NetApp Hybrid Multicloud für Red Hat OpenShift Container-Workloads

Die Lösung testet und validiert Migration und zentralisierten Datenschutz mit der OpenShift-Containerplattform (OCP), OpenShift Advanced Cluster Manager (ACM), NetApp ONTAP, NetApp BlueXP und NetApp Trident Protect (ACC).

Für diese Lösung wurden die folgenden Szenarien von NetApp getestet und validiert. Die Lösung ist basierend auf den folgenden Merkmalen in mehrere Szenarien unterteilt:

- vor Ort
- Wolke
  - selbstverwaltete OpenShift-Cluster und selbstverwalteter NetApp Speicher
  - Vom Anbieter verwaltete OpenShift-Cluster und vom Anbieter verwalteter NetApp Speicher

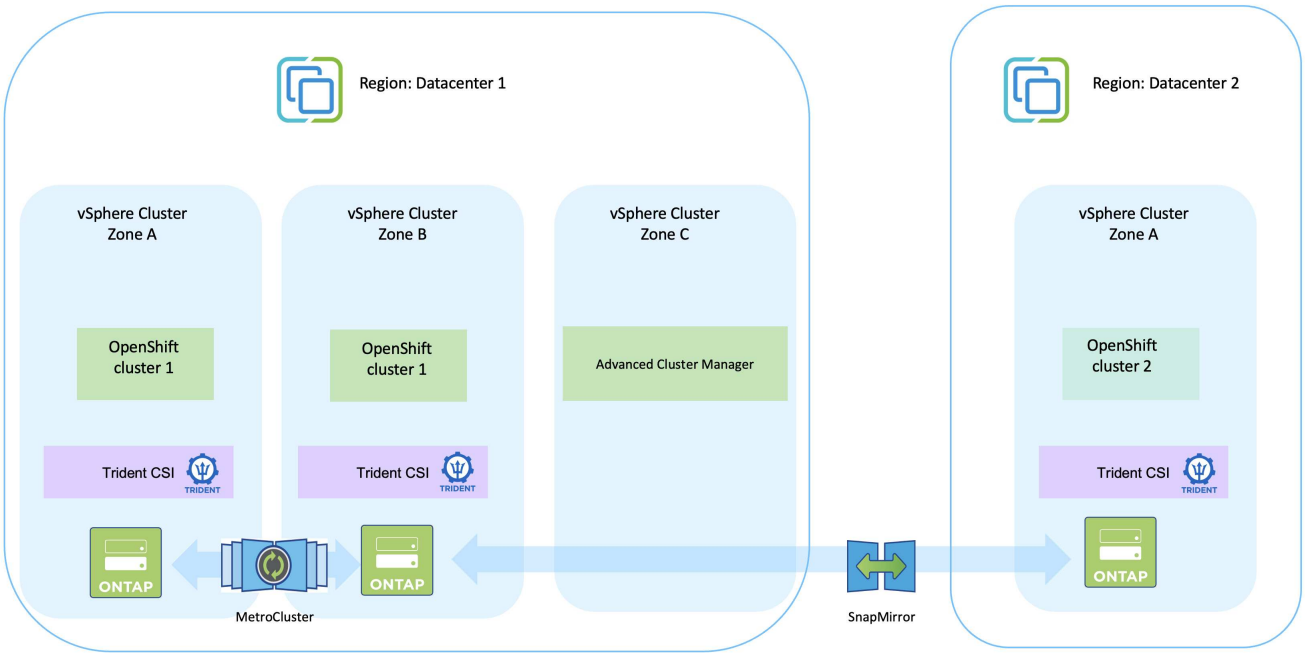
Wir werden in Zukunft weitere Lösungen und Anwendungsfälle entwickeln.

Szenario 1: Datenschutz und Migration innerhalb der lokalen Umgebung mit Trident Protect

Vor Ort: selbstverwaltete OpenShift-Cluster und selbstverwalteter NetApp Speicher

- Erstellen Sie mit ACC Snapshot-Kopien, Backups und Wiederherstellungen zum Schutz Ihrer Daten.
- Führen Sie mit ACC eine SnapMirror -Replikation von Containeranwendungen durch.

