



NetApp Hybrid-Multi-Cloud mit Red hat OpenShift

NetApp Solutions

NetApp
April 26, 2024

Inhalt

- NetApp Hybrid-Multi-Cloud mit Container-Workloads Red hat OpenShift 1
 - NetApp Hybrid-Multi-Cloud-Lösungen für Container-Workloads mit Red hat OpenShift. 1
 - NetApp Hybrid-Multi-Cloud-Lösungen für Container-Workloads mit Red hat OpenShift. 14
 - NetApp Hybrid-Multi-Cloud-Lösungen für Container-Workloads mit Red hat OpenShift. 25
 - NetApp Hybrid-Multi-Cloud-Lösungen für Container-Workloads mit Red hat OpenShift. 42

NetApp Hybrid-Multi-Cloud mit Container-Workloads Red hat OpenShift

NetApp Hybrid-Multi-Cloud-Lösungen für Container-Workloads mit Red hat OpenShift

Überblick

Bei NetApp beobachten wir eine deutliche Zunahme bei Kunden, die ihre älteren Enterprise-Applikationen modernisieren und neue Applikationen mithilfe von Containern und Orchestrierungsplattformen auf Basis von Kubernetes erstellen. Die Red hat OpenShift Container Platform ist ein Beispiel, das wir von vielen unserer Kunden angenommen sehen.

Immer mehr Kunden beginnen mit der Einführung von Containern in ihrem Unternehmen. NetApp ist perfekt aufgestellt, um die persistenten Storage-Anforderungen ihrer zustandsbehafteten Applikationen und klassischen Datenmanagementanforderungen zu erfüllen, beispielsweise Datensicherung, Datensicherheit und Datenmigration. Diese Bedürfnisse werden jedoch mit verschiedenen Strategien, Werkzeugen und Methoden erfüllt.

NetApp ONTAP basierte Storage-Optionen, die unten aufgeführt sind, bieten Sicherheit, Datensicherung, Zuverlässigkeit und Flexibilität für Container- und Kubernetes-Implementierungen.

- Automatisierter, lokaler Storage:
 - NetApp Fabric Attached Storage (FAS), NetApp All-Flash-FAS-Arrays (AFF), NetApp All-SAN-Arrays (ASA) und ONTAP Select
- Von Providern gemanagter Storage in On-Premises:
 - NetApp Keystone stellt Storage-as-a-Service (STaaS) bereit
- Automatisierter Storage in der Cloud:
 - NetApp Cloud Volumes ONTAP (CVO) bieten Self-Managed-Storage in den Hyperscalern
- Von Providern gemanagter Storage in der Cloud:
 - Cloud Volumes Service für Google Cloud (CVS), Azure NetApp Files (ANF) und Amazon FSX für NetApp ONTAP bieten vollständig gemanagten Storage in den Hyperscalern

ONTAP feature highlights



Storage Administration <ul style="list-style-type: none">• Multi-tenancy• FlexVol & FlexGroup• LUN• Quotas• ONTAP CLI & API• System Manager & BlueXP	Performance & Scalability <ul style="list-style-type: none">• FlexCache• FlexClone• nconnect, session trunking, multipathing• Scale-out clusters
Availability & Resilience <ul style="list-style-type: none">• Multi-AZ HA deployment (MetroCluster)• SnapShot & SnapRestore• SnapMirror• SnapMirror Business Continuity (MetroCluster)• SnapMirror Cloud	Access Protocols <ul style="list-style-type: none">• NFS –v3, v4, v4.1, v4.2• SMB – v2, v3• iSCSI• Multi-protocol access
Storage Efficiency <ul style="list-style-type: none">• Deduplication & Compression• Compaction• Thin provisioning• Data Tiering (Fabric Pool)	Security & Compliance <ul style="list-style-type: none">• Fpolicy & Vscan• Active Directory integration• LDAP & Kerberos• Certificate based authentication

NetApp BlueXP ermöglicht Ihnen das Management Ihrer gesamten Storage- und Datenbestände über eine einzige Managementoberfläche.

Mit BlueXP können Sie Cloud-Storage erstellen und verwalten (z. B. Cloud Volumes ONTAP und Azure NetApp Files), Daten verschieben, schützen und analysieren sowie zahlreiche lokale und Edge-Storage-Geräte kontrollieren.

NetApp Astra Trident ist ein CSI-konformer Storage Orchestrator, der eine schnelle und einfache Nutzung von persistentem Storage ermöglicht und von einer Vielzahl der oben genannten NetApp Storage-Optionen unterstützt wird. Es handelt sich um eine Open-Source-Software, die von NetApp gewartet und unterstützt wird.

Astra Trident CSI feature highlights



CSI specific <ul style="list-style-type: none">• CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies• CSI topology• Volume expansion	Security <ul style="list-style-type: none">• Dynamic-export policy management• iSCSI initiator-groups dynamic management• iSCSI bidirectional CHAP
Control <ul style="list-style-type: none">• Storage and performance consumption• Monitoring• Volume Import• Cross Namespace Volume Access	Installation methods <ul style="list-style-type: none">• Binary• Helm chart• Operator• GitOps
Choose your access mode <ul style="list-style-type: none">• RWO (ReadWriteOnce, i.e 1↔1)• RWX (ReadWriteMany, i.e 1↔n)• ROX (ReadOnlyMany)• RWOP (ReadWriteOnce POD)	Choose your protocol <ul style="list-style-type: none">• NFS• SMB• iSCSI

Geschäftskritische Container-Workloads benötigen mehr als nur persistente Volumes. Ihre Datenmanagement-Anforderungen erfordern auch den Schutz und die Migration der Kubernetes-Objekte für die Applikation.



Neben Benutzerdaten umfassen Applikationsdaten kubernetes-Objekte. Folgende Beispiele sind vorhanden: - kubernetes-Objekte wie Pods-Spezifikationen, PVCs, Implementierungen, Services – benutzerdefinierte Konfigurationsobjekte wie Konfigurationszuordnungen und -Geheimnisse – persistente Daten wie Snapshot-Kopien, Backups, Klone – benutzerdefinierte Ressourcen wie CRS und CRDs

NetApp Astra Control ist sowohl als vollständig gemanagte als auch als selbst gemanagte Software erhältlich und bietet Orchestrierung für solides Applikations-Datenmanagement. Siehe "[Astra-Dokumentation](#)" Weitere Informationen zur Astra Produktfamilie.

Diese Referenzdokumentation unterstützt die Validierung der Migration und des Schutzes von Container-basierten Applikationen, die auf der RedHat OpenShift Container-Plattform über das NetApp Astra Control Center implementiert werden. Darüber hinaus bietet die Lösung allgemeine Details zur Bereitstellung und zur Verwendung von Red hat Advanced Cluster Management (ACM) für die Verwaltung der Container-Plattformen. In diesem Dokument werden auch Einzelheiten zur Integration von NetApp Storage in Container-Plattformen mit Red hat OpenShift mithilfe der Astra Trident CSI-bereitstellung erläutert. Astra Control Center wird auf dem Hub-Cluster bereitgestellt und wird für das Management der Container-Applikationen und ihres Lebenszyklus von persistentem Storage verwendet. Schließlich bietet es eine Lösung für Replizierung, Failover und Failback für Container-Workloads auf gemanagten Red hat OpenShift-Clustern in AWS (ROSA), die Amazon FSX für NetApp ONTAP (FSxN) als persistenten Storage verwenden.

Wertversprechen von NetApp Hybrid-Multi-Cloud-Lösungen für Container-Workloads mit Red hat OpenShift

Die meisten Kunden beginnen nicht nur mit der Entwicklung von Kubernetes-basierten Umgebungen ohne die vorhandene Infrastruktur. Möglicherweise handelt es sich bei ihnen um eine herkömmliche IT-Abteilung, die die meisten ihrer Enterprise-Applikationen auf Virtual Machines ausführt (z. B. in großen VMware-Umgebungen). Dann beginnen

sie, kleine containerbasierte Umgebungen zu erstellen, die die Anforderungen ihrer modernen Applikationsentwicklungsteams erfüllen. Diese Initiativen beginnen in der Regel klein und werden immer mehr verbreitet, wenn die Teams diese neuen Technologien und Fähigkeiten erlernen und beginnen, die vielen Vorteile der Einführung zu erkennen. Die gute Nachricht für Kunden ist, dass NetApp die Anforderungen beider Umgebungen erfüllen kann. Mit diesen Lösungen für Hybrid-Multi-Clouds mit Red hat OpenShift können NetApp Kunden moderne Cloud-Technologien und -Services einführen, ohne die gesamte Infrastruktur und das gesamte Unternehmen überarbeiten zu müssen. Ganz gleich, ob Applikationen und Daten der Kunden lokal, in der Cloud, auf Virtual Machines oder in Containern gehostet werden – NetApp bietet konsistentes Datenmanagement, Sicherung, Sicherheit und Portabilität. Mit diesen neuen Lösungen wird derselbe Wert, den NetApp seit Jahrzehnten in On-Premises-Datacenter-Umgebungen bietet, für das gesamte Datenhorizont des Unternehmens verfügbar sein, ohne dass erhebliche Investitionen in die Tools, die Anschaffung neuer Fähigkeiten oder die Entwicklung neuer Teams erforderlich sind. NetApp unterstützt Kunden dabei, diese geschäftlichen Herausforderungen zu bewältigen – unabhängig von der aktuellen Phase des Cloud-Übergangs.

NetApp Hybrid-Multi-Cloud mit Red hat OpenShift:

- Die Lösung bietet Kunden validierte Designs und Verfahren, die zeigen, wie Kunden ihre Daten und Applikationen am besten managen, schützen, sichern und migrieren können, wenn sie Red hat OpenShift mit NetApp Storage-Lösungen einsetzen.
- Präsentieren von Best Practices für Kunden, die Red hat OpenShift mit NetApp Storage in VMware Umgebungen, Bare Metal-Infrastruktur oder einer Kombination aus beidem ausführen
- Strategien und Optionen sowohl für On-Premises- und Cloud-Umgebungen als auch für Hybrid-Umgebungen aufzeigen, in denen beide eingesetzt werden

Unterstützte Lösungen für die NetApp Hybrid-Multi-Cloud-Umgebung für Container-Workloads mit Red hat OpenShift

Die Lösung testet und validiert Migration und zentralisierte Datensicherung mit OpenShift Container-Plattform (OCP), OpenShift Advanced Cluster Manager (ACM), NetApp ONTAP, NetApp BlueXP und NetApp Astra Control Center (ACC).

Folgende Szenarien werden von NetApp getestet und validiert. Die Lösung ist in mehrere Szenarien aufgeteilt, die auf folgenden Merkmalen basieren:

- On-Premises
- Cloud
 - Selbst gemanagte OpenShift-Cluster und selbstverwalteter NetApp Storage
 - Von Providern gemanagte OpenShift-Cluster und NetApp Storage, der vom Provider gemanagt wird

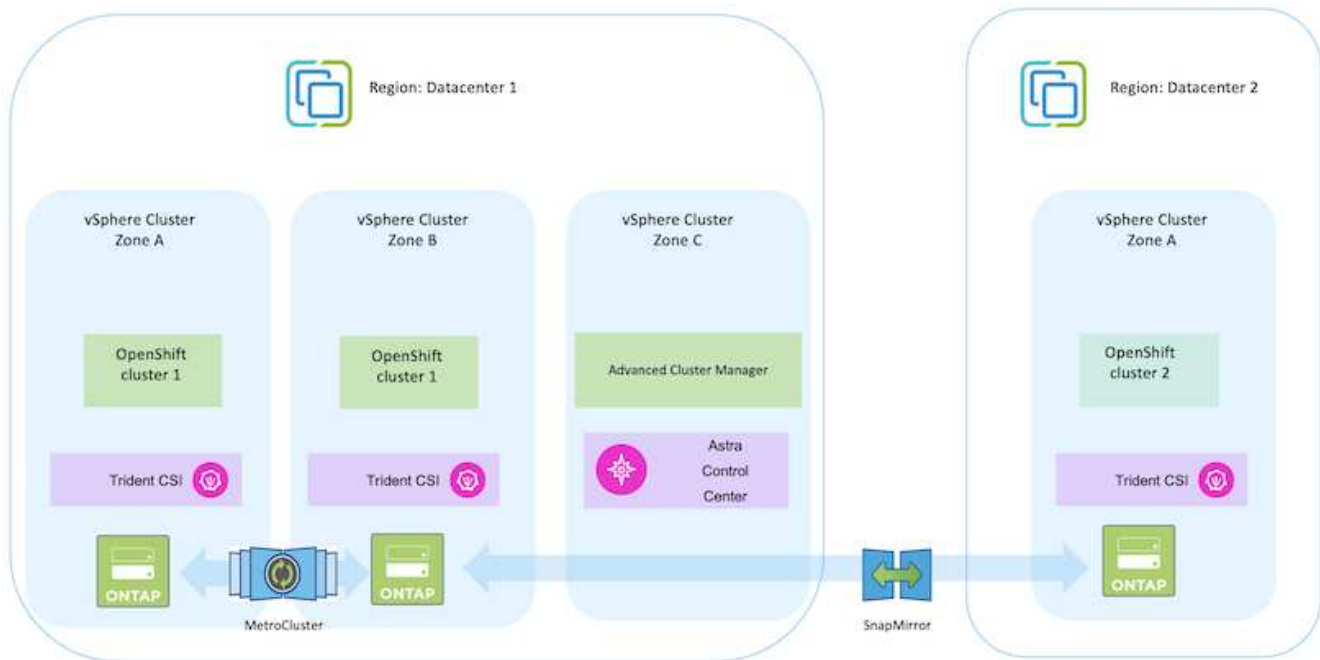
Wir werden in Zukunft weitere Lösungen und Anwendungsfälle entwickeln.

Szenario 1: Datenschutz und Migration innerhalb der On-Premise-Umgebung mittels ACC

Lokal: Selbst gemanagte OpenShift-Cluster und automatisierter NetApp Storage

- Erstellen Sie mithilfe von ACC Snapshot Kopien, Backups und Wiederherstellungen für den Datenschutz.
- Führen Sie mithilfe von ACC eine SnapMirror Replizierung der Container-Applikationen durch.

Szenario 1

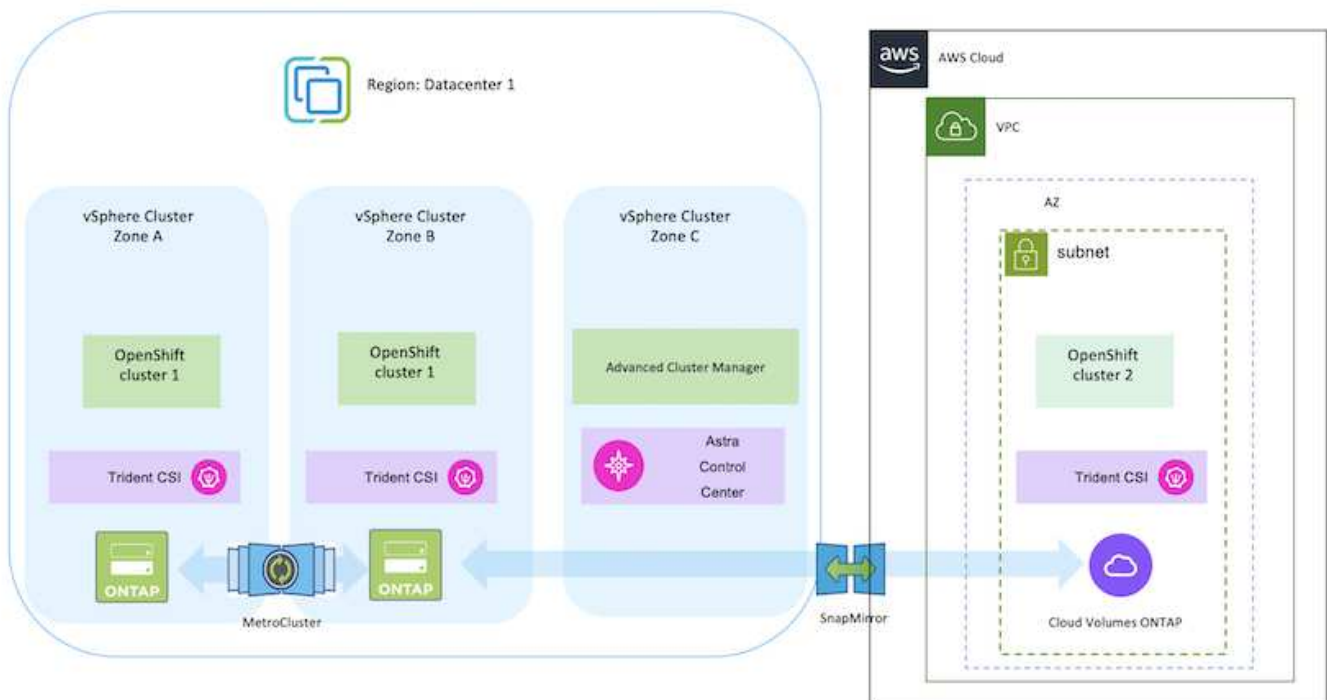


Szenario 2: Datensicherung und Migration von der On-Premises-Umgebung in die AWS-Umgebung mittels ACC

On-Premises: Selbst verwalteter OpenShift-Cluster und selbstverwalteter Storage AWS Cloud: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Storage

- Führen Sie mithilfe von ACC Backups und Wiederherstellungen für den Datenschutz durch.
- Führen Sie mithilfe von ACC eine SnapMirror Replizierung der Container-Applikationen durch.

Szenario 2

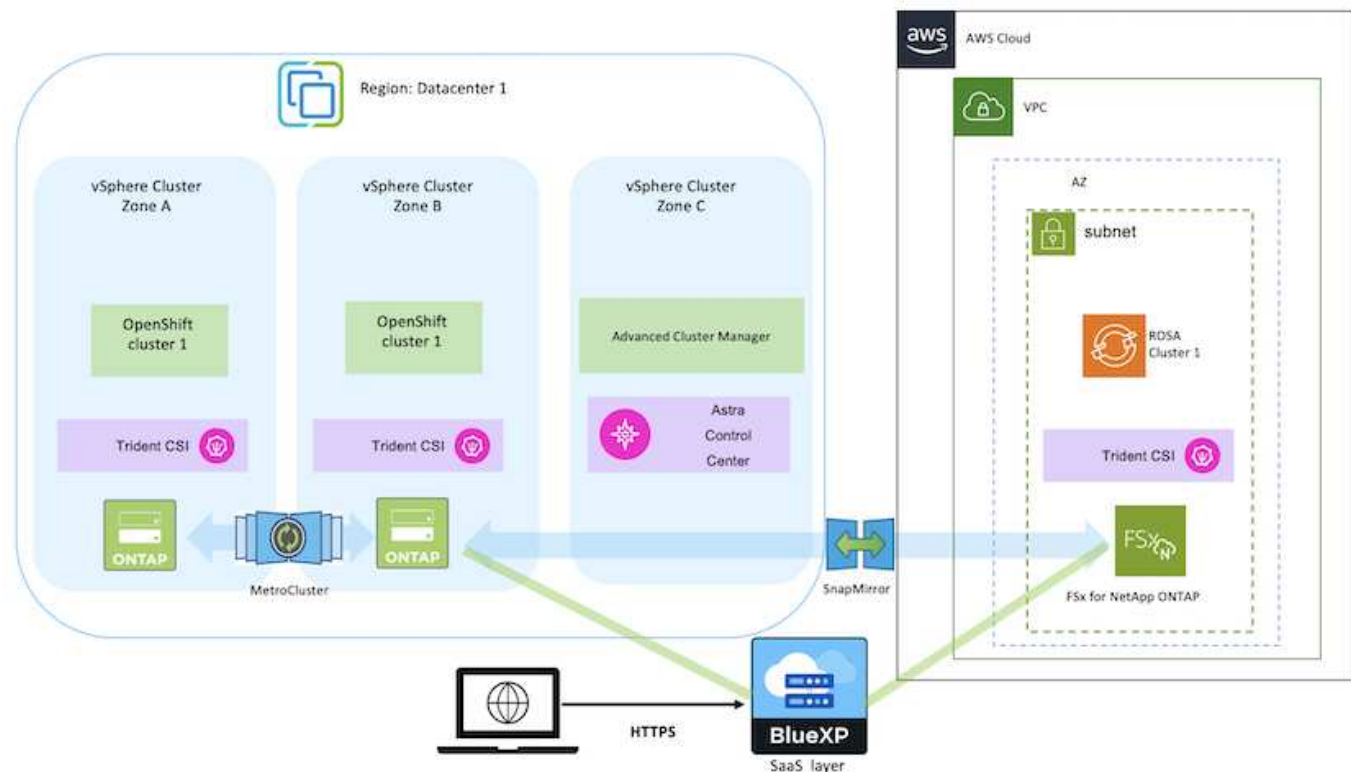


Szenario 3: Datensicherung und Migration von der On-Premises-Umgebung in die AWS-Umgebung

On-Premises: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Storage AWS Cloud: Vom Provider verwaltetes OpenShift-Cluster (ROSA) und Provider-Managed Storage (FSxN)

- Führen Sie mit BlueXP die Replizierung persistenter Volumes (FSxN) durch.
- Erstellen Sie mithilfe von OpenShift GitOps Anwendungsmetadaten neu.

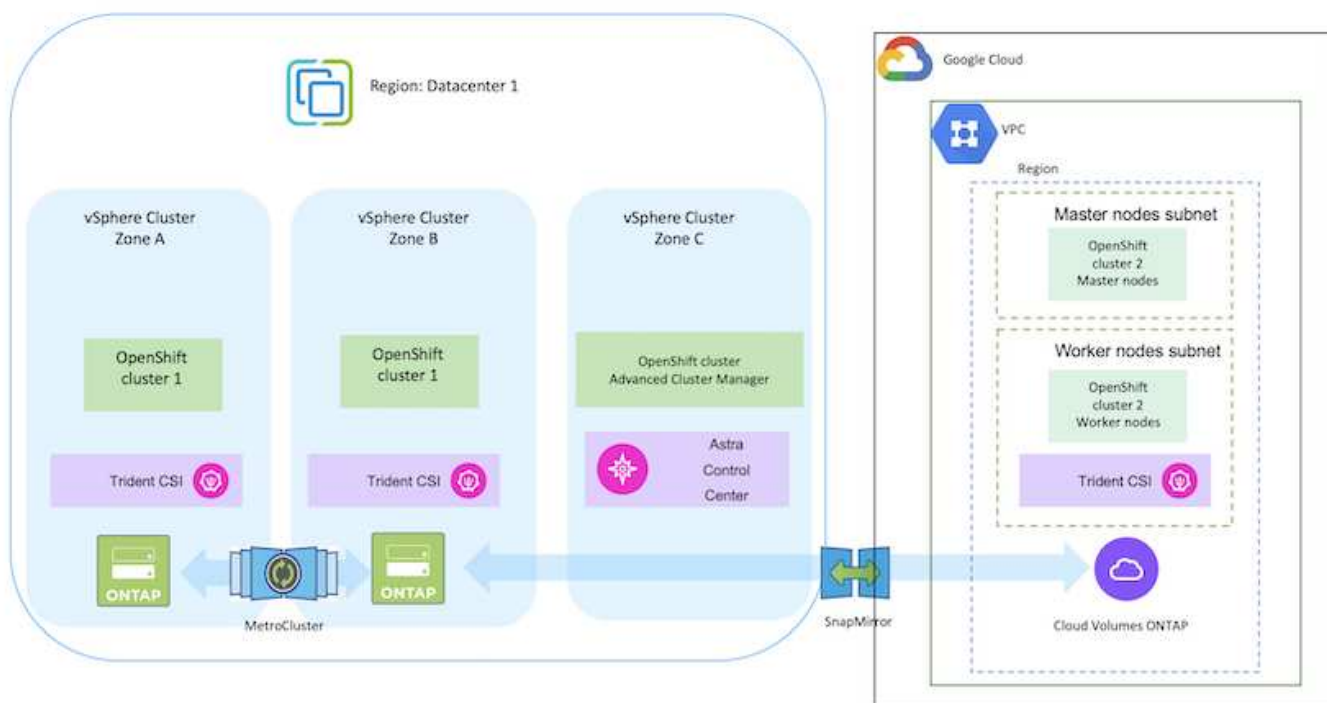
Szenario 3



Szenario 4: Datenschutz und Migration von der On-Premise-Umgebung in die GCP-Umgebung mittels ACC

On-Premises: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Storage Google Cloud: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Storage

- Führen Sie mithilfe von ACC Backups und Wiederherstellungen für den Datenschutz durch.
- Führen Sie mithilfe von ACC eine SnapMirror Replizierung der Container-Applikationen durch.

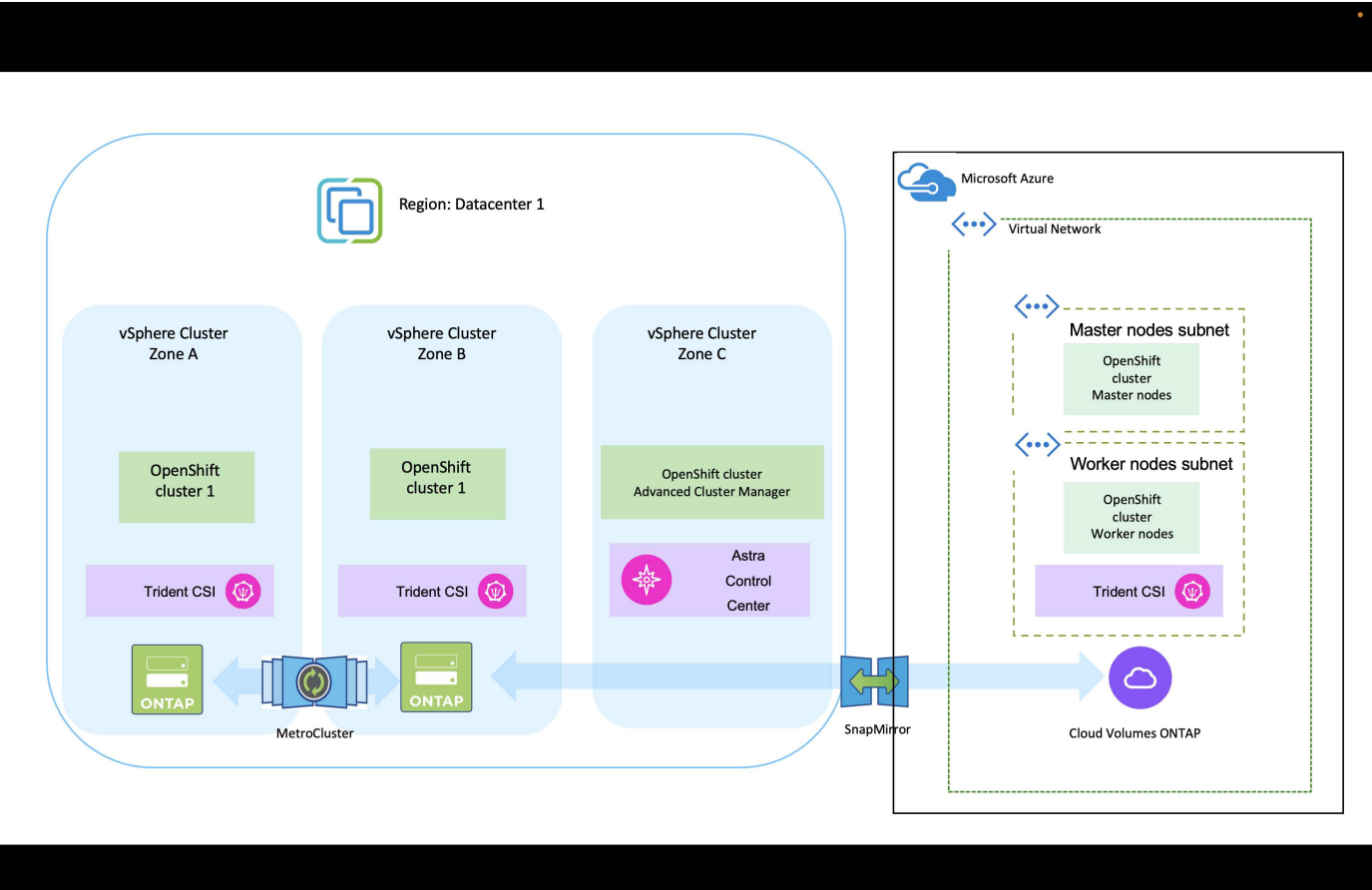


Hinweise zur Verwendung von ONTAP in einer MetroCluster-Konfiguration finden Sie unter ["Hier"](#).

Szenario 5: Datenschutz und Migration von der On-Premises-Umgebung in die Azure-Umgebung mittels ACC

On-Premises: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Storage
Azure Cloud: Automatisiertes OpenShift-Cluster und automatisierter Storage

- Führen Sie mithilfe von ACC Backups und Wiederherstellungen für den Datenschutz durch.
- Führen Sie mithilfe von ACC eine SnapMirror Replizierung der Container-Applikationen 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 die Migration und zentralisierte Datensicherung mit der OpenShift Container-Plattform, OpenShift Advanced Cluster Manager, NetApp ONTAP und NetApp Astra Control Center.

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

* 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 On-Premises und in AWS
NetApp Astra Trident	Trident Server und Client 23.04.0
NetApp Astra Control Center	ACC 22.11.0-82
NetApp ONTAP	ONTAP 9.12.1
AWS FSX for NetApp ONTAP	Single AZ

Szenario 4 der Lösung wurde mit den Versionen validiert, wie in der folgenden Tabelle dargestellt:

* 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 On-Premises und in Google Cloud
NetApp Astra Trident	Trident Server und Client 23.07.0
NetApp Astra Control Center	ACC 23.07.0-25
NetApp ONTAP	ONTAP 9.12.1
Cloud Volumes ONTAP	Single AZ, Single Node, 9.14.0

Szenario 5 der Lösung wurde mit den Versionen validiert, wie in der folgenden Tabelle dargestellt:

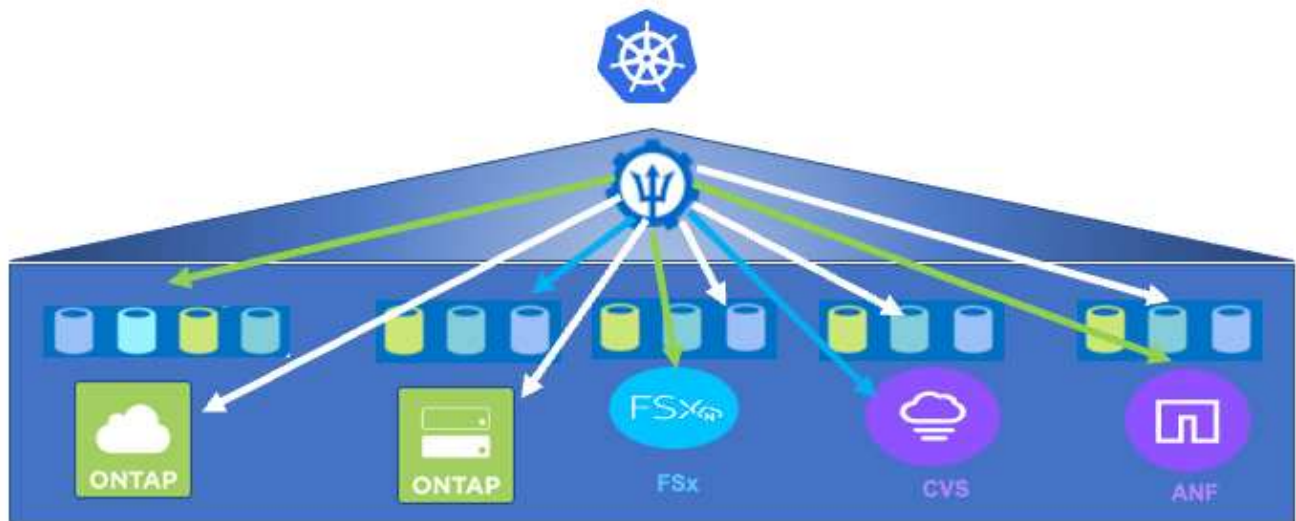
* Komponente*	Version
VMware	VSphere Client Version 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
Quell- und Zielcluster	OpenShift 4.13.25 On-Premises und in Azure
NetApp Astra Trident	Trident Server, Client und Astra Control Provisioner 23.10.0
NetApp Astra Control Center	ACC 23.10
NetApp ONTAP	ONTAP 9.12.1
Cloud Volumes ONTAP	Single AZ, Single Node, 9.14.0

Unterstützte NetApp Storage-Integrationen in Red hat Open Shift Container

Ganz gleich, ob die Red hat Open Shift Container auf VMware oder in den Hyperscalern ausgeführt werden, NetApp Astra Trident kann als CSI-bereitstellung für die verschiedenen von ihm unterstützten Back-End-Storage-Typen von NetApp verwendet

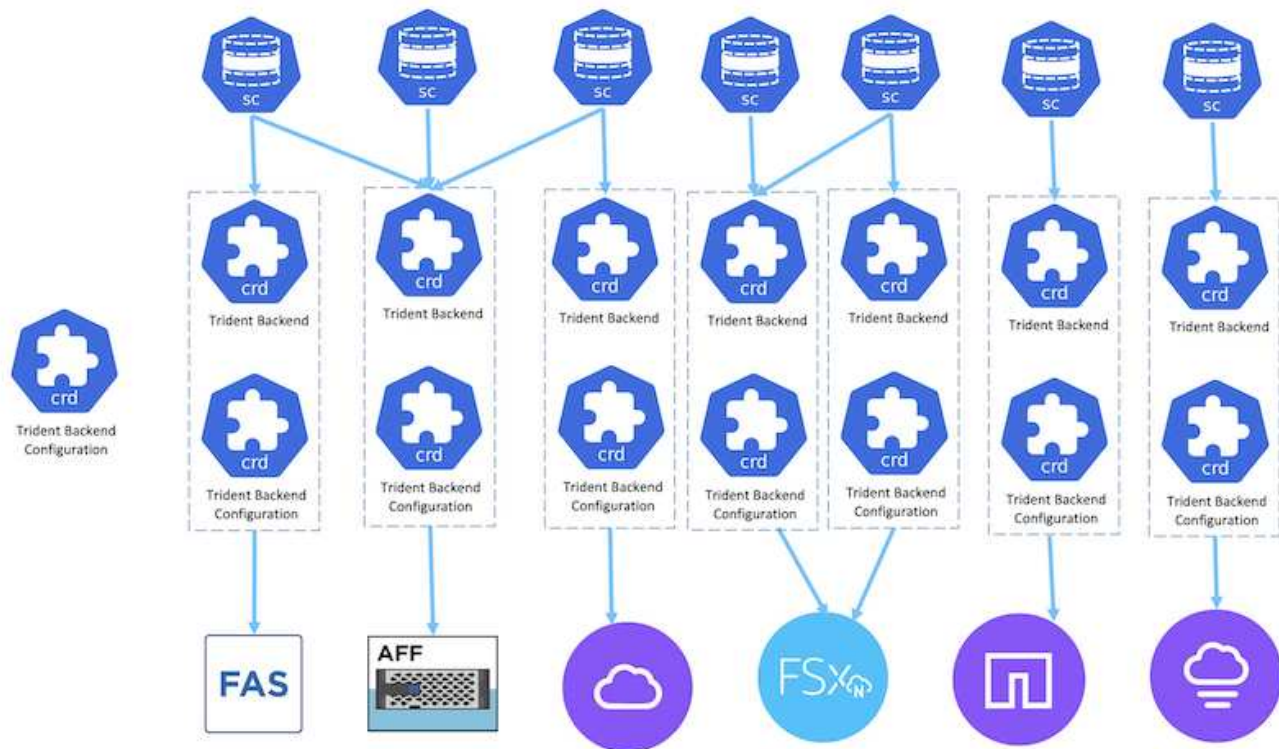
werden.

In der folgenden Abbildung sind die verschiedenen NetApp Back-End-Storage-Systeme dargestellt, die mithilfe von NetApp Astra Trident in OpenShift-Cluster integriert werden können.

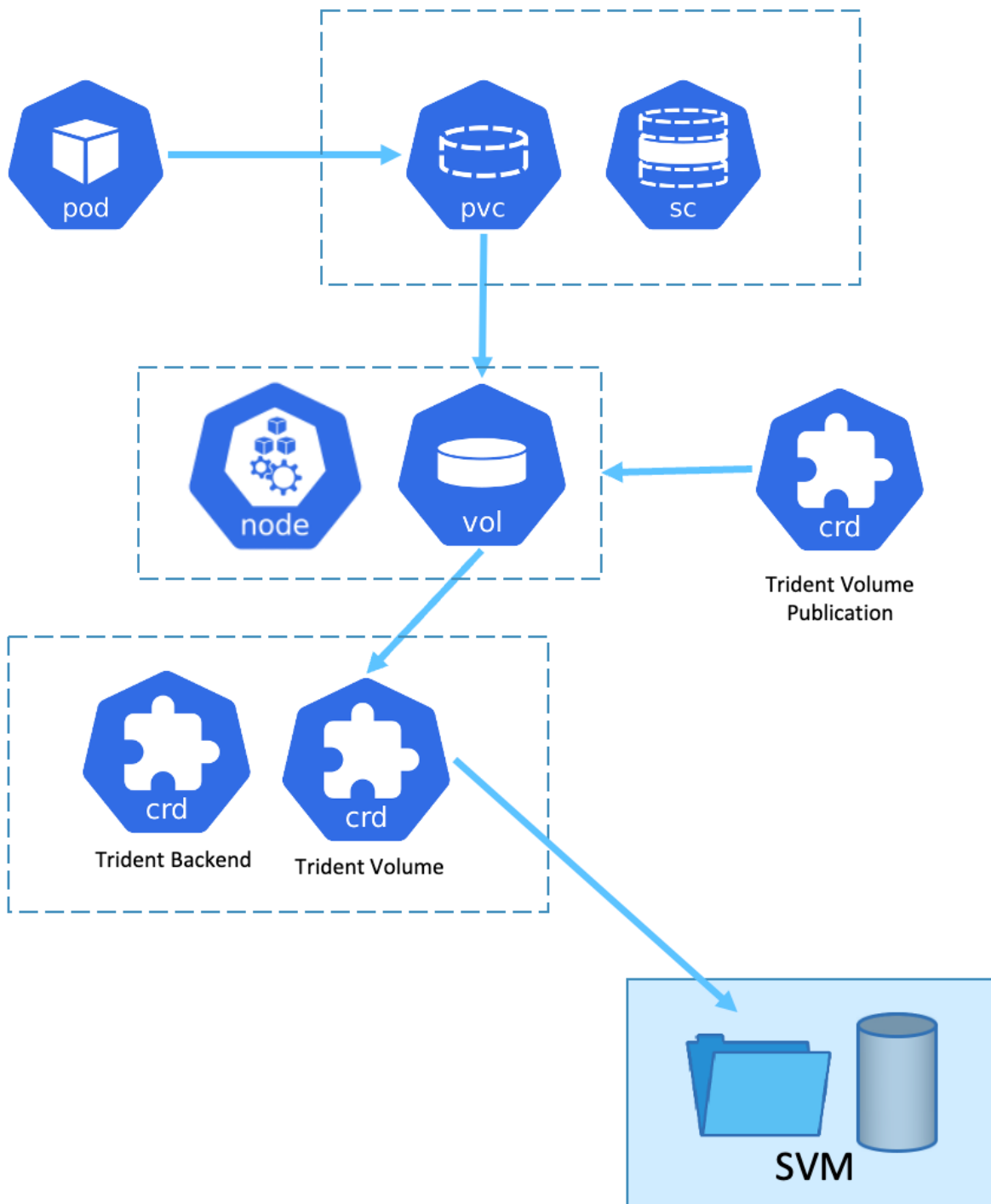


Die ONTAP Storage Virtual Machine (SVM) bietet sichere Mandantenfähigkeit. Ein einziger OpenShift-Cluster kann eine Verbindung zu einer einzelnen SVM oder mehreren SVMs oder sogar zu mehreren ONTAP-Clustern herstellen. Die Storage-Klasse filtert den Back-End-Speicher nach Parametern oder Etiketten. Storage-Administratoren definieren die Parameter für die Verbindung zum Storage-System über eine dreigearbeitete Backend-Konfiguration. Bei erfolgreichem Verbindungsaufbau erstellt es das dreilagige Backend und füllt die Informationen aus, die von der Speicherklasse gefiltert werden können.