Szenario 1

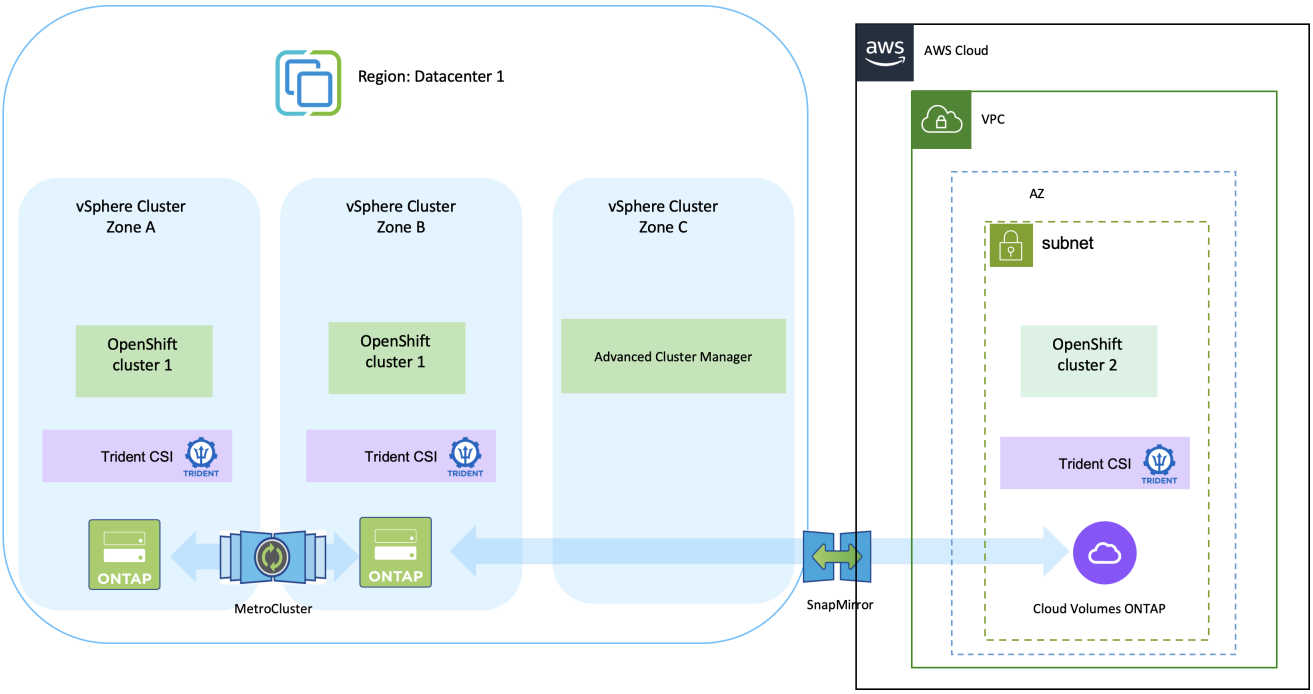


Szenario 2: Datenschutz und Migration von der lokalen Umgebung in die AWS-Umgebung mit Trident Protect

Vor Ort: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Speicher AWS Cloud: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Speicher

- Führen Sie mit ACC Sicherungen und Wiederherstellungen zum Schutz Ihrer Daten durch.
- Führen Sie mit ACC eine SnapMirror -Replikation von Containeranwendungen durch.

Szenario 2

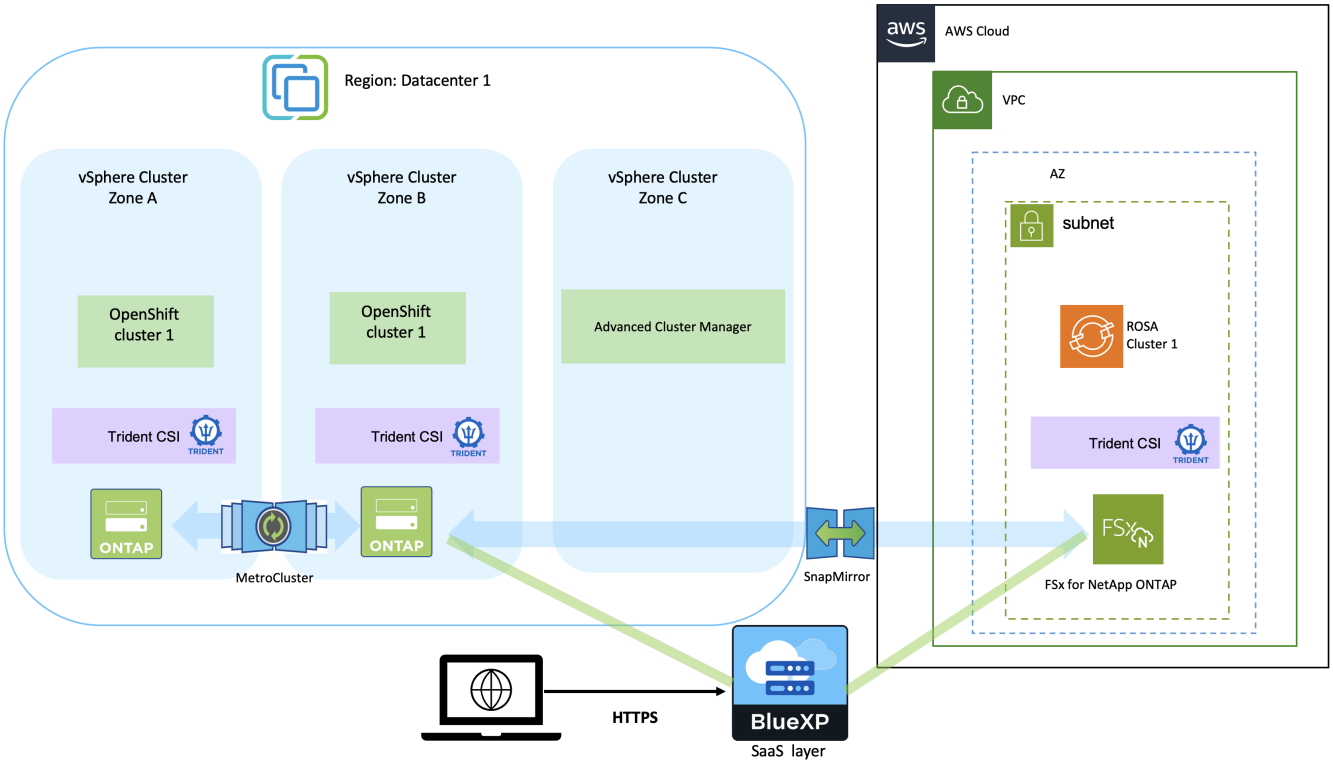


Szenario 3: Datenschutz und Migration von der lokalen Umgebung in die AWS-Umgebung

Vor Ort: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Speicher AWS Cloud: Vom Anbieter verwalteter OpenShift-Cluster (ROSA) und vom Anbieter verwalteter Speicher (FSx ONTAP)

- Führen Sie mit BlueXP die Replikation persistenter Volumes (FSx ONTAP) durch.
- Erstellen Sie mithilfe von OpenShift GitOps Anwendungsmetadaten neu.

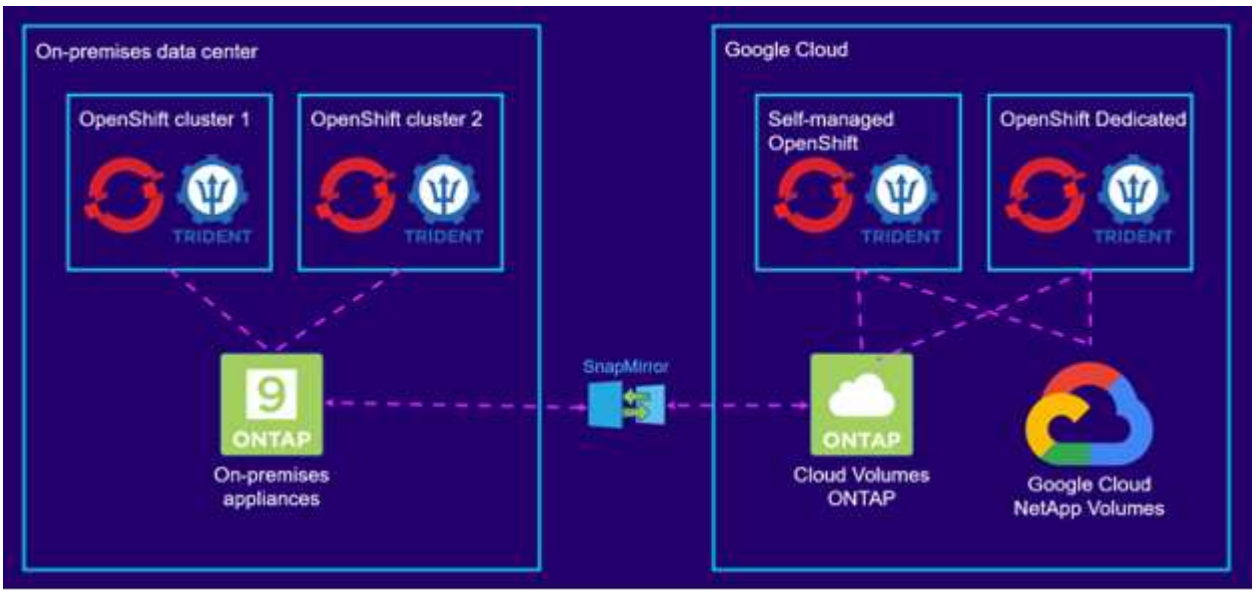
Szenario 3



Szenario 4: Datenschutz und Migration von der lokalen Umgebung zur GCP-Umgebung mit Trident Protect

Vor Ort: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Speicher Google Cloud: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Speicher

- Führen Sie mit ACC Sicherungen und Wiederherstellungen zum Schutz Ihrer Daten durch.
- Führen Sie mit ACC eine SnapMirror -Replikation von Containeranwendungen durch.