Die Beziehung zwischen Storageclass und Backend ist unten dargestellt.



Applikationseigentümer fordert persistentes Volume mithilfe von Storage-Klassen an. Die Storage-Klasse filtert den Back-End Storage. Die Beziehung zwischen dem Pod und dem Back-End Storage wird unten dargestellt.



CSI-Optionen (Container Storage Interface)

In vSphere Umgebungen können Kunden zur Integration mit ONTAP VMware CSI-Treiber und/oder Astra Trident CSI wählen. Mit VMware CSI werden die persistenten Volumes als lokale SCSI-Festplatten verwendet, mit Trident dagegen über ein Netzwerk. Da VMware CSI keine RWX-Zugriffsmodi mit ONTAP unterstützt, müssen Applikationen Trident CSI verwenden, wenn der RWX-Modus erforderlich ist. FC-basierte Implementierungen bevorzugen VMware CSI und SnapMirror Business Continuity (SMBC) bietet Hochverfügbarkeit auf Zonenebene.

VMware CSI unterstützt

- Core-Block-basierte Datastores (FC, FCoE, iSCSI, NVMeoF)
- Dateibasierte Core-Datastores (NFS v3, v4)
- VVol Datastores (Block und Datei)

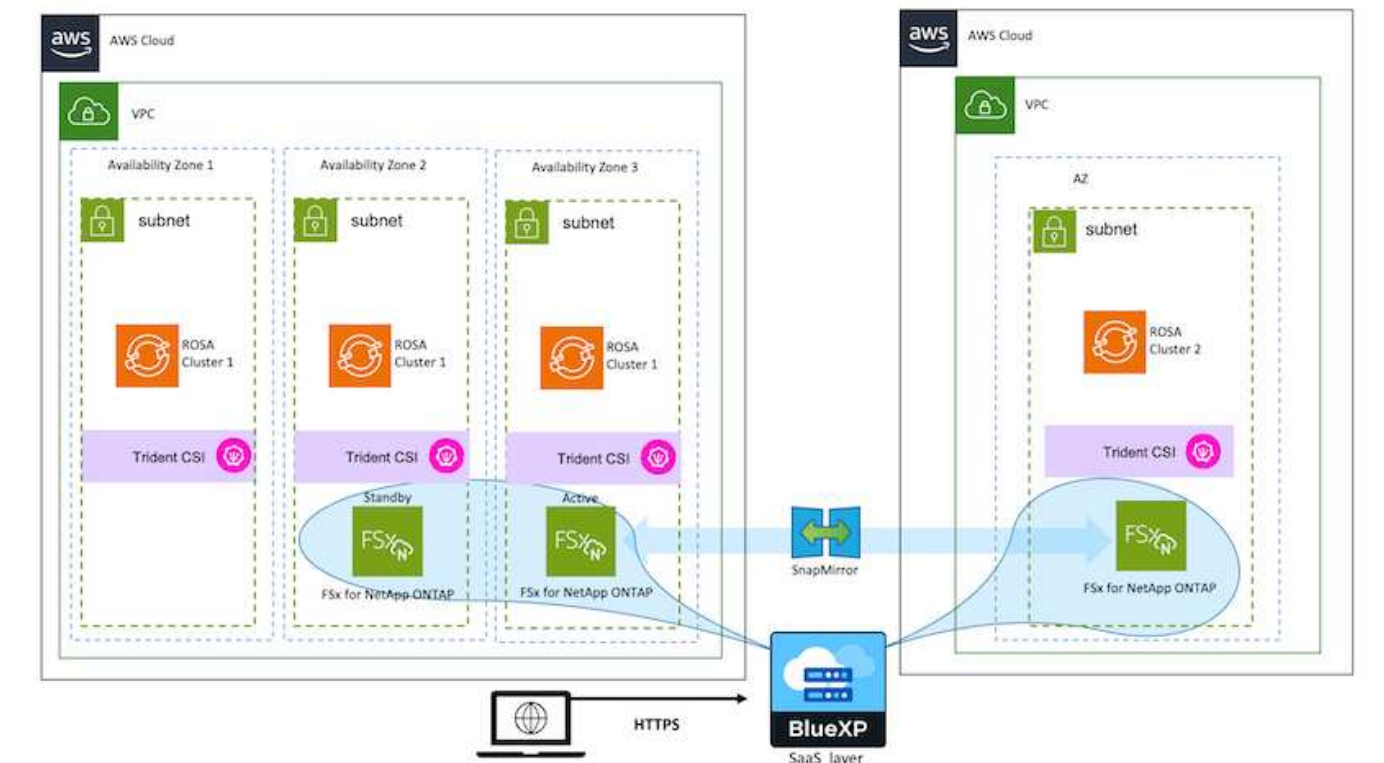
Trident verfügt über folgende Treiber zur Unterstützung von ONTAP

- ontap-san (dediziertes Volume)
- ontap-san-Economy (gemeinsam genutztes Volume)
- ontap-nas (dediziertes Volume)
- ontap-nas-Economy (gemeinsam genutztes Volume)
- ontap-nas-Flexgroup (dediziertes, großes Volume)

Sowohl für VMware CSI als auch für Astra Trident CSI unterstützt ONTAP nconnect, Session-Trunking, kerberos usw. für NFS- und Multipathing, chap-Authentifizierung usw. für Blockprotokolle.

In AWS kann FSX für NetApp ONTAP (FSxN) in einer einzelnen Verfügbarkeitszone (AZ) oder in Multi AZ implementiert werden. Für Produktions-Workloads, die Hochverfügbarkeit erfordern, bietet eine Multi-AZ-Fehlertoleranz auf zonaler Ebene und einen besseren NVMe-Lese-Cache als eine einzelne AZ. Weitere Informationen finden Sie unter ["AWS Performance-Richtlinien"](#).

Um Kosten für den Disaster Recovery-Standort zu sparen, kann ein einzelner AZ FSX ONTAP genutzt werden.



Weitere Informationen zur Anzahl der von FSX ONTAP unterstützten SVMs finden Sie unter ["Management der FSX ONTAP-Storage-Virtual Machine"](#)

NetApp Hybrid-Multi-Cloud-Lösungen für Container-Workloads mit Red hat OpenShift

Überblick

Bei NetApp beobachten wir eine deutliche Zunahme bei Kunden, die ihre älteren Enterprise-Applikationen modernisieren und neue Applikationen mithilfe von Containern und Orchestrierungsplattformen auf Basis von Kubernetes erstellen. Die Red hat OpenShift Container Platform ist ein Beispiel, das wir von vielen unserer Kunden angenommen sehen.

Immer mehr Kunden beginnen mit der Einführung von Containern in ihrem Unternehmen. NetApp ist perfekt aufgestellt, um die persistenten Storage-Anforderungen ihrer zustandsbehafteten Applikationen und klassischen Datenmanagementanforderungen zu erfüllen, beispielsweise Datensicherung, Datensicherheit und Datenmigration. Diese Bedürfnisse werden jedoch mit verschiedenen Strategien, Werkzeugen und Methoden erfüllt.

NetApp ONTAP basierte Storage-Optionen, die unten aufgeführt sind, bieten Sicherheit, Datensicherung, Zuverlässigkeit und Flexibilität für Container- und Kubernetes-Implementierungen.

- Automatisierter, lokaler Storage:
 - NetApp Fabric Attached Storage (FAS), NetApp All-Flash-FAS-Arrays (AFF), NetApp All-SAN-Arrays (ASA) und ONTAP Select
- Von Providern gemanagter Storage in On-Premises:
 - NetApp Keystone stellt Storage-as-a-Service (STaaS) bereit
- Automatisierter Storage in der Cloud:
 - NetApp Cloud Volumes ONTAP (CVO) bieten Self-Managed-Storage in den Hyperscalern
- Von Providern gemanagter Storage in der Cloud:
 - Cloud Volumes Service für Google Cloud (CVS), Azure NetApp Files (ANF) und Amazon FSX für NetApp ONTAP bieten vollständig gemanagten Storage in den Hyperscalern

ONTAP feature highlights



Storage Administration <ul style="list-style-type: none">• Multi-tenancy• FlexVol & FlexGroup• LUN• Quotas• ONTAP CLI & API• System Manager & BlueXP	Performance & Scalability <ul style="list-style-type: none">• FlexCache• FlexClone• nconnect, session trunking, multipathing• Scale-out clusters
Availability & Resilience <ul style="list-style-type: none">• Multi-AZ HA deployment (MetroCluster)• SnapShot & SnapRestore• SnapMirror• SnapMirror Business Continuity (MetroCluster)• SnapMirror Cloud	Access Protocols <ul style="list-style-type: none">• NFS –v3, v4, v4.1, v4.2• SMB – v2, v3• iSCSI• Multi-protocol access
Storage Efficiency <ul style="list-style-type: none">• Deduplication & Compression• Compaction• Thin provisioning• Data Tiering (Fabric Pool)	Security & Compliance <ul style="list-style-type: none">• Fpolicy & Vscan• Active Directory integration• LDAP & Kerberos• Certificate based authentication

NetApp BlueXP ermöglicht Ihnen das Management Ihrer gesamten Storage- und Datenbestände über eine einzige Managementoberfläche.

Mit BlueXP können Sie Cloud-Storage erstellen und verwalten (z. B. Cloud Volumes ONTAP und Azure NetApp Files), Daten verschieben, schützen und analysieren sowie zahlreiche lokale und Edge-Storage-Geräte kontrollieren.

NetApp Astra Trident ist ein CSI-konformer Storage Orchestrator, der eine schnelle und einfache Nutzung von persistentem Storage ermöglicht und von einer Vielzahl der oben genannten NetApp Storage-Optionen unterstützt wird. Es handelt sich um eine Open-Source-Software, die von NetApp gewartet und unterstützt wird.

Astra Trident CSI feature highlights



CSI specific <ul style="list-style-type: none">• CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies• CSI topology• Volume expansion	Security <ul style="list-style-type: none">• Dynamic-export policy management• iSCSI initiator-groups dynamic management• iSCSI bidirectional CHAP
Control <ul style="list-style-type: none">• Storage and performance consumption• Monitoring• Volume Import• Cross Namespace Volume Access	Installation methods <ul style="list-style-type: none">• Binary• Helm chart• Operator• GitOps
Choose your access mode <ul style="list-style-type: none">• RWO (ReadWriteOnce, i.e 1↔1)• RWX (ReadWriteMany, i.e 1↔n)• ROX (ReadOnlyMany)• RWOP (ReadWriteOnce POD)	Choose your protocol <ul style="list-style-type: none">• NFS• SMB• iSCSI

Geschäftskritische Container-Workloads benötigen mehr als nur persistente Volumes. Ihre Datenmanagement-Anforderungen erfordern auch den Schutz und die Migration der Kubernetes-Objekte für die Applikation.



Neben Benutzerdaten umfassen Applikationsdaten kubernetes-Objekte. Folgende Beispiele sind vorhanden: - kubernetes-Objekte wie Pods-Spezifikationen, PVCs, Implementierungen, Services – benutzerdefinierte Konfigurationsobjekte wie Konfigurationszuordnungen und -Geheimnisse – persistente Daten wie Snapshot-Kopien, Backups, Klone – benutzerdefinierte Ressourcen wie CRS und CRDs

NetApp Astra Control ist sowohl als vollständig gemanagte als auch als selbst gemanagte Software erhältlich und bietet Orchestrierung für solides Applikations-Datenmanagement. Siehe "[Astra-Dokumentation](#)" Weitere Informationen zur Astra Produktfamilie.

Diese Referenzdokumentation unterstützt die Validierung der Migration und des Schutzes von Container-basierten Applikationen, die auf der RedHat OpenShift Container-Plattform über das NetApp Astra Control Center implementiert werden. Darüber hinaus bietet die Lösung allgemeine Details zur Bereitstellung und zur Verwendung von Red hat Advanced Cluster Management (ACM) für die Verwaltung der Container-Plattformen. In diesem Dokument werden auch Einzelheiten zur Integration von NetApp Storage in Container-Plattformen mit Red hat OpenShift mithilfe der Astra Trident CSI-bereitstellung erläutert. Astra Control Center wird auf dem Hub-Cluster bereitgestellt und wird für das Management der Container-Applikationen und ihres Lebenszyklus von persistentem Storage verwendet. Schließlich bietet es eine Lösung für Replizierung, Failover und Failback für Container-Workloads auf gemanagten Red hat OpenShift-Clustern in AWS (ROSA), die Amazon FSX für NetApp ONTAP (FSxN) als persistenten Storage verwenden.

NetApp Lösung mit Container-Plattform-Workloads von Red hat OpenShift auf VMware

Falls Kunden ihre modernen Container-Applikationen in ihren privaten Datacentern auf einer Infrastruktur ausführen müssen, ist dies möglich. Sie sollten die Container-Plattform Red hat OpenShift (OCP) planen und bereitstellen, um eine erfolgreiche produktionsbereite Umgebung für die Bereitstellung ihrer Container-Workloads zu

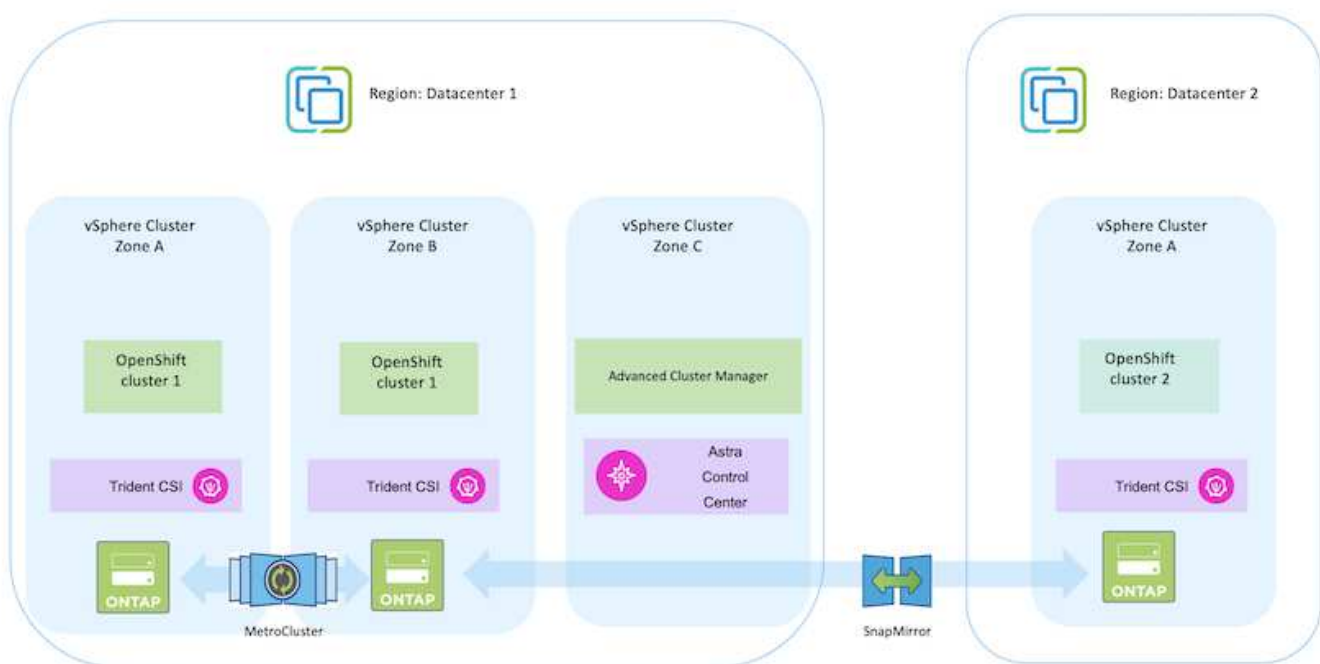
schaffen. Die OCP Cluster können auf VMware oder Bare Metal bereitgestellt werden.

NetApp ONTAP Storage bietet Datensicherung, Zuverlässigkeit und Flexibilität für Container-Implementierungen. Astra Trident dient als dynamische Storage-bereitstellung zur Nutzung von persistentem ONTAP Storage für statusorientierte Applikationen von Kunden. Astra Control Center kann zur Orchestrierung der vielen Datenmanagementanforderungen zustandsbehafteter Applikationen eingesetzt werden, wie zum Beispiel Datensicherung, Migration und Business Continuity.

Mit VMware vSphere bietet NetApp ONTAP Tools ein vCenter Plug-in, das zur Bereitstellung von Datenspeichern verwendet werden kann. Wenden Sie Tags an und verwenden Sie es mit OpenShift zum Speichern der Node-Konfiguration und -Daten. NVMe-basierter Storage bietet eine niedrigere Latenz und hohe Performance.

Diese Lösung bietet Details zur Datensicherung und Migration von Container-Workloads mithilfe von Astra Control Center. Für diese Lösung werden die Container-Workloads auf Red hat OpenShift-Clustern auf vSphere innerhalb der On-Premises-Umgebung bereitgestellt. HINWEIS: Wir werden in Zukunft eine Lösung für Container-Workloads auf OpenShift-Clustern auf Bare-Metal bereitstellen.

Datensicherungs- und Migrationslösung für Container-Workloads mit OpenShift mithilfe von Astra Control Center



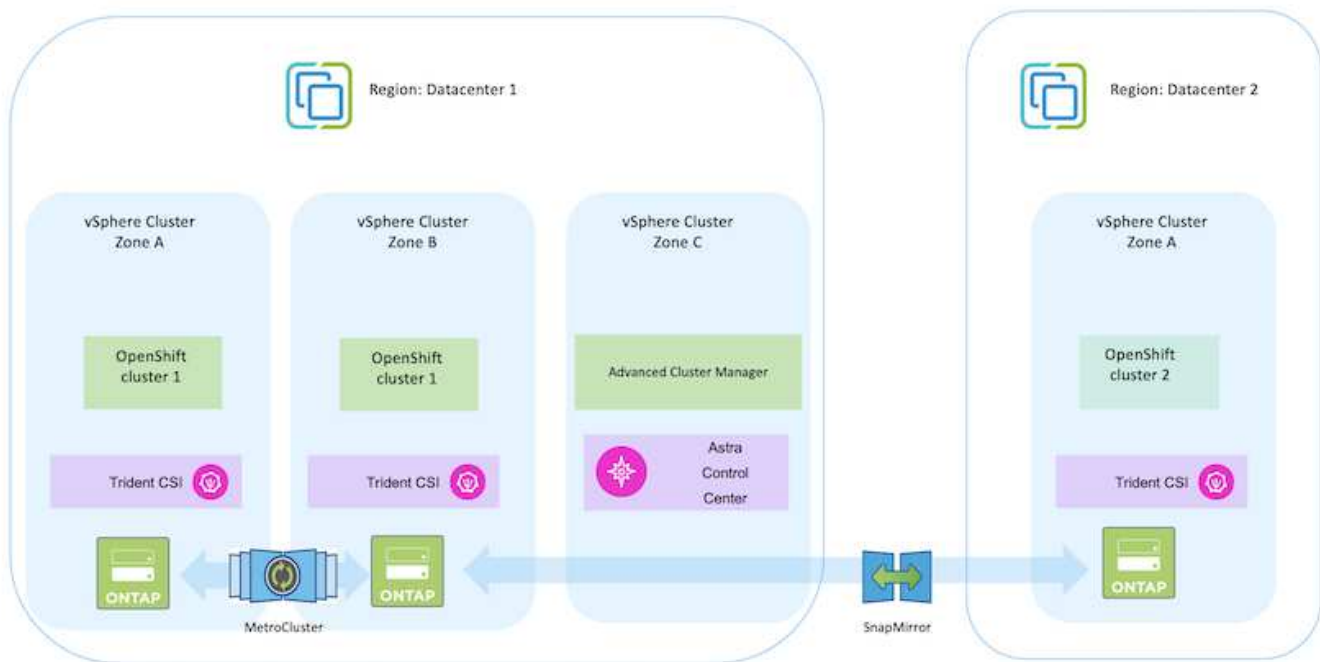
Bereitstellung und Konfiguration der Container-Plattform Red hat OpenShift unter VMware

Dieser Abschnitt beschreibt einen allgemeinen Workflow, in dem erläutert wird, wie OpenShift-Cluster eingerichtet und gemanagt und zustandsbehaftete Anwendungen auf ihnen verwaltet werden. Es zeigt die Nutzung von NetApp ONTAP Storage-Arrays mit Hilfe von Astra Trident zur Bereitstellung persistenter Volumes. Einzelheiten zur Nutzung von Astra Control Center für die Durchführung von Datensicherungs- und Migrationsaktivitäten für die zustandsbehafteten Applikationen werden bereitgestellt.



Es gibt verschiedene Möglichkeiten, Red hat OpenShift Container Platform Cluster bereitzustellen. Diese allgemeine Beschreibung des Setups enthält Dokumentations-Links für die spezifische verwendete Methode. Weitere Methoden finden Sie in den entsprechenden Links im "[Ressourcen](#)".

Im folgenden Diagramm sind die in einem Datacenter unter VMware implementierten Cluster dargestellt.



Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

Bereitstellung und Konfiguration einer CentOS VM

- Sie wird in der VMware vSphere Umgebung implementiert.
- Mit dieser VM werden einige Komponenten wie NetApp Astra Trident und das NetApp Astra Control Center für die Lösung implementiert.
- Auf dieser VM wird während der Installation ein Root-Benutzer konfiguriert.

OpenShift-Container-Plattform-Cluster auf VMware vSphere (Hub-Cluster) implementieren und konfigurieren

Beachten Sie die Anweisungen zum ["Unterstützte Bereitstellung"](#) Methode zum Bereitstellen eines OCP-Clusters.



Denken Sie daran: - Erstellen Sie ssh öffentlichen und privaten Schlüssel für den Installer zur Verfügung zu stellen. Mit diesen Schlüsseln können Sie sich bei Bedarf bei den Master- und Worker-Knoten anmelden. - Laden Sie das Installationsprogramm vom unterstützten Installer herunter. Dieses Programm wird zum Booten der VMs verwendet, die Sie in der VMware vSphere-Umgebung für die Master- und Worker-Knoten erstellen. - VMs sollten die Mindestanforderung an CPU, Arbeitsspeicher und Festplatte haben. (Siehe vm Create-Befehle auf ["Das"](#) Seite für den Master- und den Worker-Knoten, die diese Informationen bereitstellen) - die diskUUID sollte auf allen VMs aktiviert sein. - Erstellen Sie mindestens 3 Knoten für Master und 3 Knoten für worker. - Sobald sie vom Installer entdeckt werden, aktivieren Sie die VMware vSphere Integration Toggle-Taste.

Installieren Sie Advanced Cluster Management auf dem Hub-Cluster

Diese wird mit dem Advanced Cluster Management Operator auf dem Hub-Cluster installiert. Beachten Sie die Anweisungen ["Hier"](#).

Installieren Sie eine interne Red hat Quay-Registrierung auf dem Hub-Cluster.

- Zum Push des Astra-Images ist eine interne Registrierung erforderlich. Eine interne Quay-Registrierung wird über den Operator im Hub-Cluster installiert.
- Beachten Sie die Anweisungen ["Hier"](#)

Zwei zusätzliche OCP-Cluster installieren (Quelle und Ziel)

- Die zusätzlichen Cluster können über die ACM auf dem Hub-Cluster bereitgestellt werden.
- Beachten Sie die Anweisungen ["Hier"](#).

Konfigurieren Sie den NetApp ONTAP Storage

- Installation eines ONTAP-Clusters mit Verbindung zu den OCP-VMs in der VMware-Umgebung
- Erstellen Sie eine SVM.
- Konfigurieren Sie NAS-Daten-LIF für den Zugriff auf den Storage in der SVM.

Installation von NetApp Trident auf den OCP-Clustern

- NetApp Trident lässt sich in allen drei Clustern installieren: Hub-, Quell- und Ziel-Cluster
- Beachten Sie die Anweisungen ["Hier"](#).
- Erstellen Sie ein Storage-Backend für ontap-nas.
- Erstellen einer Storage-Klasse für ontap-nas
- Siehe Anweisungen ["Hier"](#).

Installation von NetApp Astra Control Center

- NetApp Astra Control Center wird über den Astra Operator auf dem Hub-Cluster installiert.
- Beachten Sie die Anweisungen ["Hier"](#).

Wichtige Fakten: * Laden Sie das NetApp Astra Control Center Image von der Support-Website herunter.
* Drücken Sie das Bild auf eine interne Registrierung. * Siehe Anweisungen [hier](#).

Stellen Sie eine Anwendung auf dem Quellcluster bereit

Verwenden Sie OpenShift GitOps, um eine Anwendung zu implementieren. (Z. B. Postgres, Ghost)

Fügen Sie die Quell- und Ziel-Cluster zu Astra Control Center hinzu.

Nachdem Sie dem Astra Control-Management einen Cluster hinzugefügt haben, können Sie Apps auf dem Cluster (außerhalb von Astra Control) installieren und anschließend in Astra Control auf der Seite Applications die Apps und ihre Ressourcen definieren. Siehe ["Beginnen Sie mit dem Management von Apps im Bereich Astra Control Center"](#).

Der nächste Schritt besteht darin, das Astra Control Center für Datensicherung und Datenmigration von der Quell- zum Ziel-Cluster zu nutzen.

Datensicherung mit Astra

Auf dieser Seite werden die Datenschutzooptionen für Container-basierte Red hat OpenShift-Anwendungen angezeigt, die unter VMware vSphere mit Astra Control Center (ACC) ausgeführt werden.

Wenn Benutzer ihre Anwendungen mit Red hat OpenShift modernisieren, sollte eine Datenschutzstrategie eingerichtet werden, um sie vor versehentlichem Löschen oder anderen menschlichen Fehlern zu schützen. Häufig ist auch eine Sicherungsstrategie für gesetzliche Vorschriften oder Compliance-Zwecke erforderlich, um ihre Daten vor einem Diaster zu schützen.

Die Anforderungen an die Datensicherung reichen von dem Zurücksetzen auf eine zeitpunktgenaue Kopie bis hin zum automatischen Failover auf eine andere Fehlerdomäne ohne menschliches Eingreifen. Viele Kunden entscheiden sich für ONTAP als bevorzugte Storage-Plattform für ihre Kubernetes-Applikationen, da sie umfassende Funktionen wie Mandantenfähigkeit, Multiprotokoll, hohe Performance und Kapazität, Replizierung und Caching für Standorte an mehreren Standorten sowie Sicherheit und Flexibilität bieten.

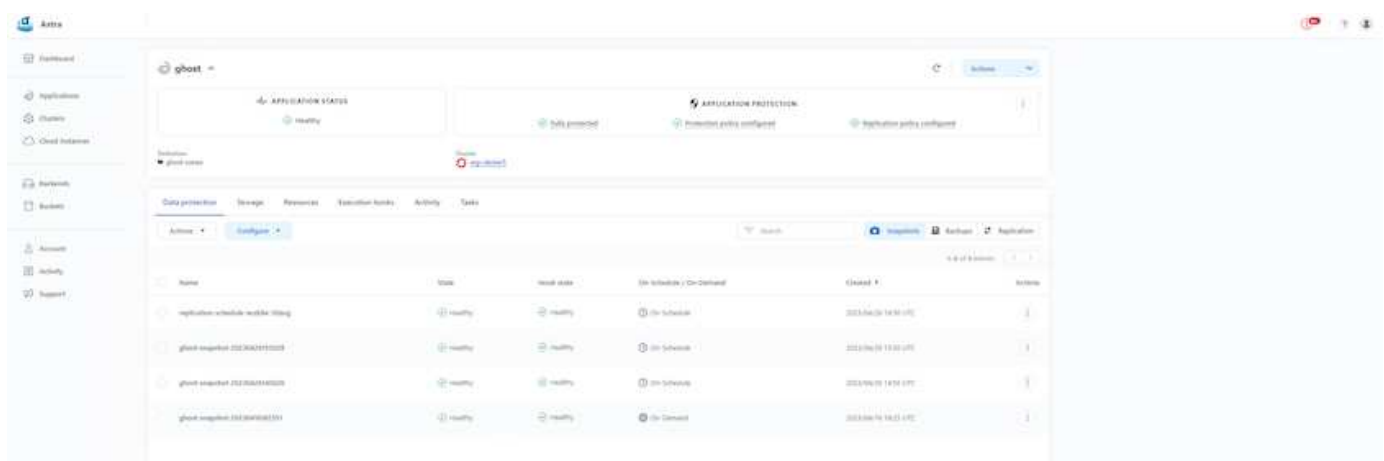
Die Datensicherung in ONTAP kann über Ad-hoc oder richtliniengesteuert erfolgen - **Snapshot - Backup und Restore**

Sowohl Snapshot-Kopien als auch Backups schützen die folgenden Datentypen: - **Die Anwendungsmetadaten, die den Status der Applikation darstellen** - **alle mit der Applikation verknüpften persistenten Datenvolumes** - **alle Ressourcenartefakte der Applikation**

Momentaufnahme mit ACC

Mithilfe von Snapshot mit ACC kann eine Point-in-Time-Kopie der Daten erfasst werden. Sicherungsrichtlinie definiert die Anzahl der zu bewahrenden Snapshot Kopien. Die minimale verfügbare Terminplanoption ist stündlich. Manuelle On-Demand Snapshot Kopien können jederzeit und in kürzeren Intervallen als geplante Snapshot Kopien erstellt werden. Snapshot-Kopien werden auf demselben bereitgestellten Volume wie die Applikation gespeichert.

Snapshot mit ACC konfigurieren

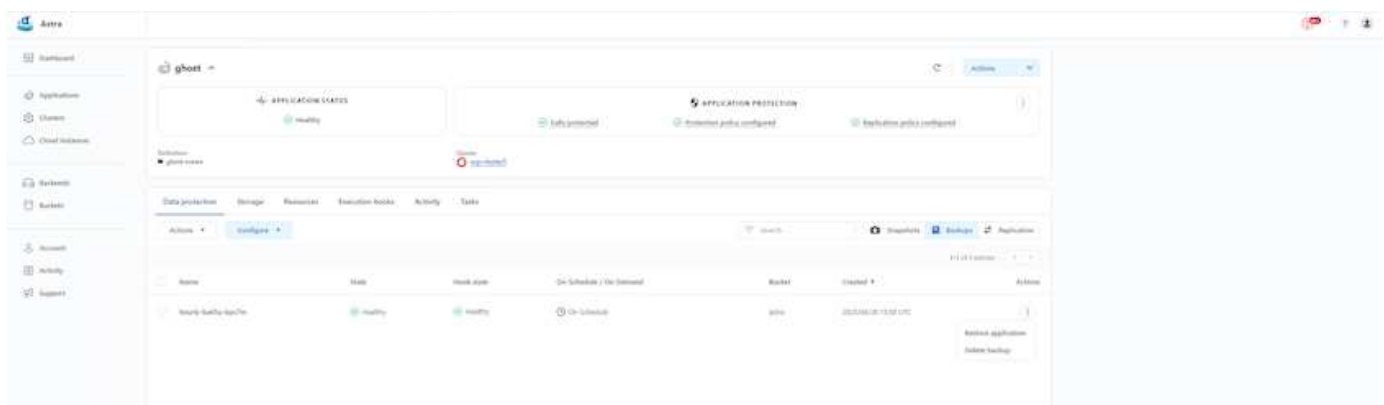


Sichern und Wiederherstellen mit ACC

Ein Backup basiert auf einem Snapshot. ACC kann Snapshot Kopien mithilfe von CSI erstellen und Backups mithilfe der zeitpunktgenauen Snapshot Kopie durchführen. Das Backup wird in einem externen Objektspeicher abgelegt (alle s3-kompatibel einschließlich ONTAP S3 an einem anderen Standort). Die Schutzrichtlinie kann für geplante Backups und die Anzahl der zu bewahrenden Backup-Versionen konfiguriert werden. Der minimale RPO beträgt eine Stunde.

Wiederherstellen einer Anwendung aus einer Sicherung mit ACC

ACC stellt die Applikation aus dem S3-Bucket wieder her, in dem die Backups gespeichert werden.



Anwendungsspezifische Ausführungshaken

Darüber hinaus können Ausführungshaken so konfiguriert werden, dass sie in Verbindung mit einer Datenschutzoperation einer verwalteten App ausgeführt werden. Obwohl die Datensicherungsfunktionen auf Storage-Array-Ebene verfügbar sind, sind für Backups und Restores häufig zusätzliche Schritte erforderlich, um die Konsistenz der Applikationen zu erhöhen. Die App-spezifischen zusätzlichen Schritte können sein: - Vor oder nach dem Erstellen einer Snapshot-Kopie. - Vor oder nach der Erstellung einer Sicherung. - Nach der Wiederherstellung aus einer Snapshot-Kopie oder Backup.

Astra Control kann diese applikationsspezifischen Schritte ausführen, die als benutzerdefinierte Skripte, sogenannte Execution Hooks, codiert werden.

["NetApp Verda GitHub Projekt"](#) Diese Lösung bietet Ausführungshaken für gängige Cloud-native Applikationen und ermöglicht so einen einfachen, robusten und einfach zu orchestrierten Schutz von Applikationen. Sie können sich gerne an diesem Projekt beteiligen, wenn Sie genügend Informationen für eine Anwendung haben, die sich nicht im Repository befindet.

Beispiel-Ausführungshaken für Pre-Snapshot einer redis-Anwendung.

Edit execution hook

HOOK DETAILS

Operation: Pre-snapshot

Hook arguments (optional): 1 pre

Hook name: redis-pre-snapshot

CONTAINER IMAGES

☐ Apply to all container images

Use a regular expression to target container images for the hook.

Container image names to match: redis

SCRIPT

+ Add

Search

Name ↓

- ☐ mariadb_mysql.sh
- ☐ postgresql.sh
- ☒ redis_hook.sh

EXECUTION HOOKS

Execution hooks allow Astra Control to execute your own custom scripts before or after a snapshot.

Read more in [Manage application execution hooks](#)

Cancel Save

Replikation mit ACC

Für regionalen Schutz oder für eine Lösung mit niedriger RPO und RTO, kann eine Applikation auf eine andere

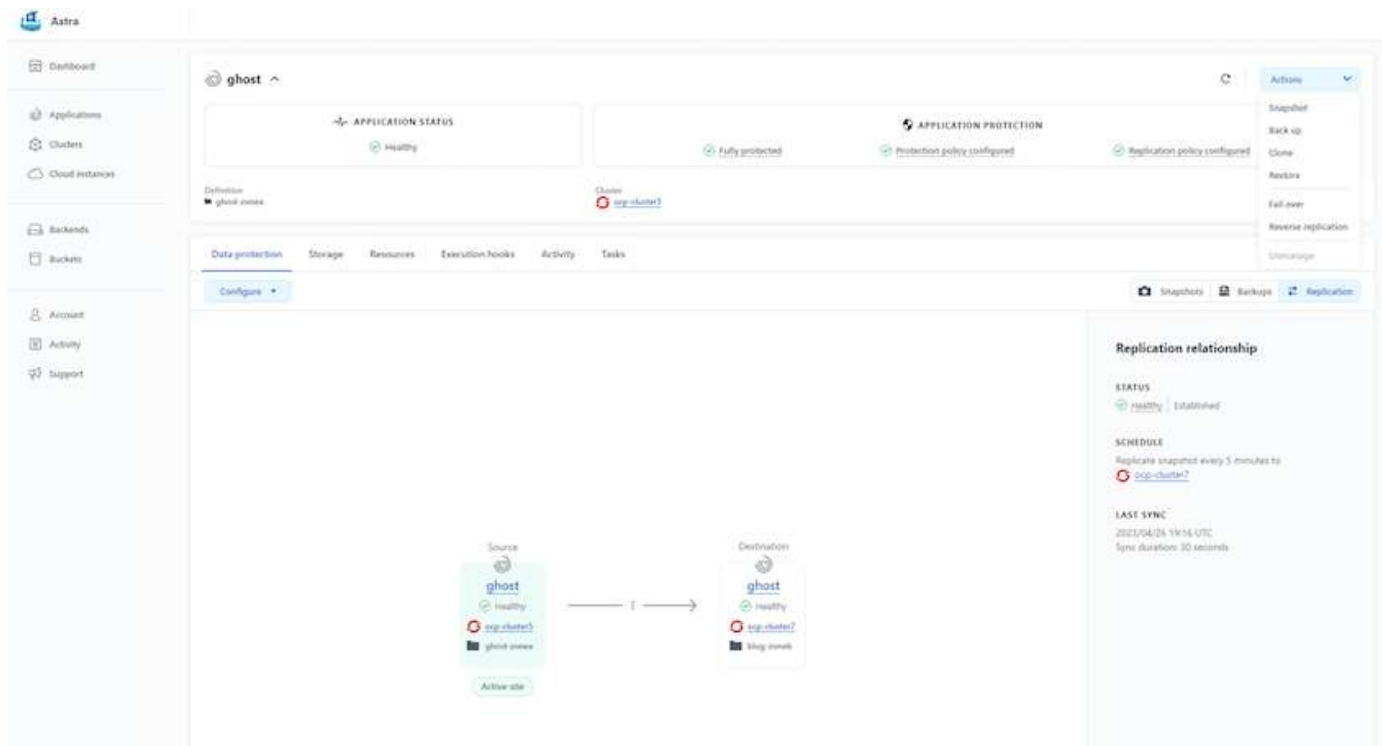
Kubernetes-Instanz repliziert werden, die an einem anderen Standort, vorzugsweise in einer anderen Region, ausgeführt wird. ACC verwendet ONTAP Async SnapMirror mit einem Recovery Point Objective von nur 5 Minuten. Die Replizierung wird durch eine Replizierung zu ONTAP durchgeführt. Bei einem Failover werden die Kubernetes-Ressourcen im Ziel-Cluster erstellt.