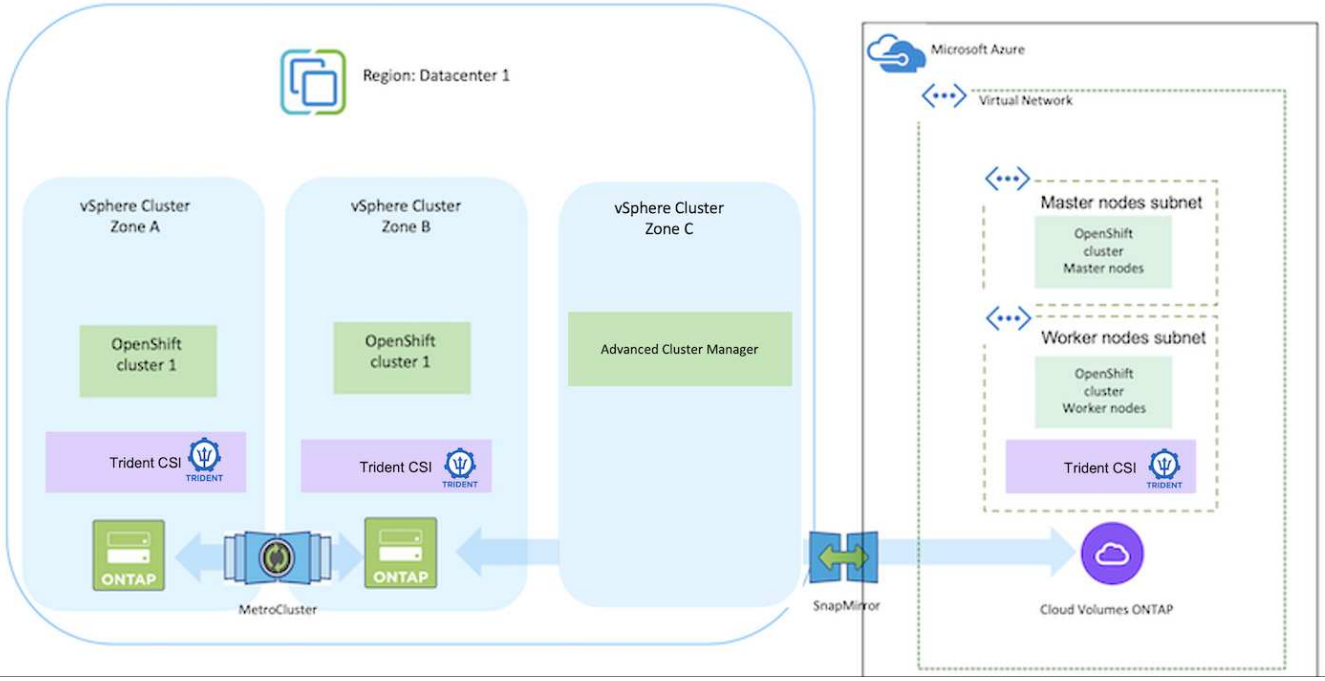


Hinweise zur Verwendung von ONTAP in einer MetroCluster -Konfiguration finden Sie unter"hier," .

Szenario 5: Datenschutz und Migration von der lokalen Umgebung in die Azure-Umgebung mit Trident Protect

Vor Ort: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Speicher Azure Cloud: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Speicher

- Führen Sie mit ACC Sicherungen und Wiederherstellungen zum Schutz Ihrer Daten durch.
- Führen Sie mit ACC eine SnapMirror -Replikation von Containeranwendungen durch.



Hinweise zur Verwendung von ONTAP in einer MetroCluster -Konfiguration finden Sie unter"hier," .

Versionen verschiedener Komponenten, die bei der Lösungsvalidierung verwendet werden

Die Lösung testet und validiert Migration und zentralisierten Datenschutz mit der OpenShift-Containerplattform, OpenShift Advanced Cluster Manager, NetApp ONTAP und NetApp Trident Protect.