Beachten Sie, dass sich die Replizierung von den Backup- und Restore-Prozessen unterscheidet, bei denen das Backup auf S3 erfolgt und die Wiederherstellung von S3 durchgeführt wird. Weitere Details zu den Unterschieden zwischen den beiden Arten der Datensicherung finden Sie unter folgendem Link: [here](#).

Siehe "[Hier](#)" Anweisungen zur Einrichtung von SnapMirror finden Sie.

SnapMirror mit ACC



speichertreiber für san-Economy und nas-Economy unterstützen keine Replikationsfunktion. Siehe "[Hier](#)" Entnehmen.

Demovideo:

["Demo-Video über Disaster Recovery mit Astra Control Center"](#)

Datensicherung mit Astra Control Center

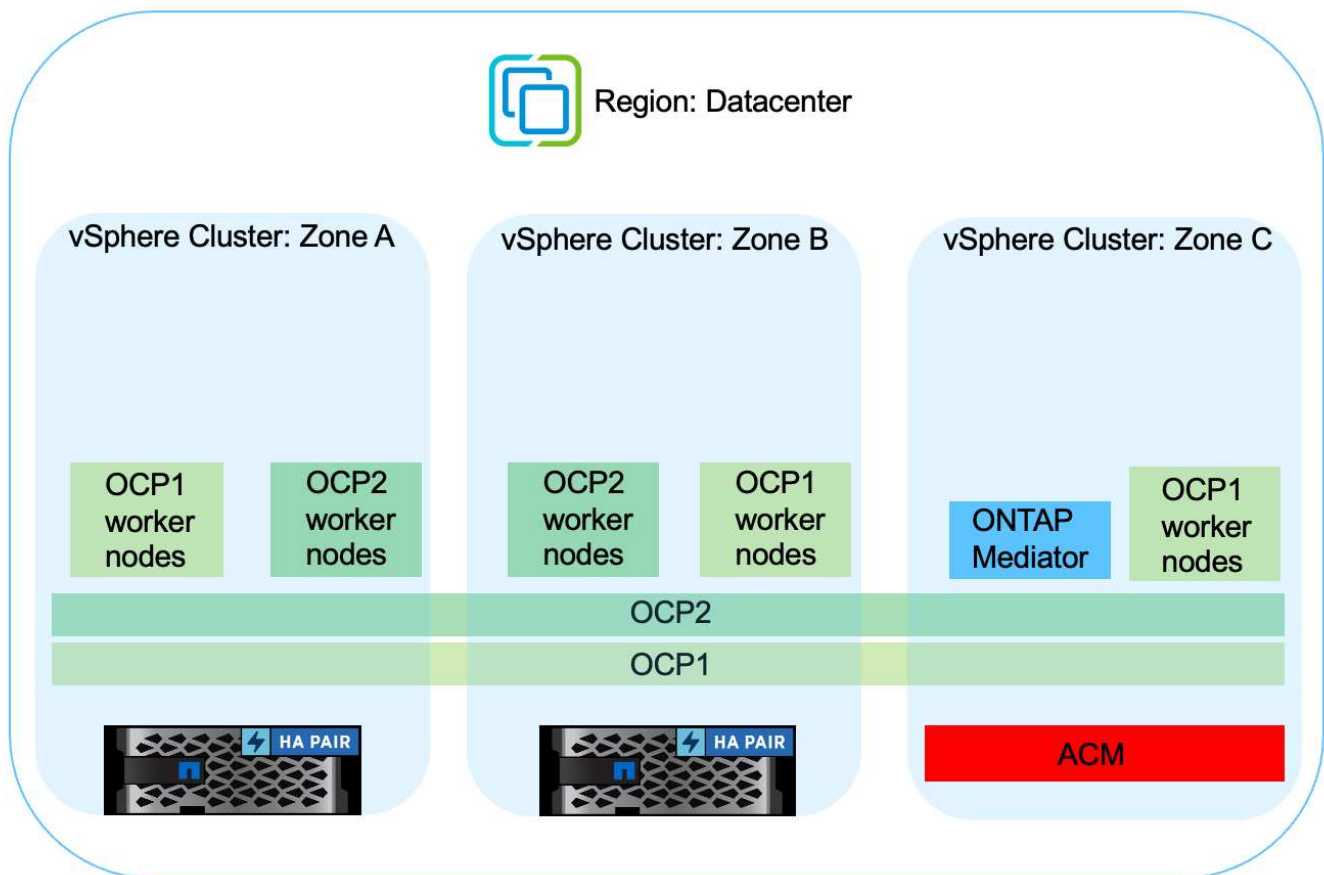
Business Continuity mit MetroCluster

Die meisten unserer Hardware-Plattform für ONTAP verfügt über Hochverfügbarkeitsfunktionen zum Schutz vor Geräteausfällen, um ein diasteres Recovery zu vermeiden. Um jedoch vor Feuer oder anderen Zwischenfällen zu schützen und das Geschäft mit RPO von null und RTO von geringem Wert fortzuführen, kommt oft eine MetroCluster Lösung zum Einsatz.

Kunden, die derzeit über ein ONTAP System verfügen, können sich auf MetroCluster erweitern, indem sie

unterstützte ONTAP Systeme innerhalb der genannten Entfernungseinschränkungen hinzufügen, um Disaster Recovery auf Zonenebene durchzuführen. Astra Trident unterstützt das CSI (Container Storage Interface) NetApp ONTAP, einschließlich der MetroCluster-Konfiguration sowie weitere Optionen wie Cloud Volumes ONTAP, Azure NetApp Files, AWS FSX für NetApp ONTAP usw. Astra Trident bietet fünf Storage-Treiberoptionen für ONTAP und alle werden für die MetroCluster Konfiguration unterstützt. Siehe ["Hier"](#) Weitere Informationen zu von Astra Trident unterstützten ONTAP Storage-Treibern.

Für die MetroCluster-Lösung ist eine Layer-2-Netzwerkerweiterung oder -Fähigkeit erforderlich, um von beiden Fehlerdomänen aus auf dieselbe Netzwerkadresse zuzugreifen. Sobald die MetroCluster-Konfiguration eingerichtet ist, ist die Lösung für Applikationseigentümer transparent, da alle Volumes in der MetroCluster svm gesichert sind und die Vorteile von SyncMirror (RPO Null) nutzen.



Geben Sie für die Trident Back-End-Konfiguration (TBC) bei Verwendung der MetroCluster-Konfiguration keine Daten-LIF und SVM an. Geben Sie die SVM-Management-IP für die Management-LIF an und verwenden Sie die vsadmin-Rollen-Anmeldedaten.

Einzelheiten zu den Datensicherungsfunktionen von Astra Control Center sind erhältlich ["Hier"](#)

Datenmigration über Astra Control Center

Auf dieser Seite werden die Optionen für die Datenmigration von Container-Workloads auf Red hat OpenShift-Clustern mit Astra Control Center (ACC) angezeigt.

Kubernetes-Applikationen müssen häufig von einer Umgebung in eine andere verschoben werden. Um eine Applikation zusammen mit ihren persistenten Daten zu migrieren, kann NetApp ACC genutzt werden.

Datenmigration zwischen verschiedenen Kubernetes-Umgebungen

ACC unterstützt verschiedene Kubernetes-Varianten, darunter Google Anthos, Red hat OpenShift, Tanzu Kubernetes Grid, Rancher Kubernetes Engine, Upstream Kubernetes, Usw. Weitere Details finden Sie unter ["Hier"](#).

Um die Anwendung von einem Cluster zu einem anderen zu migrieren, können Sie eine der folgenden Funktionen von ACC verwenden:

- **Replikation**
- **Sicherung und Wiederherstellung**
- **Klon**

Siehe ["Abschnitt zur Datensicherung"](#) Für die Optionen **Replikation und Backup und Restore**.

Siehe ["Hier"](#) Für weitere Details über **Klonen**.



Die Astra Replizierungsfunktion wird nur mit der Trident Container Storage Interface (CSI) unterstützt. Die Replikation wird jedoch nicht von nas-Economy- und san-Economy-Treibern unterstützt.

Durchführen der Datenreplikation mit ACC

The screenshot displays the Astra console interface for configuring and monitoring a replication relationship. On the left is a navigation sidebar with options like Dashboard, Applications, Clusters, Cloud instances, Backends, Buckets, Account, Activity, and Support. The main panel shows the 'ghost' application configuration. At the top, there are status boxes for 'APPLICATION STATUS' (Healthy), 'APPLICATION PROTECTION' (Fully protected), and 'Protection policy configured'. Below this, a diagram illustrates the replication relationship between a 'Source' cluster (ghost) and a 'Destination' cluster (ghost). The 'Source' cluster is labeled 'Active site' and the 'Destination' is labeled 'Blog posts'. A 'Replication relationship' panel on the right provides details: STATUS is 'Healthy' and 'Established'; SCHEDULE is 'Replicate snapshot every 5 minutes to ocp-cluster2'; and LAST SYNC is '2023/04/26 11:14 UTC' with a 'Sync duration: 30 seconds'. An 'Actions' menu on the far right includes options like Snapshot, Back up, Clone, Restore, Fail over, Reverse replication, and Unmanage.

NetApp Hybrid-Multi-Cloud-Lösungen für Container-Workloads mit Red hat OpenShift

Überblick

Bei NetApp beobachten wir eine deutliche Zunahme bei Kunden, die ihre älteren Enterprise-Applikationen

modernisieren und neue Applikationen mithilfe von Containern und Orchestrierungsplattformen auf Basis von Kubernetes erstellen. Die Red hat OpenShift Container Platform ist ein Beispiel, das wir von vielen unserer Kunden angenommen sehen.

Immer mehr Kunden beginnen mit der Einführung von Containern in ihrem Unternehmen. NetApp ist perfekt aufgestellt, um die persistenten Storage-Anforderungen ihrer zustandsbehafteten Applikationen und klassischen Datenmanagementanforderungen zu erfüllen, beispielsweise Datensicherung, Datensicherheit und Datenmigration. Diese Bedürfnisse werden jedoch mit verschiedenen Strategien, Werkzeugen und Methoden erfüllt.

NetApp ONTAP basierte Storage-Optionen, die unten aufgeführt sind, bieten Sicherheit, Datensicherung, Zuverlässigkeit und Flexibilität für Container- und Kubernetes-Implementierungen.

- Automatisierter, lokaler Storage:
 - NetApp Fabric Attached Storage (FAS), NetApp All-Flash-FAS-Arrays (AFF), NetApp All-SAN-Arrays (ASA) und ONTAP Select
- Von Providern gemanagter Storage in On-Premises:
 - NetApp Keystone stellt Storage-as-a-Service (STaaS) bereit
- Automatisierter Storage in der Cloud:
 - NetApp Cloud Volumes ONTAP (CVO) bieten Self-Managed-Storage in den Hyperscalern
- Von Providern gemanagter Storage in der Cloud:
 - Cloud Volumes Service für Google Cloud (CVS), Azure NetApp Files (ANF) und Amazon FSX für NetApp ONTAP bieten vollständig gemanagten Storage in den Hyperscalern

ONTAP feature highlights



Storage Administration <ul style="list-style-type: none"> Multi-tenancy FlexVol & FlexGroup LUN Quotas ONTAP CLI & API System Manager & BlueXP 	Performance & Scalability <ul style="list-style-type: none"> FlexCache FlexClone nconnect, session trunking, multipathing Scale-out clusters
Availability & Resilience <ul style="list-style-type: none"> Multi-AZ HA deployment (MetroCluster) SnapShot & SnapRestore SnapMirror SnapMirror Business Continuity SnapMirror Cloud 	Access Protocols <ul style="list-style-type: none"> NFS –v3, v4, v4.1, v4.2 SMB – v2, v3 iSCSI Multi-protocol access
Storage Efficiency <ul style="list-style-type: none"> Deduplication & Compression Compaction Thin provisioning Data Tiering (Fabric Pool) 	Security & Compliance <ul style="list-style-type: none"> Fpolicy & Vscan Active Directory integration LDAP & Kerberos Certificate based authentication

NetApp BlueXP ermöglicht Ihnen das Management Ihrer gesamten Storage- und Datenbestände über eine einzige Managementoberfläche.

Mit BlueXP können Sie Cloud-Storage erstellen und verwalten (z. B. Cloud Volumes ONTAP und Azure NetApp Files), Daten verschieben, schützen und analysieren sowie zahlreiche lokale und Edge-Storage-Geräte kontrollieren.

NetApp Astra Trident ist ein CSI-konformer Storage Orchestrator, der eine schnelle und einfache Nutzung von persistentem Storage ermöglicht und von einer Vielzahl der oben genannten NetApp Storage-Optionen unterstützt wird. Es handelt sich um eine Open-Source-Software, die von NetApp gewartet und unterstützt wird.

Astra Trident CSI feature highlights



CSI specific <ul style="list-style-type: none"> • CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies • CSI topology • Volume expansion 	Security <ul style="list-style-type: none"> • Dynamic-export policy management • iSCSI initiator-groups dynamic management • iSCSI bidirectional CHAP
Control <ul style="list-style-type: none"> • Storage and performance consumption • Monitoring • Volume Import • Cross Namespace Volume Access 	Installation methods <ul style="list-style-type: none"> • Binary • Helm chart • Operator • GitOps
Choose your access mode <ul style="list-style-type: none"> • RWO (ReadWriteOnce, i.e 1↔1) • RWX (ReadWriteMany, i.e 1↔n) • ROX (ReadOnlyMany) • RWOP (ReadWriteOnce POD) 	Choose your protocol <ul style="list-style-type: none"> • NFS • SMB • iSCSI

Geschäftskritische Container-Workloads benötigen mehr als nur persistente Volumes. Ihre Datenmanagement-Anforderungen erfordern auch den Schutz und die Migration der Kubernetes-Objekte für die Applikation.



Neben Benutzerdaten umfassen Applikationsdaten kubernetes-Objekte. Folgende Beispiele sind vorhanden: - kubernetes-Objekte wie Pods-Spezifikationen, PVCs, Implementierungen, Services – benutzerdefinierte Konfigurationsobjekte wie Konfigurationszuordnungen und -Geheimnisse – persistente Daten wie Snapshot-Kopien, Backups, Klone – benutzerdefinierte Ressourcen wie CRS und CRDs

NetApp Astra Control ist sowohl als vollständig gemanagte als auch als selbst gemanagte Software erhältlich und bietet Orchestrierung für solides Applikations-Datenmanagement. Siehe "[Astra-Dokumentation](#)" Weitere Informationen zur Astra Produktfamilie.

Diese Referenzdokumentation unterstützt die Validierung der Migration und des Schutzes von Container-basierten Applikationen, die auf der RedHat OpenShift Container-Plattform über das NetApp Astra Control Center implementiert werden. Darüber hinaus bietet die Lösung allgemeine Details zur Bereitstellung und zur Verwendung von Red hat Advanced Cluster Management (ACM) für die Verwaltung der Container-Plattformen. In diesem Dokument werden auch Einzelheiten zur Integration von NetApp Storage in Container-Plattformen mit Red hat OpenShift mithilfe der Astra Trident CSI-bereitstellung erläutert. Astra Control Center wird auf dem Hub-Cluster bereitgestellt und wird für das Management der Container-Applikationen und ihres Lebenszyklus von persistentem Storage verwendet. Schließlich bietet es eine Lösung für Replizierung, Failover und Failback für Container-Workloads auf gemanagten Red hat OpenShift-Clustern in AWS (ROSA), die Amazon FSX für NetApp ONTAP (FSxN) als persistenten Storage verwenden.

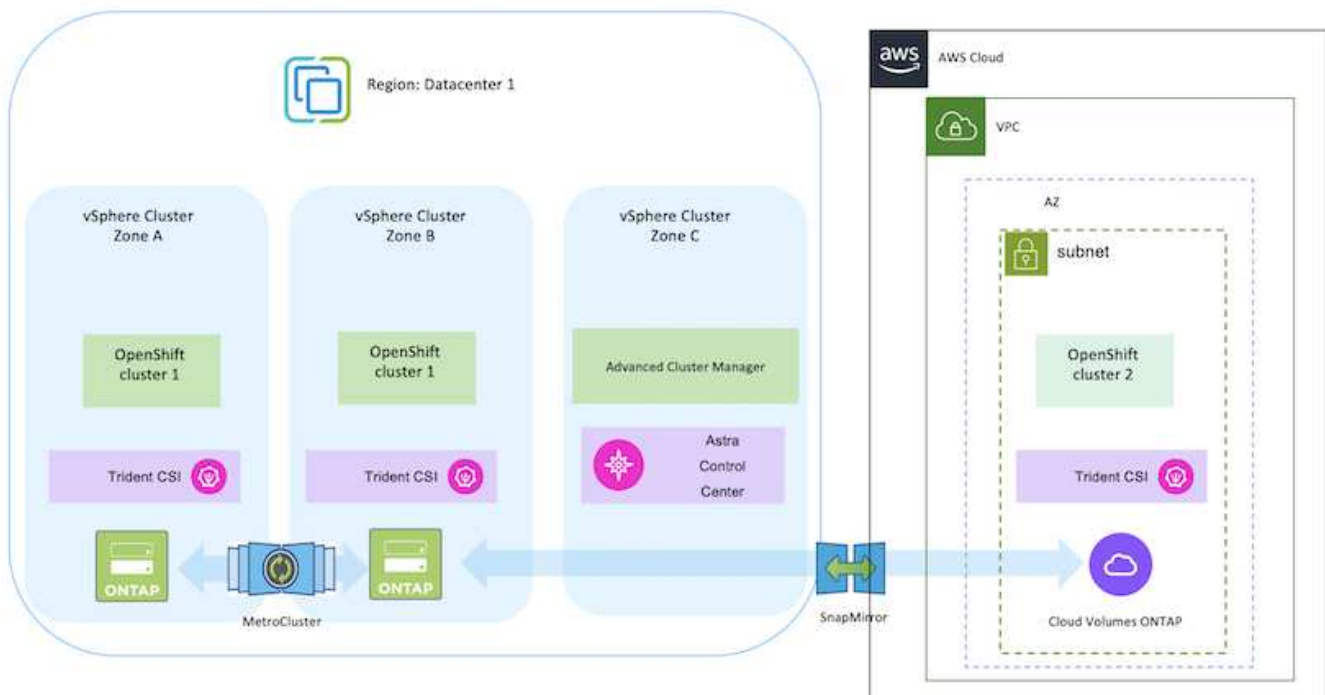
NetApp Lösung mit Container-Plattform-Workloads von Red hat OpenShift in der Hybrid Cloud

Kunden sind möglicherweise an einem Punkt ihrer Modernisierungsstrategie, wenn sie einige ausgewählte Workloads oder alle Workloads aus ihren Datacentern in die Cloud verschieben möchten. Sie können aus verschiedenen Gründen dafür entscheiden, selbst gemanagte OpenShift-Container und selbst gemanagten NetApp Storage in der Cloud zu verwenden. Sie sollten die Container-Plattform Red hat OpenShift (OCP) in der Cloud planen und bereitstellen, um eine erfolgreiche produktionsbereite Umgebung für die Migration ihrer Container-Workloads aus ihren Rechenzentren zu schaffen. Die OCP-Cluster können in ihren Datacentern auf VMware oder Bare Metal bereitgestellt werden und in AWS, Azure oder Google Cloud in der Cloud-Umgebung.

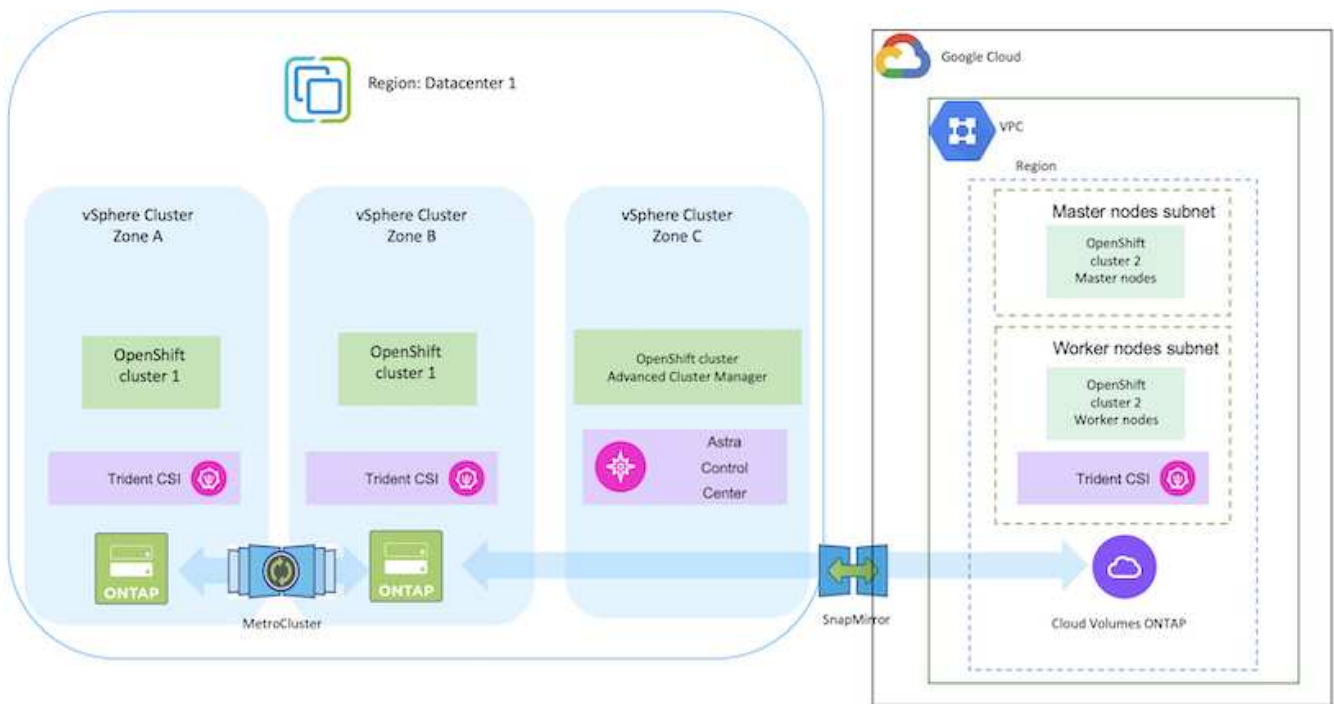
NetApp Cloud Volumes ONTAP Storage bietet Datensicherung, Zuverlässigkeit und Flexibilität für Container-Implementierungen in AWS, Azure und Google Cloud. Astra Trident dient als dynamische Storage-bereitstellung zur Nutzung des persistenten Cloud Volumes ONTAP Storage für zustandsbehaftete Applikationen von Kunden. Astra Control Center kann zur Orchestrierung der vielen Datenmanagementanforderungen zustandsbehafteter Applikationen eingesetzt werden, wie zum Beispiel Datensicherung, Migration und Business Continuity.

Datensicherungslösung und Migrationslösung für OpenShift-Container-Workloads in einer Hybrid Cloud mithilfe von Astra Control Center

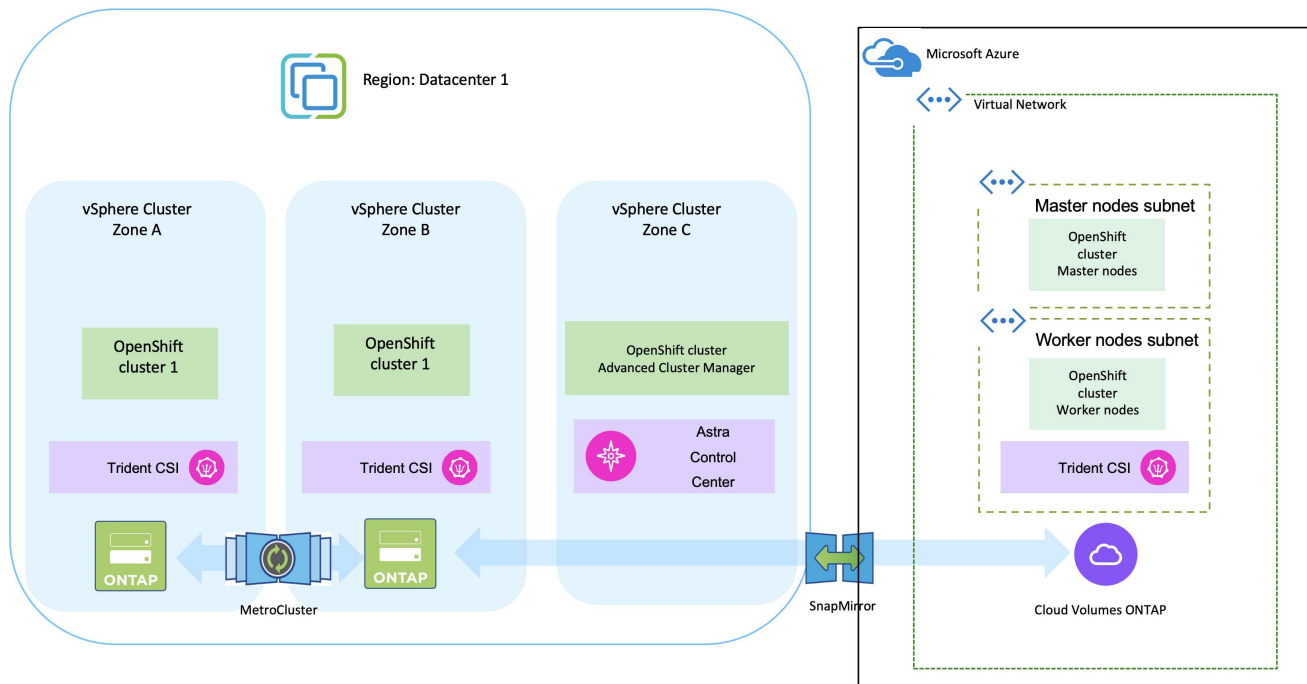
On-Premises- und AWS



On-Premises und Google Cloud



On-Premises-Systeme und Azure Cloud



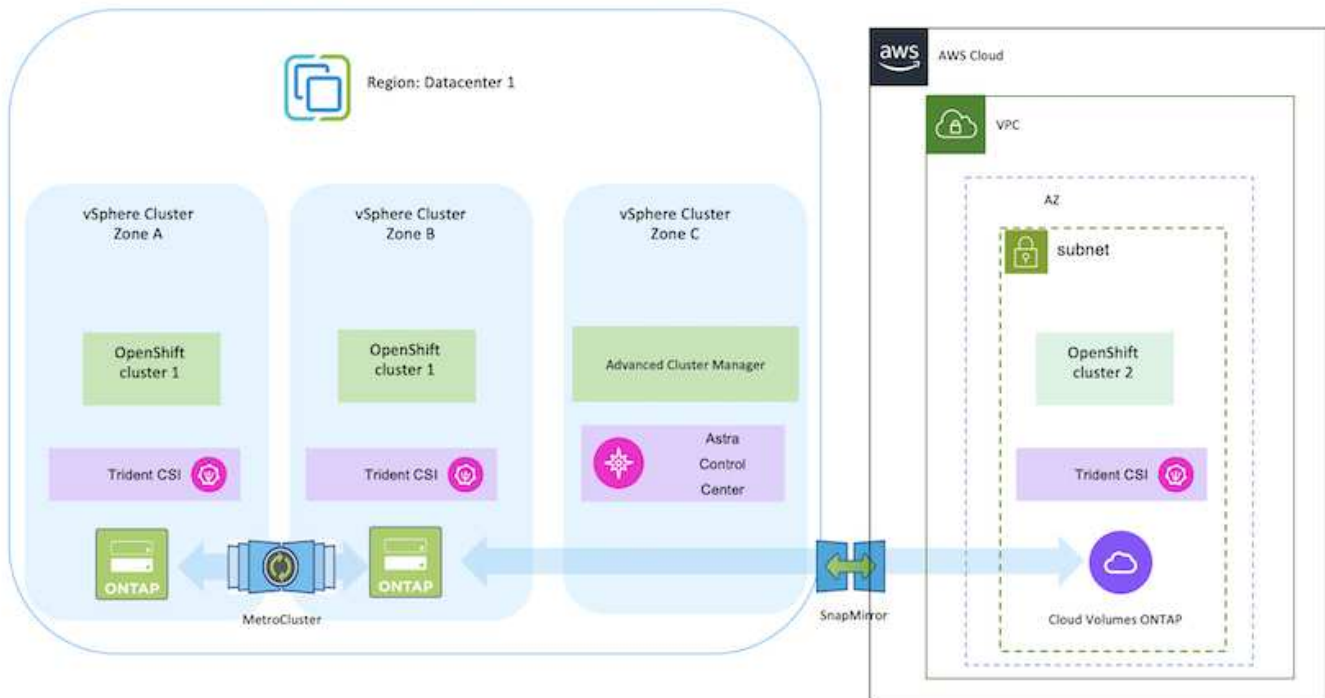
Implementierung und Konfiguration der Container-Plattform Red hat OpenShift auf AWS

In diesem Abschnitt wird ein High-Level-Workflow beschrieben, in dem Sie OpenShift-Cluster in AWS einrichten und managen und zustandsbehaftete Anwendungen darauf implementieren. Es zeigt die Nutzung von NetApp Cloud Volumes ONTAP Storage mit Hilfe von Astra Trident zur Bereitstellung persistenter Volumes. Einzelheiten zur Nutzung von Astra Control Center für die Durchführung von Datensicherungs- und Migrationsaktivitäten für die zustandsbehafteten Applikationen werden bereitgestellt.



Es gibt verschiedene Möglichkeiten zur Implementierung von Red hat OpenShift Container-Plattform-Clustern auf AWS. Diese allgemeine Beschreibung des Setups enthält Dokumentations-Links für die spezifische verwendete Methode. Weitere Methoden finden Sie in den entsprechenden Links im ["Ressourcen"](#).

Das folgende Diagramm zeigt die Cluster, die auf AWS implementiert und über ein VPN mit dem Datacenter verbunden sind.



Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

Installieren Sie über Advanced Cluster Management einen OCP-Cluster in AWS.

- Erstellen Sie eine VPC mit einer Site-to-Site-VPN-Verbindung (mit pfsense), um eine Verbindung zum On-Premises-Netzwerk herzustellen.
- Das Netzwerk vor Ort verfügt über eine Internetverbindung.
- 3 private Subnetze in 3 verschiedenen AZS erstellen.
- Erstellen Sie eine Route 53 private gehostete Zone und einen DNS-Resolver für die VPC.

Erstellen Sie mithilfe des ACM-Assistenten (Advanced Cluster Management) OpenShift-Cluster auf AWS. Siehe Anweisungen "[Hier](#)".



Sie können das Cluster auch in AWS über die OpenShift Hybrid Cloud-Konsole erstellen. Siehe "[Hier](#)" Weitere Anweisungen.



Wenn Sie den Cluster mit ACM erstellen, können Sie die Installation anpassen, indem Sie die yaml-Datei nach dem Ausfüllen der Details in der Formularansicht bearbeiten. Nach dem Erstellen des Clusters können Sie sich über ssh bei den Nodes des Clusters zur Fehlerbehebung oder zur manuellen Konfiguration anmelden. Verwenden Sie den SSH-Schlüssel, den Sie während der Installation angegeben haben, und den Benutzernamen-Kern, um sich anzumelden.

Implementieren Sie Cloud Volumes ONTAP in AWS mit BlueXP.

- Installieren Sie den Connector in einer lokalen VMware-Umgebung. Siehe Anweisungen "[Hier](#)".
- Stellen Sie über den Connector eine CVO-Instanz in AWS bereit. Siehe Anweisungen "[Hier](#)".



Der Connector kann auch in der Cloud-Umgebung installiert werden. Siehe "[Hier](#)" Finden Sie weitere Informationen.

Installation von Astra Trident im OCP Cluster

- Implementieren Sie Trident Operator mit Helm. Siehe Anweisungen "[Hier](#)".
- Back-End und Storage-Klasse erstellen Siehe Anweisungen "[Hier](#)".

Fügen Sie das OCP-Cluster in AWS zum Astra Control Center hinzu.

Fügen Sie das OCP-Cluster in AWS zum Astra Control Center hinzu.

Verwendung der CSI-Topology-Funktion von Trident für Multi-Zone-Architekturen

Heute können Cloud-Provider Kubernetes/OpenShift-Cluster-Administratoren Nodes der zonbasierten Cluster erstellen. Die Nodes können sich in verschiedenen Verfügbarkeitszonen innerhalb einer Region oder über verschiedene Regionen hinweg befinden. Astra Trident verwendet CSI Topology, um die Provisionierung von Volumes für Workloads in einer Multi-Zone-Architektur zu vereinfachen. Mithilfe der CSI Topology-Funktion kann der Zugriff auf Volumes auf einen Teil von Nodes basierend auf Regionen und Verfügbarkeitszonen begrenzt werden. Siehe "[Hier](#)" Entnehmen.



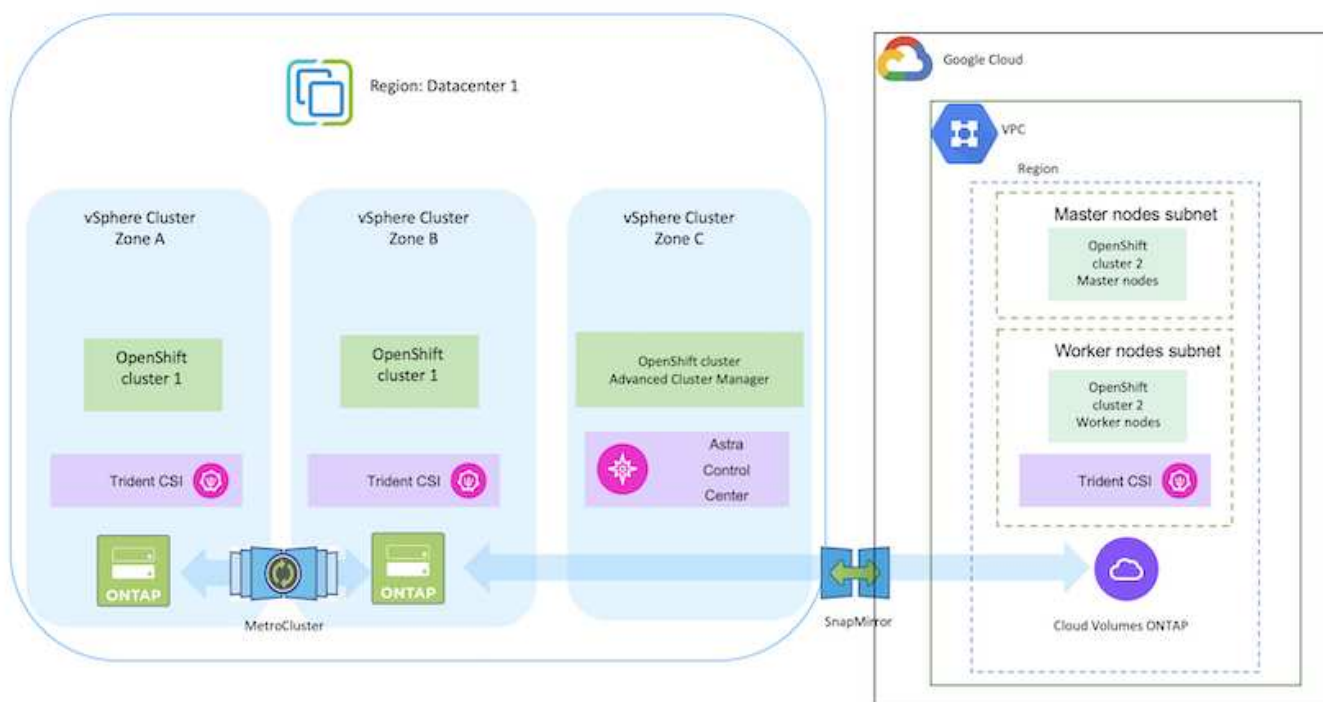
Kubernetes unterstützt zwei Volume-Bindungsmodi: - Wenn **VolumeBindingMode auf Immediate** (Standard) eingestellt ist, erstellt Astra Trident das Volume ohne Topologieorientierung. Persistente Volumes werden erstellt, ohne dass sie von den Planungsanforderungen des anfragenden Pods abhängig sind. - Wenn **VolumeBindingMode auf WaitForFirstConsumer** gesetzt wird, wird die Erstellung und Bindung eines Persistent Volume für eine PVC verzögert, bis ein Pod, der die PVC verwendet, geplant und erstellt wird. Auf diese Weise werden Volumes erstellt, um Planungseinschränkungen zu erfüllen, die durch Topologieanforderungen durchgesetzt werden. Astra Trident Storage-Back-Ends können für die selektive Bereitstellung von Volumes basierend auf Verfügbarkeitszonen entwickelt werden (Topologieorientiertes Back-End). Bei StorageClasses, die ein solches Backend nutzen, wird ein Volume nur erstellt, wenn es von einer Applikation angefordert wird, die in einer unterstützten Region/Zone geplant ist. (Topologieorientierte StorageClass) "[Hier](#)" Entnehmen.