Die Szenarien 1, 2 und 3 der Lösung wurden mit den in der folgenden Tabelle gezeigten Versionen validiert:

Komponente	Version
VMware	vSphere-Client-Version 8.0.0.10200 VMware ESXi, 8.0.0, 20842819
Hub-Cluster	OpenShift 4.11.34
Quell- und Zielcluster	OpenShift 4.12.9 vor Ort und in AWS
* NetApp Trident*	Trident Server und Client 23.04.0
* NetApp Trident Protect*	Trident Protect 22.11.0-82

* NetApp ONTAP*	ONTAP 9.12.1
AWS FSx ONTAP	Einzel-AZ

Szenario 4 der Lösung wurde mit den in der folgenden Tabelle gezeigten Versionen validiert:

Komponente	Version
VMware	vSphere-Client-Version 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
Hub-Cluster	OpenShift 4.13.13
Quell- und Zielcluster	OpenShift 4.13.12 vor Ort und in Google Cloud
* NetApp Trident*	Trident Server und Client 23.07.0
* NetApp ONTAP*	ONTAP 9.12.1
* Cloud Volumes ONTAP*	Einzelne AZ, einzelner Knoten, 9.14.0

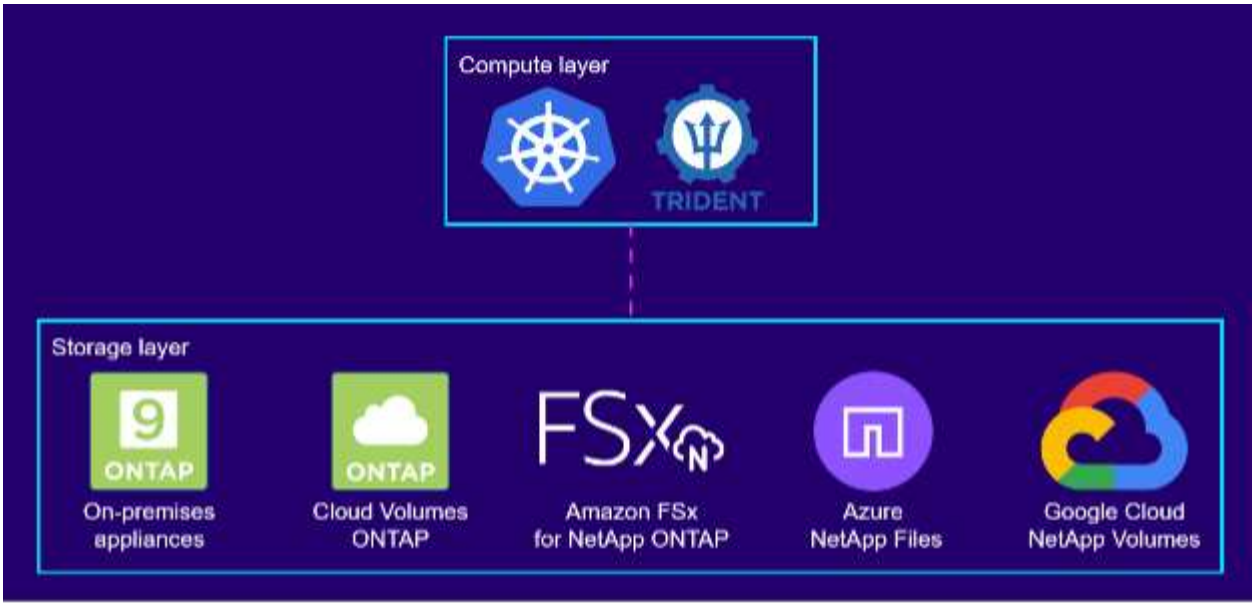
Szenario 5 der Lösung wurde mit den in der folgenden Tabelle gezeigten Versionen validiert:

Komponente	Version
VMware	vSphere-Client-Version 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
Quell- und Zielcluster	OpenShift 4.13.25 vor Ort und in Azure
* NetApp Trident*	Trident Server und Client und Astra Control Provisioner 23.10.0
* NetApp Trident Protect*	Trident Protect 23.10
* NetApp ONTAP*	ONTAP 9.12.1
* Cloud Volumes ONTAP*	Einzelne AZ, einzelner Knoten, 9.14.0

Unterstützte NetApp Storage-Integrationen mit Red Hat OpenShift Containers

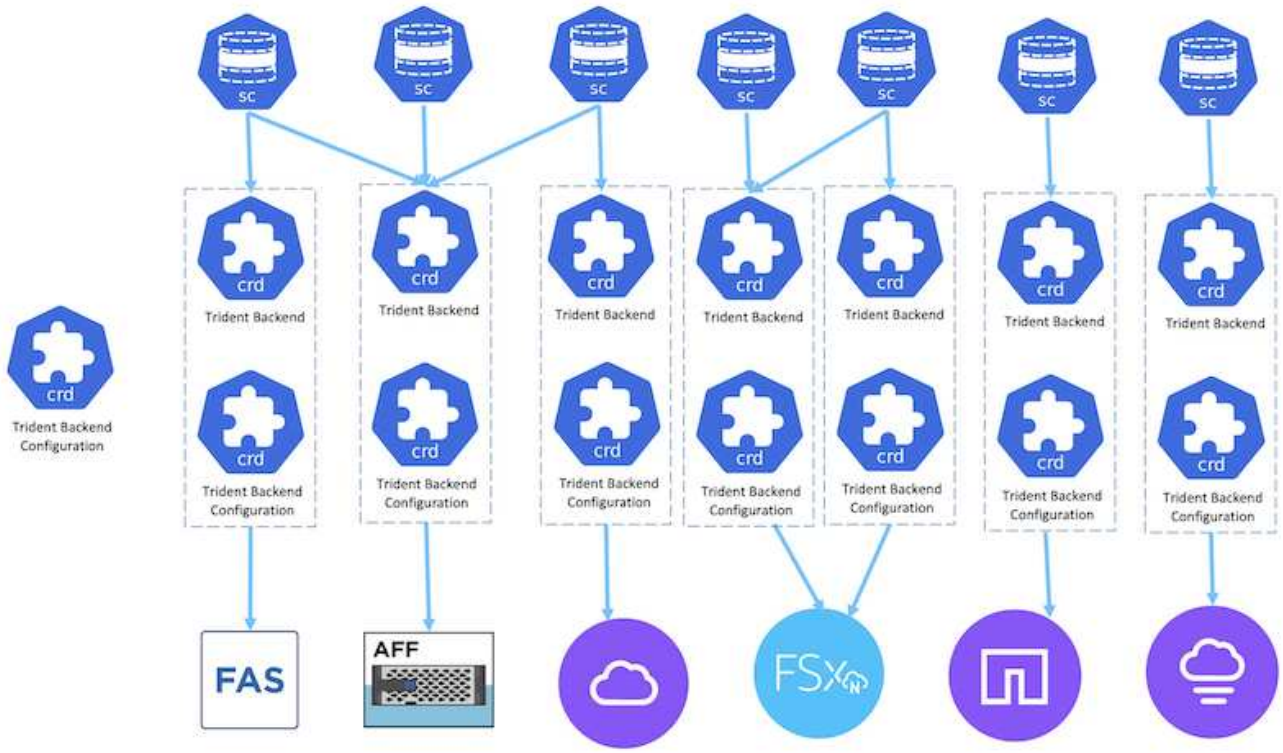
Unabhängig davon, ob die Red Hat OpenShift-Container auf VMware oder in den Hyperscalern ausgeführt werden, kann NetApp Trident als CSI-Provisioner für die verschiedenen Arten von Backend NetApp -Speicher verwendet werden, die es unterstützt.

Das folgende Diagramm zeigt die verschiedenen Backend NetApp -Speicher, die mithilfe von NetApp Trident in OpenShift-Cluster integriert werden können.