Bereitstellung und Konfiguration der Container-Plattform Red hat OpenShift auf GCP

Bereitstellung und Konfiguration der Container-Plattform Red hat OpenShift auf GCP

Dieser Abschnitt beschreibt einen allgemeinen Workflow zur Einrichtung und Verwaltung von OpenShift-Clustern in GCP und zur Bereitstellung zustandsbehafteter Anwendungen. Es zeigt die Nutzung von NetApp Cloud Volumes ONTAP Storage mit Hilfe von Astra Trident zur Bereitstellung persistenter Volumes. Einzelheiten zur Nutzung von Astra Control Center für die Durchführung von Datensicherungs- und Migrationsaktivitäten für die zustandsbehafteten Applikationen werden bereitgestellt.

Das folgende Diagramm zeigt die auf GCP bereitgestellten und über ein VPN mit dem Datacenter verbundenen Cluster.





Es gibt verschiedene Möglichkeiten, Red hat OpenShift Container Platform Cluster in GCP bereitzustellen. Diese allgemeine Beschreibung des Setups enthält Dokumentations-Links für die spezifische verwendete Methode. Weitere Methoden finden Sie in den entsprechenden Links im "[Ressourcen](#)".

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

Installieren Sie einen OCP-Cluster auf GCP über die CLI.

- Stellen Sie sicher, dass Sie alle angegebenen Voraussetzungen erfüllt haben "[Hier](#)".
- Für die VPN-Verbindung zwischen On-Premises und GCP wurde eine pfsense VM erstellt und konfiguriert. Anweisungen hierzu finden Sie unter "[Hier](#)".
 - Die Remote-Gateway-Adresse in pfsense kann erst konfiguriert werden, nachdem Sie ein VPN-Gateway in der Google Cloud Platform erstellt haben.
 - Die Remote-Netzwerk-IP-Adressen für die Phase 2 können erst konfiguriert werden, nachdem das OpenShift-Cluster-Installationsprogramm ausgeführt und die Infrastrukturkomponenten für den Cluster erstellt hat.
 - Das VPN in Google Cloud kann erst konfiguriert werden, nachdem durch das Installationsprogramm die Infrastrukturkomponenten für den Cluster erstellt wurden.
- Jetzt den OpenShift-Cluster auf GCP installieren.
 - Rufen Sie das Installationsprogramm und das Pull-Geheimnis ab, und implementieren Sie den Cluster wie in der Dokumentation beschrieben "[Hier](#)".
 - Bei der Installation wird ein VPC-Netzwerk in der Google Cloud Platform erstellt. Außerdem wird eine private Zone in Cloud DNS erstellt und Datensätze hinzugefügt.
 - Verwenden Sie die CIDR-Blockadresse des VPC-Netzwerks, um pfsense zu konfigurieren und die VPN-Verbindung aufzubauen. Stellen Sie sicher, dass Firewalls korrekt eingerichtet sind.
 - Fügen Sie im DNS der lokalen Umgebung mithilfe der IP-Adresse in den A-Datensätzen des Google Cloud DNS Einen Eintrag hinzu.
 - Die Installation des Clusters ist abgeschlossen und stellt eine kubeconfig-Datei sowie einen Benutzernamen und ein Passwort für die Anmeldung bei der Konsole des Clusters bereit.

Implementieren Sie Cloud Volumes ONTAP in GCP mit BlueXP.

- Installieren Sie einen Connector in Google Cloud. Siehe Anweisungen "[Hier](#)".
- Stellen Sie über den Connector eine CVO-Instanz in Google Cloud bereit. Anweisungen finden Sie hier. <https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-gcp.html>

Astra Trident im OCP-Cluster in GCP installieren

- Wie in der Abbildung dargestellt, gibt es viele Methoden für die Implementierung von Astra Trident "[Hier](#)".
- Für dieses Projekt wurde Astra Trident mithilfe der Anweisungen manuell implementiert, indem der Astra Trident Operator installiert wurde "[Hier](#)".
- Back-End- und Storage-Klassen erstellen Siehe Anweisungen "[Hier](#)".

Fügen Sie den OCP-Cluster in GCP zum Astra Control Center hinzu.

- Erstellen Sie eine separate KubeConfig-Datei mit einer Cluster-Rolle, die die erforderlichen Mindestberechtigungen für das Management eines Clusters durch Astra Control enthält. Die Anweisungen sind zu finden ["Hier"](#).
- Fügen Sie das Cluster gemäß den Anweisungen zu Astra Control Center hinzu ["Hier"](#)

Verwendung der CSI-Topology-Funktion von Trident für Multi-Zone-Architekturen

Heute können Cloud-Provider Kubernetes/OpenShift-Cluster-Administratoren Nodes der zonbasierten Cluster erstellen. Die Nodes können sich in verschiedenen Verfügbarkeitszonen innerhalb einer Region oder über verschiedene Regionen hinweg befinden. Astra Trident verwendet CSI Topology, um die Provisionierung von Volumes für Workloads in einer Multi-Zone-Architektur zu vereinfachen. Mithilfe der CSI Topology-Funktion kann der Zugriff auf Volumes auf einen Teil von Nodes basierend auf Regionen und Verfügbarkeitszonen begrenzt werden. Siehe ["Hier"](#) Entnehmen.



Kubernetes unterstützt zwei Volume-Bindungsmodi: - Wenn **VolumeBindingMode auf Immediate** (Standard) eingestellt ist, erstellt Astra Trident das Volume ohne Topologieorientierung. Persistente Volumes werden erstellt, ohne dass sie von den Planungsanforderungen des anfragenden Pods abhängig sind. - Wenn **VolumeBindingMode auf WaitForFirstConsumer** gesetzt wird, wird die Erstellung und Bindung eines Persistent Volume für eine PVC verzögert, bis ein Pod, der die PVC verwendet, geplant und erstellt wird. Auf diese Weise werden Volumes erstellt, um Planungseinschränkungen zu erfüllen, die durch Topologieanforderungen durchgesetzt werden. Astra Trident Storage-Back-Ends können für die selektive Bereitstellung von Volumes basierend auf Verfügbarkeitszonen entwickelt werden (Topologieorientiertes Back-End). Bei StorageClasses, die ein solches Backend nutzen, wird ein Volume nur erstellt, wenn es von einer Applikation angefordert wird, die in einer unterstützten Region/Zone geplant ist. (Topologieorientierte StorageClass) ["Hier"](#) Entnehmen.

Demonstrationsvideo

[OpenShift Cluster-Installation auf der Google Cloud Platform](#)

[Importieren von OpenShift-Clustern in Astra Control Center](#)

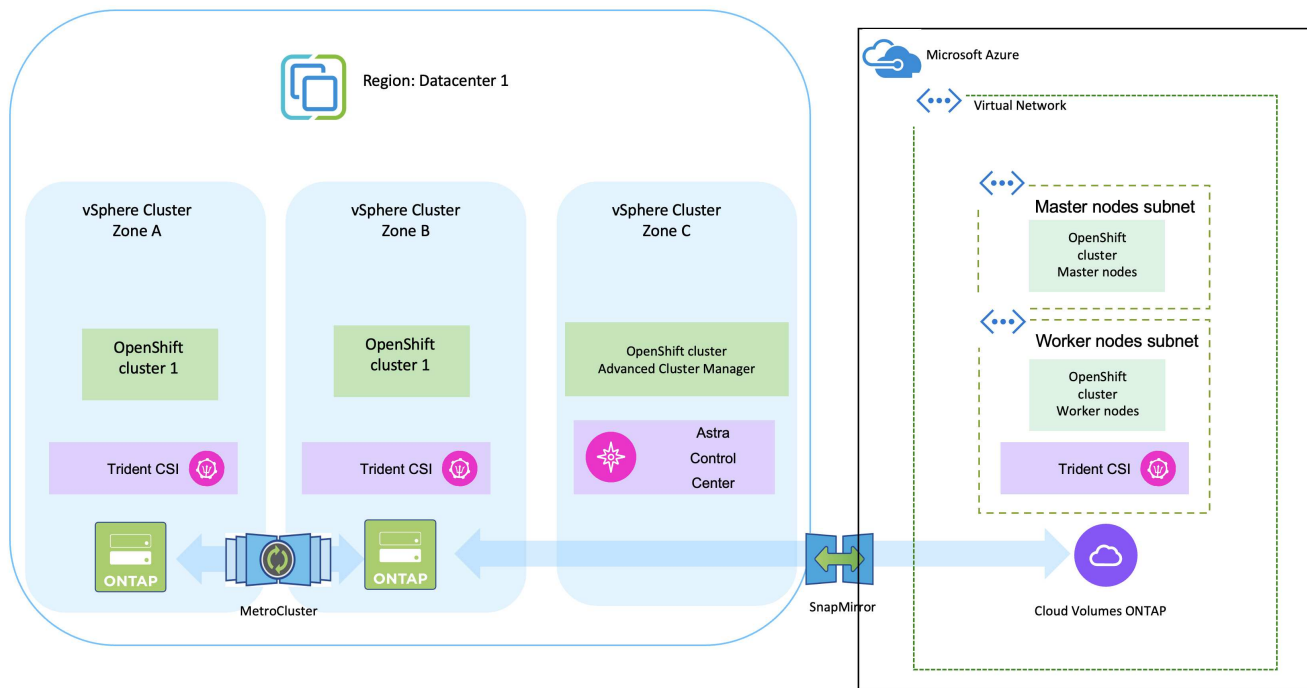
Implementierung und Konfiguration der Container-Plattform Red hat OpenShift auf Azure

Implementierung und Konfiguration der Container-Plattform Red hat OpenShift auf Azure

In diesem Abschnitt wird ein High-Level-Workflow beschrieben, in dem erläutert wird, wie OpenShift-Cluster in Azure eingerichtet und gemanagt und zustandsbehaftete Anwendungen darauf bereitgestellt werden. Er zeigt die Nutzung von NetApp Cloud Volumes ONTAP Storage mit Unterstützung von Astra Trident/Astra Control Provisioner für persistente Volumes. Einzelheiten zur Nutzung von Astra Control Center für die Durchführung von Datensicherungs- und Migrationsaktivitäten für die zustandsbehafteten Applikationen werden bereitgestellt.

Das folgende Diagramm zeigt die auf Azure implementierten Cluster, die über ein VPN mit dem Datacenter

verbunden sind.



Es gibt verschiedene Möglichkeiten zur Implementierung von Red hat OpenShift Container-Plattform-Clustern in Azure. Diese allgemeine Beschreibung des Setups enthält Dokumentations-Links für die spezifische verwendete Methode. Weitere Methoden finden Sie in den entsprechenden Links im "[Ressourcen](#)".

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

Installieren Sie einen OCP-Cluster in Azure über die CLI.

- Stellen Sie sicher, dass Sie alle angegebenen Voraussetzungen erfüllt haben ["Hier"](#).
- Erstellen Sie ein VPN, Subnetze und Netzwerksicherheitsgruppen sowie eine private DNS-Zone. Erstellen Sie ein VPN-Gateway und eine Site-to-Site-VPN-Verbindung.
- Für die VPN-Verbindung zwischen On-Premises und Azure wurde eine pfSense VM erstellt und konfiguriert. Anweisungen hierzu finden Sie unter ["Hier"](#).
- Rufen Sie das Installationsprogramm und das Pull-Geheimnis ab, und implementieren Sie den Cluster wie in der Dokumentation beschrieben ["Hier"](#).
- Die Installation des Clusters ist abgeschlossen und stellt eine kubeconfig-Datei sowie einen Benutzernamen und ein Passwort für die Anmeldung bei der Konsole des Clusters bereit.

Im Folgenden finden Sie eine Beispieldatei `install-config.yaml`.

```
apiVersion: v1
baseDomain: sddc.netapp.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 512
        diskType: "StandardSSD_LRS"
        type: Standard_D2s_v3
        ultraSSDCapability: Disabled
      #zones:
      #- "1"
      #- "2"
      #- "3"
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 1024
        diskType: Premium_LRS
        type: Standard_D8s_v3
        ultraSSDCapability: Disabled
  replicas: 3
```

```

metadata:
  creationTimestamp: null
  name: azure-cluster
networking:
  clusterNetwork:
    - cidr: 10.128.0.0/14
      hostPrefix: 23
  machineNetwork:
    - cidr: 10.0.0.0/16
  networkType: OVNKubernetes
  serviceNetwork:
    - 172.30.0.0/16
platform:
  azure:
    baseDomainResourceGroupName: ocp-base-domain-rg
    cloudName: AzurePublicCloud
    computeSubnet: ocp-subnet2
    controlPlaneSubnet: ocp-subnet1
    defaultMachinePlatform:
      osDisk:
        diskSizeGB: 1024
        diskType: "StandardSSD_LRS"
        ultraSSDCapability: Disabled
    networkResourceGroupName: ocp-nc-us-rg
    #outboundType: UserDefinedRouting
    region: northcentralus
    resourceGroupName: ocp-cluster-ncusrg
    virtualNetwork: ocp_vnet_ncus
publish: Internal
pullSecret:

```

Implementieren Sie Cloud Volumes ONTAP in Azure mit BlueXP.

- Installieren Sie einen Connector in Azure. Siehe Anweisungen ["Hier"](#).
- Stellen Sie über den Connector eine CVO-Instanz in Azure bereit. Anweisungen finden Sie unter dem Link: <https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-azure.html> [hier.]

Installation von Astra Control Provisioner im OCP Cluster in Azure

- Bei diesem Projekt wurde Astra Control Provisioner (ACP) auf allen Clustern installiert (On-Premises-Cluster, On-Premises-Cluster, in dem Astra Control Center implementiert ist, und der Cluster in Azure). Weitere Informationen zur Astra Control Provisionierung ["Hier"](#).
- Back-End- und Storage-Klassen erstellen Siehe Anweisungen ["Hier"](#).

Fügen Sie das OCP-Cluster in Azure dem Astra Control Center hinzu.

- Erstellen Sie eine separate KubeConfig-Datei mit einer Cluster-Rolle, die die erforderlichen Mindestberechtigungen für das Management eines Clusters durch Astra Control enthält. Die Anweisungen sind zu finden ["Hier"](#).
- Fügen Sie das Cluster gemäß den Anweisungen zu Astra Control Center hinzu ["Hier"](#)

Verwendung der CSI-Topology-Funktion von Trident für Multi-Zone-Architekturen

Heute können Cloud-Provider Kubernetes/OpenShift-Cluster-Administratoren Nodes der zonbasierten Cluster erstellen. Die Nodes können sich in verschiedenen Verfügbarkeitszonen innerhalb einer Region oder über verschiedene Regionen hinweg befinden. Astra Trident verwendet CSI Topology, um die Provisionierung von Volumes für Workloads in einer Multi-Zone-Architektur zu vereinfachen. Mithilfe der CSI Topology-Funktion kann der Zugriff auf Volumes auf einen Teil von Nodes basierend auf Regionen und Verfügbarkeitszonen begrenzt werden. Siehe ["Hier"](#) Entnehmen.



Kubernetes unterstützt zwei Volume-Bindungsmodi: - Wenn **VolumeBindingMode auf Immediate** (Standard) eingestellt ist, erstellt Astra Trident das Volume ohne Topologieorientierung. Persistente Volumes werden erstellt, ohne dass sie von den Planungsanforderungen des anfragenden Pods abhängig sind. - Wenn **VolumeBindingMode auf WaitForFirstConsumer** gesetzt wird, wird die Erstellung und Bindung eines Persistent Volume für eine PVC verzögert, bis ein Pod, der die PVC verwendet, geplant und erstellt wird. Auf diese Weise werden Volumes erstellt, um Planungseinschränkungen zu erfüllen, die durch Topologieanforderungen durchgesetzt werden. Astra Trident Storage-Back-Ends können für die selektive Bereitstellung von Volumes basierend auf Verfügbarkeitszonen entwickelt werden (Topologieorientiertes Back-End). Bei StorageClasses, die ein solches Backend nutzen, wird ein Volume nur erstellt, wenn es von einer Applikation angefordert wird, die in einer unterstützten Region/Zone geplant ist. (Topologieorientierte StorageClass) ["Hier"](#) Entnehmen.

Demonstrationsvideo

[Verwendung von Astra Control für Failover und Failback von Applikationen](#)

Datensicherung über Astra Control Center

Auf dieser Seite werden die Datenschutzoptionen für Container-basierte Red hat OpenShift-Anwendungen angezeigt, die auf VMware vSphere oder in der Cloud mit Astra Control Center (ACC) ausgeführt werden.

Wenn Benutzer ihre Anwendungen mit Red hat OpenShift modernisieren, sollte eine Datenschutzstrategie eingerichtet werden, um sie vor versehentlichem Löschen oder anderen menschlichen Fehlern zu schützen. Häufig ist auch eine Sicherungsstrategie für gesetzliche Vorschriften oder Compliance-Zwecke erforderlich, um ihre Daten vor einem Diaster zu schützen.

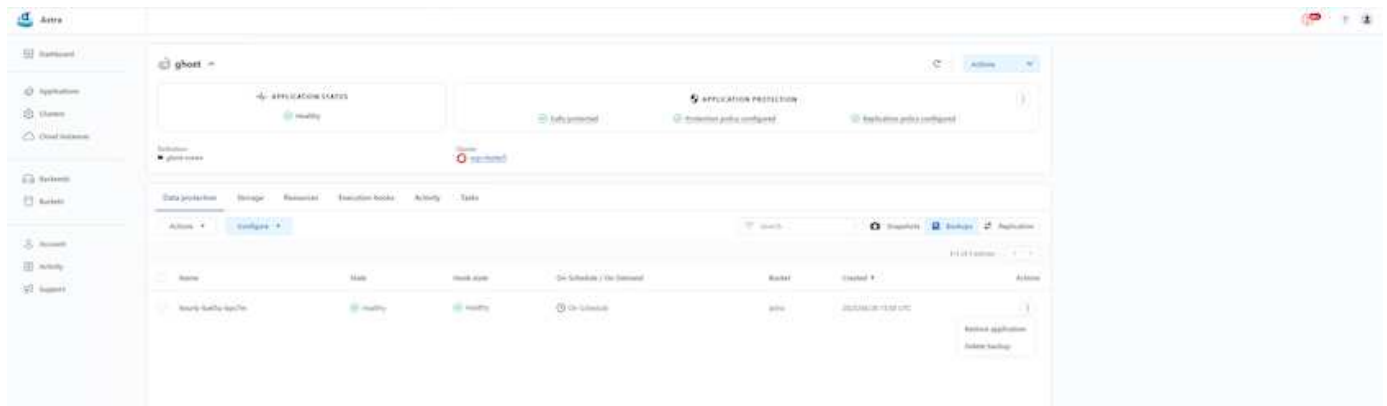
Die Anforderungen an die Datensicherung reichen von dem Zurücksetzen auf eine zeitpunktgenaue Kopie bis hin zum automatischen Failover auf eine andere Fehlerdomäne ohne menschliches Eingreifen. Viele Kunden entscheiden sich für ONTAP als bevorzugte Storage-Plattform für ihre Kubernetes-Applikationen, da sie umfassende Funktionen wie Mandantenfähigkeit, Multiprotokoll, hohe Performance und Kapazität, Replizierung und Caching für Standorte an mehreren Standorten sowie Sicherheit und Flexibilität bieten.