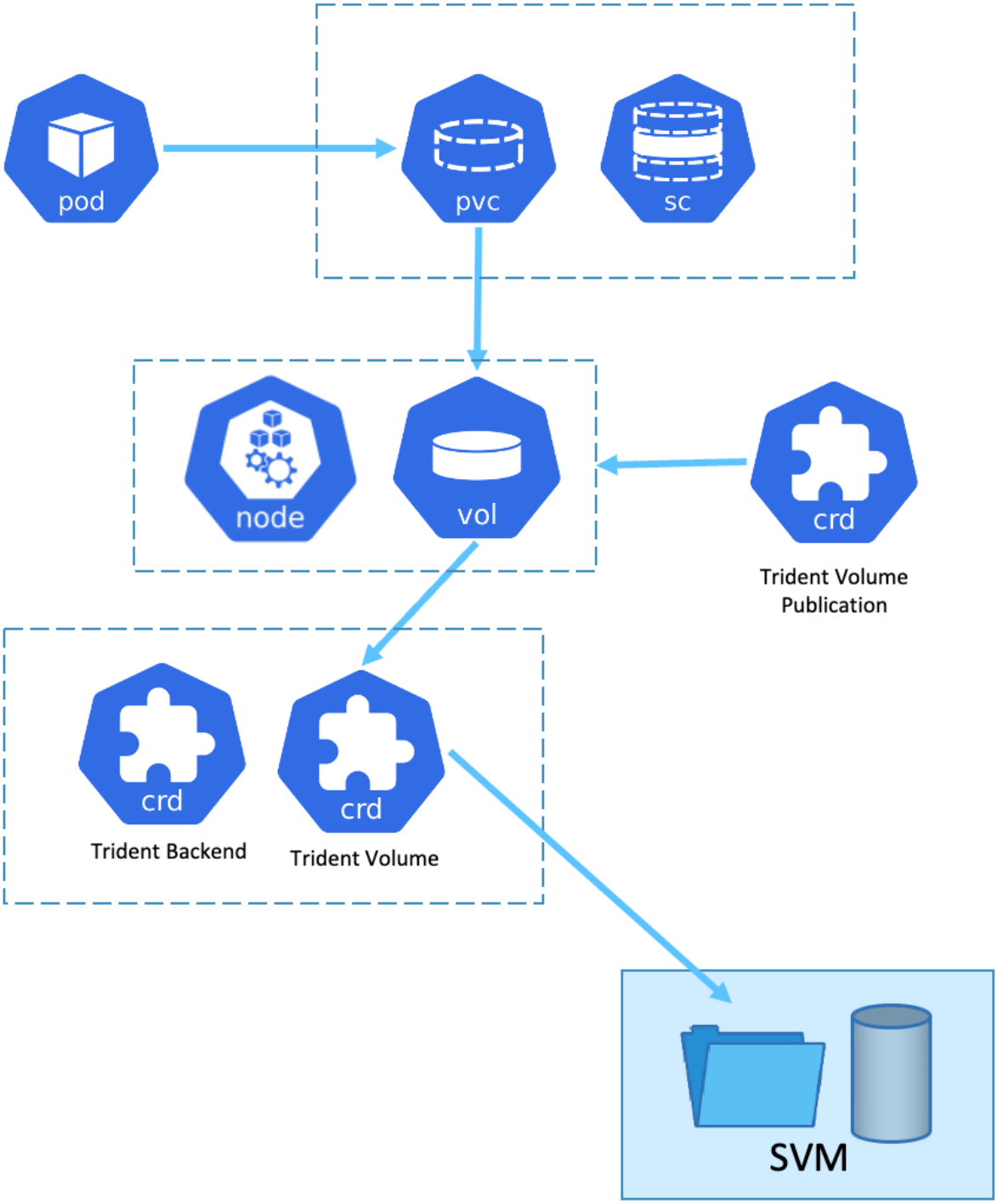
ONTAP Storage Virtual Machine (SVM) bietet sichere Mandantenfähigkeit. Ein einzelner OpenShift-Cluster kann eine Verbindung zu einem oder mehreren SVMs oder sogar zu mehreren ONTAP Clustern herstellen. Die Speicherklasse filtert den Backend-Speicher basierend auf Parametern oder Bezeichnungen. Speicheradministratoren definieren die Parameter für die Verbindung mit dem Speichersystem mithilfe der Trident-Backend-Konfiguration. Bei erfolgreichem Verbindungsaufbau erstellt es das Trident-Backend und füllt die Informationen, die die Speicherklasse filtern kann.

Die Beziehung zwischen der Speicherklasse und dem Backend wird unten dargestellt.



Der Anwendungsbesitzer fordert ein dauerhaftes Volume unter Verwendung der Speicherklasse an. Die Speicherklasse filtert den Backend-Speicher.

Die Beziehung zwischen dem Pod und dem Backend-Speicher wird unten dargestellt.



Optionen für die Container Storage Interface (CSI)

In vSphere-Umgebungen können Kunden den VMware CSI-Treiber und/oder Trident CSI zur Integration mit ONTAP auswählen. Bei VMware CSI werden die persistenten Volumes als lokale SCSI-Festplatten verwendet, während sie bei Trident über das Netzwerk verwendet werden.

Da VMware CSI keine RWX-Zugriffsmodi mit ONTAP unterstützt, müssen Anwendungen Trident CSI verwenden, wenn der RWX-Modus erforderlich ist. Bei FC-basierten Bereitstellungen wird VMware CSI bevorzugt und SnapMirror Business Continuity (SMBC) bietet Hochverfügbarkeit auf Zonenebene.

VMware CSI unterstützt

- Core Block-basierte Datenspeicher (FC, FCoE, iSCSI, NVMeoF)
- Core File-basierte Datenspeicher (NFS v3, v4)
- vVol-Datenspeicher (Block und Datei)

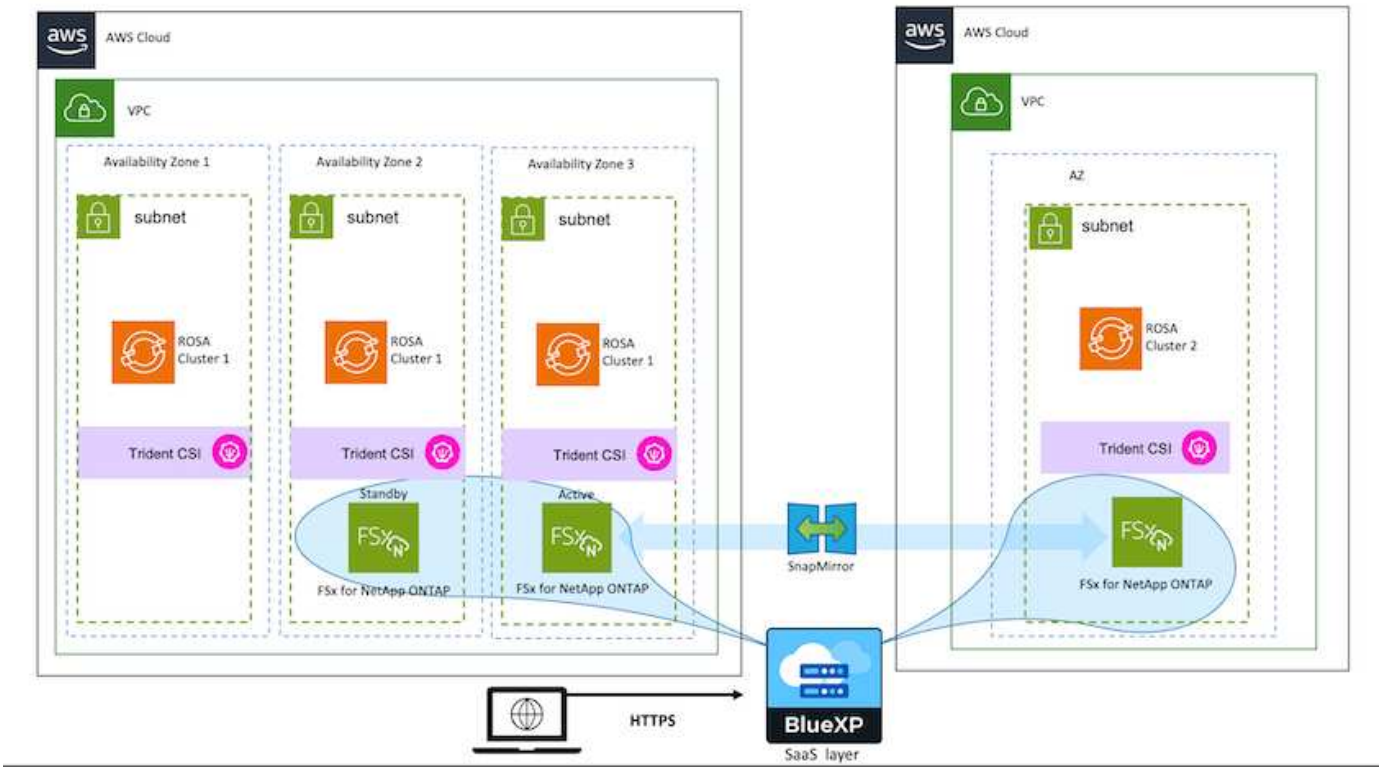
Trident verfügt über folgende Treiber zur Unterstützung von ONTAP

- ontap-san (dediziertes Volume)
- ontap-san-economy (gemeinsam genutztes Volume)
- ontap-nas (dediziertes Volume)
- ontap-nas-economy (gemeinsam genutztes Volume)
- ontap-nas-flexgroup (dediziertes Großvolume)

Sowohl für VMware CSI als auch für Trident CSI unterstützt ONTAP Nconnect, Session Trunking, Kerberos usw. für NFS und Multipathing, Chap-Authentifizierung usw. für Blockprotokolle.

In AWS kann Amazon FSx for NetApp ONTAP (FSx ONTAP) in einer einzelnen Availability Zone (AZ) oder in mehreren AZs bereitgestellt werden. Für Produktions-Workloads, die eine hohe Verfügbarkeit erfordern, bietet Multi-AZ Fehlertoleranz auf Zonenebene und verfügt im Vergleich zu Single-AZ über einen besseren NVMe-Lesecache. Weitere Informationen finden Sie unter"AWS-Leistungsrichtlinien" .

Um Kosten für die Notfallwiederherstellungssite zu sparen, kann ein einzelner AZ FSx ONTAP verwendet werden.



Informationen zur Anzahl der von FSx ONTAP unterstützten SVMs finden Sie unter"Verwalten der virtuellen FSx ONTAP -Speichermaschine"

Zusätzliche Dokumentation

Hier finden Sie einige zusätzliche Dokumentationen als Referenz:

1. "VMware vSphere"
2. "Produktdokumentation zur OpenShift Container-Plattform"
3. "Installieren von OpenShift-Containerplattformclustern"
4. "Produktdokumentation zur erweiterten Clusterverwaltung"
5. "Erstellen eines Clusters mit ACM"
6. "Bereitstellen von Red Hat Quay auf OpenShift"
7. "Trident"
8. "ONTAP 9"
9. "NetApp Verda"- Verda (Open Source) verfügt über eine Sammlung von Referenzausführungs-Hooks für beliebte Cloud-native datenintensive Anwendungen
10. "NetApp BlueXP"
11. "Red Hat OpenShift Service auf AWS"
12. "Amazon FSx ONTAP"
13. "Installieren von OpenShift-Clustern auf GCP"
14. "Installieren von OpenShift-Clustern auf Azure"

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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