Möglicherweise haben Kunden als Erweiterung ihres Datacenters eine Cloud-Umgebung eingerichtet, um von den Vorteilen der Cloud zu profitieren und gut vorbereitet zu sein, um ihre Workloads zu einem späteren Zeitpunkt zu verschieben. Für solche Kunden ist das Sichern ihrer OpenShift-Anwendungen und ihrer Daten in der Cloud-Umgebung unausweichlich. Anschließend können sie die Anwendungen und die zugehörigen Daten entweder in einem OpenShift-Cluster in der Cloud oder in ihrem Rechenzentrum wiederherstellen.

Sichern und Wiederherstellen mit ACC

Anwendungseigentümer können die von ACC erkannten Anwendungen überprüfen und aktualisieren. ACC kann Snapshot Kopien mithilfe von CSI erstellen und Backups mithilfe der zeitpunktgenauen Snapshot Kopie durchführen. Das Backup-Ziel kann ein Objektspeicher in der Cloud-Umgebung sein. Die Schutzrichtlinie kann für geplante Backups und die Anzahl der zu bewahrenden Backup-Versionen konfiguriert werden. Der minimale RPO beträgt eine Stunde.

Wiederherstellen einer Anwendung aus einer Sicherung mit ACC



Anwendungsspezifische Ausführungshaken

Obwohl die Datensicherungsfunktionen auf Storage-Array-Ebene verfügbar sind, sind häufig zusätzliche Schritte erforderlich, um Backup- und Restore-Vorgänge applikationskonsistent zu gestalten. Die App-spezifischen zusätzlichen Schritte können sein: - Vor oder nach dem Erstellen einer Snapshot-Kopie. - Vor oder nach der Erstellung einer Sicherung. - Nach der Wiederherstellung aus einer Snapshot-Kopie oder Backup. Astra Control kann diese applikationsspezifischen Schritte ausführen, die als benutzerdefinierte Skripte, sogenannte Execution Hooks, codiert werden.

NetApp "[Open-Source-Projekt Verda](#)" Diese Lösung bietet Ausführungshaken für gängige Cloud-native Applikationen und ermöglicht so einen einfachen, robusten und einfach zu orchestrierten Schutz von Applikationen. Sie können sich gerne an diesem Projekt beteiligen, wenn Sie genügend Informationen für eine Anwendung haben, die sich nicht im Repository befindet.

Beispiel-Ausführungshaken für Pre-Snapshot einer redis-Anwendung.

Edit execution hook
✕

HOOK DETAILS ?

Operation

Pre-snapshot

▼

Hook arguments (optional)

1 pre ✕ ?

Enter hook arguments

Hook name

redis-pre-snapshot

CONTAINER IMAGES ?

☐ Apply to all container images

Use a regular expression to target container images for the hook.

Container image names to match

redis

SCRIPT ?

+ Add

Search

Name ↓

☐ mariadb_mysql.sh

☐ postgresql.sh

☒ redis_hook.sh

Cancel

Save ✓

EXECUTION HOOKS

Execution hooks allow Astra Control to execute your own custom scripts before or after a snapshot.

Read more in

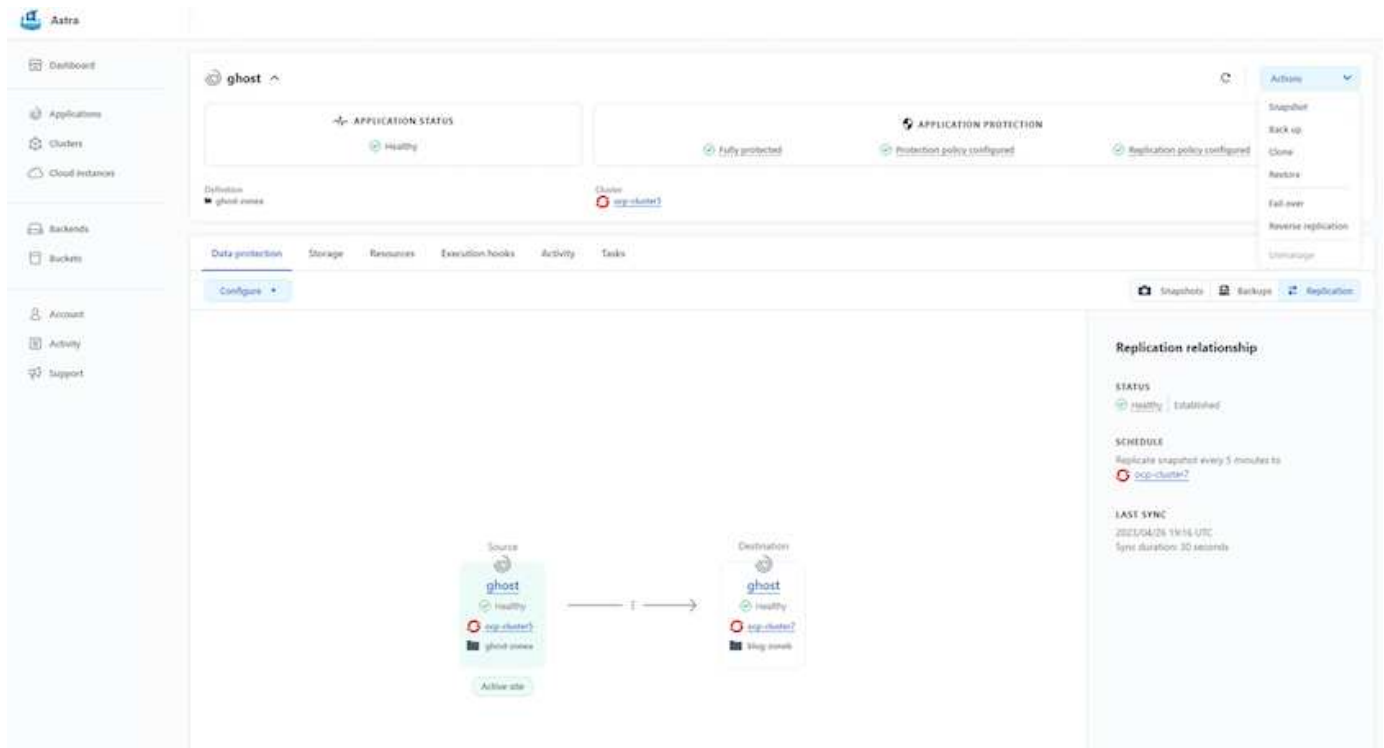
[Manage application execution hooks](#)

Replikation mit ACC

Für regionalen Schutz oder für eine Lösung mit niedriger RPO und RTO, kann eine Applikation auf eine andere Kubernetes-Instanz repliziert werden, die an einem anderen Standort, vorzugsweise in einer anderen Region, ausgeführt wird. ACC verwendet ONTAP Async SnapMirror mit einem Recovery Point Objective von nur 5 Minuten. Siehe ["Hier"](#) Anweisungen zur Einrichtung von SnapMirror finden Sie.

SnapMirror mit ACC

40



speichertreiber für san-Economy und nas-Economy unterstützen keine Replikationsfunktion. Siehe ["Hier"](#) Entnehmen.

Demovideo:

["Demo-Video über Disaster Recovery mit Astra Control Center"](#)

Datensicherung mit Astra Control Center

Einzelheiten zu den Datensicherungsfunktionen von Astra Control Center sind erhältlich ["Hier"](#)

Disaster Recovery (Failover und Failback mit Replikation) mit ACC

[Verwendung von Astra Control für Failover und Failback von Applikationen](#)

Datenmigration über Astra Control Center

Auf dieser Seite werden die Optionen für die Datenmigration von Container-Workloads auf Red hat OpenShift-Clustern mit Astra Control Center (ACC) angezeigt. Insbesondere können Kunden ACC nutzen, um: Einige ausgewählte Workloads oder alle Workloads aus ihren On-Premises-Datacentern in die Cloud zu verschieben – ihre Apps zu Testzwecken oder zum Verschieben aus dem Datacenter in die Cloud in die Cloud zu klonen

Datenmigration

Um eine Anwendung von einer Umgebung in eine andere zu migrieren, können Sie eine der folgenden Funktionen von ACC verwenden:

- **Replikation**

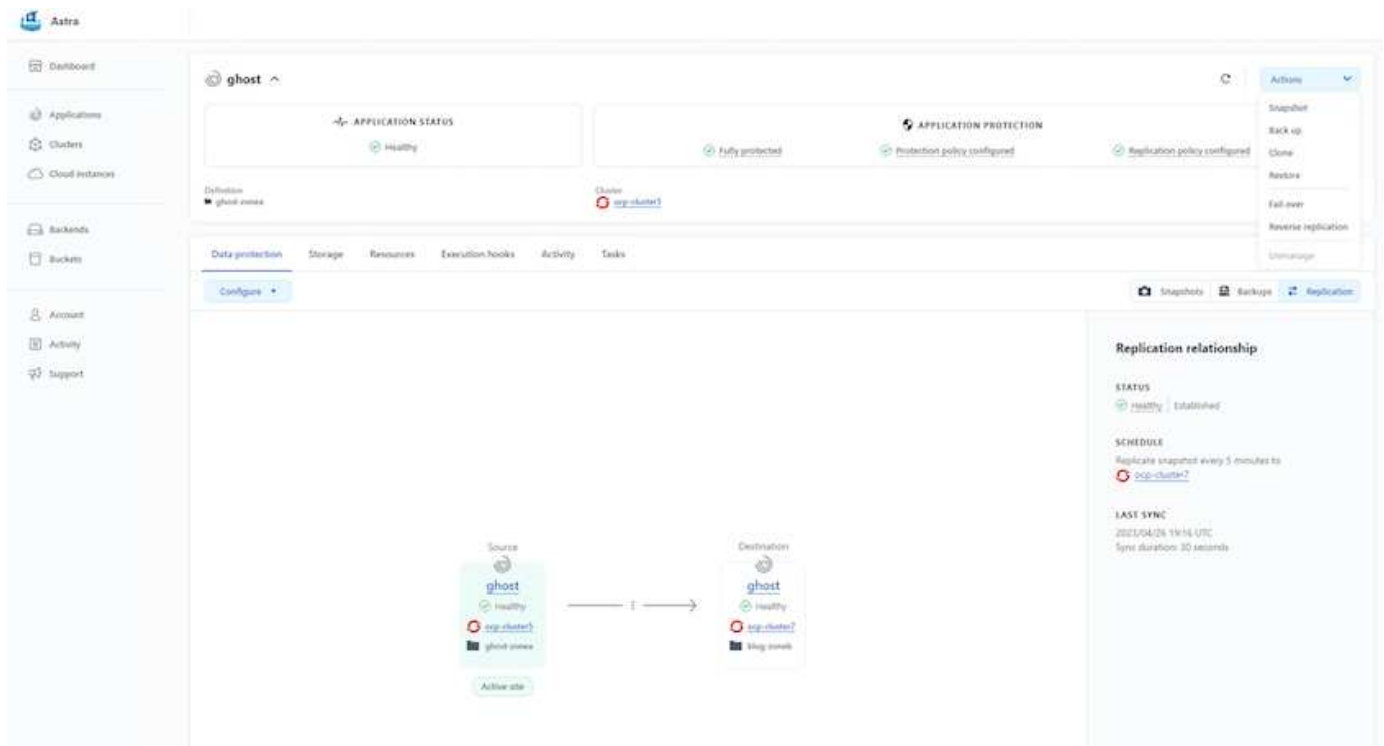
- **Sicherung und Wiederherstellung**
- **Klon**

Siehe "[Abschnitt zur Datensicherung](#)" Für die Optionen **Replikation und Backup und Restore**. Siehe "[Hier](#)" Für weitere Details über **Klonen**.



Die Astra Replizierungsfunktion wird nur mit der Trident Container Storage Interface (CSI) unterstützt. Die Replikation wird jedoch nicht von nas-Economy- und san-Economy-Treibern unterstützt.

Durchführen der Datenreplikation mit ACC



NetApp Hybrid-Multi-Cloud-Lösungen für Container-Workloads mit Red hat OpenShift

Überblick

Bei NetApp beobachten wir eine deutliche Zunahme bei Kunden, die ihre älteren Enterprise-Applikationen modernisieren und neue Applikationen mithilfe von Containern und Orchestrierungsplattformen auf Basis von Kubernetes erstellen. Die Red hat OpenShift Container Platform ist ein Beispiel, das wir von vielen unserer Kunden angenommen sehen.

Immer mehr Kunden beginnen mit der Einführung von Containern in ihrem Unternehmen. NetApp ist perfekt aufgestellt, um die persistenten Storage-Anforderungen ihrer zustandsbehafteten Applikationen und klassischen Datenmanagementanforderungen zu erfüllen, beispielsweise Datensicherung, Datensicherheit und Datenmigration. Diese Bedürfnisse werden jedoch mit verschiedenen Strategien, Werkzeugen und Methoden erfüllt.

NetApp ONTAP basierte Storage-Optionen, die unten aufgeführt sind, bieten Sicherheit, Datensicherung,

- Automatisierter, lokaler Storage:
 - NetApp Fabric Attached Storage (FAS), NetApp All-Flash-FAS-Arrays (AFF), NetApp All-SAN-Arrays (ASA) und ONTAP Select
- Von Providern gemanagter Storage in On-Premises:
 - NetApp Keystone stellt Storage-as-a-Service (STaaS) bereit
- Automatisierter Storage in der Cloud:
 - NetApp Cloud Volumes ONTAP (CVO) bieten Self-Managed-Storage in den Hyperscalern
- Von Providern gemanagter Storage in der Cloud:
 - Cloud Volumes Service für Google Cloud (CVS), Azure NetApp Files (ANF) und Amazon FSX für NetApp ONTAP bieten vollständig gemanagten Storage in den Hyperscalern

ONTAP feature highlights



Storage Administration <ul style="list-style-type: none">• Multi-tenancy• FlexVol & FlexGroup• LUN• Quotas• ONTAP CLI & API• System Manager & BlueXP	Performance & Scalability <ul style="list-style-type: none">• FlexCache• FlexClone• nconnect, session trunking, multipathing• Scale-out clusters
Availability & Resilience <ul style="list-style-type: none">• Multi-AZ HA deployment (MetroCluster)• SnapShot & SnapRestore• SnapMirror• SnapMirror Business Continuity• SnapMirror Cloud	Access Protocols <ul style="list-style-type: none">• NFS –v3, v4, v4.1, v4.2• SMB – v2, v3• iSCSI• Multi-protocol access
Storage Efficiency <ul style="list-style-type: none">• Deduplication & Compression• Compaction• Thin provisioning• Data Tiering (Fabric Pool)	Security & Compliance <ul style="list-style-type: none">• Fpolicy & Vscan• Active Directory integration• LDAP & Kerberos• Certificate based authentication

NetApp BlueXP ermöglicht Ihnen das Management Ihrer gesamten Storage- und Datenbestände über eine einzige Managementoberfläche.

Mit BlueXP können Sie Cloud-Storage erstellen und verwalten (z. B. Cloud Volumes ONTAP und Azure NetApp Files), Daten verschieben, schützen und analysieren sowie zahlreiche lokale und Edge-Storage-Geräte kontrollieren.

NetApp Astra Trident ist ein CSI-konformer Storage Orchestrator, der eine schnelle und einfache Nutzung von persistentem Storage ermöglicht und von einer Vielzahl der oben genannten NetApp Storage-Optionen unterstützt wird. Es handelt sich um eine Open-Source-Software, die von NetApp gewartet und unterstützt wird.

Astra Trident CSI feature highlights



CSI specific <ul style="list-style-type: none"> • CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies • CSI topology • Volume expansion 	Security <ul style="list-style-type: none"> • Dynamic-export policy management • iSCSI initiator-groups dynamic management • iSCSI bidirectional CHAP
Control <ul style="list-style-type: none"> • Storage and performance consumption • Monitoring • Volume Import • Cross Namespace Volume Access 	Installation methods <ul style="list-style-type: none"> • Binary • Helm chart • Operator • GitOps
Choose your access mode <ul style="list-style-type: none"> • RWO (ReadWriteOnce, i.e 1↔1) • RWX (ReadWriteMany, i.e 1↔n) • ROX (ReadOnlyMany) • RWOP (ReadWriteOnce POD) 	Choose your protocol <ul style="list-style-type: none"> • NFS • SMB • iSCSI

Geschäftskritische Container-Workloads benötigen mehr als nur persistente Volumes. Ihre Datenmanagement-Anforderungen erfordern auch den Schutz und die Migration der Kubernetes-Objekte für die Applikation.



Neben Benutzerdaten umfassen Applikationsdaten kubernetes-Objekte. Folgende Beispiele sind vorhanden: - kubernetes-Objekte wie Pods-Spezifikationen, PVCs, Implementierungen, Services – benutzerdefinierte Konfigurationsobjekte wie Konfigurationszuordnungen und -Geheimnisse – persistente Daten wie Snapshot-Kopien, Backups, Klone – benutzerdefinierte Ressourcen wie CRS und CRDs

NetApp Astra Control ist sowohl als vollständig gemanagte als auch als selbst gemanagte Software erhältlich und bietet Orchestrierung für solides Applikations-Datenmanagement. Siehe "[Astra-Dokumentation](#)" Weitere Informationen zur Astra Produktfamilie.

Diese Referenzdokumentation unterstützt die Validierung der Migration und des Schutzes von Container-basierten Applikationen, die auf der RedHat OpenShift Container-Plattform über das NetApp Astra Control Center implementiert werden. Darüber hinaus bietet die Lösung allgemeine Details zur Bereitstellung und zur Verwendung von Red hat Advanced Cluster Management (ACM) für die Verwaltung der Container-Plattformen. In diesem Dokument werden auch Einzelheiten zur Integration von NetApp Storage in Container-Plattformen mit Red hat OpenShift mithilfe der Astra Trident CSI-bereitstellung erläutert. Astra Control Center wird auf dem Hub-Cluster bereitgestellt und wird für das Management der Container-Applikationen und ihres Lebenszyklus von persistentem Storage verwendet. Schließlich bietet es eine Lösung für Replizierung, Failover und Failback für Container-Workloads auf gemanagten Red hat OpenShift-Clustern in AWS (ROSA), die Amazon FSX für NetApp ONTAP (FSxN) als persistenten Storage verwenden.

Die NetApp Lösung mit gemanagten Container-Plattform-Workloads aus Red hat OpenShift auf AWS

Die NetApp Lösung mit gemanagten Container-Plattform-Workloads aus Red hat OpenShift auf AWS

Möglicherweise sind Kunden „aus der Cloud hervorgegangen“ oder bereits an einem Punkt der Modernisierung angelangt, wenn sie bereit sind, einige ausgewählte Workloads

oder alle Workloads aus ihrem Datacenter in die Cloud zu verschieben. Sie können dafür wählen, von Providern gemanagte OpenShift-Container und von Providern gemanagten NetApp Storage in der Cloud zu verwenden, um ihre Workloads auszuführen. Sie sollten die verwalteten Container-Cluster (ROSA) von Red hat OpenShift in der Cloud planen und bereitstellen, um eine erfolgreiche produktionsbereite Umgebung für ihre Container-Workloads zu schaffen. In der AWS-Cloud können sie auch FSX für NetApp ONTAP für die Storage-Anforderungen implementieren.

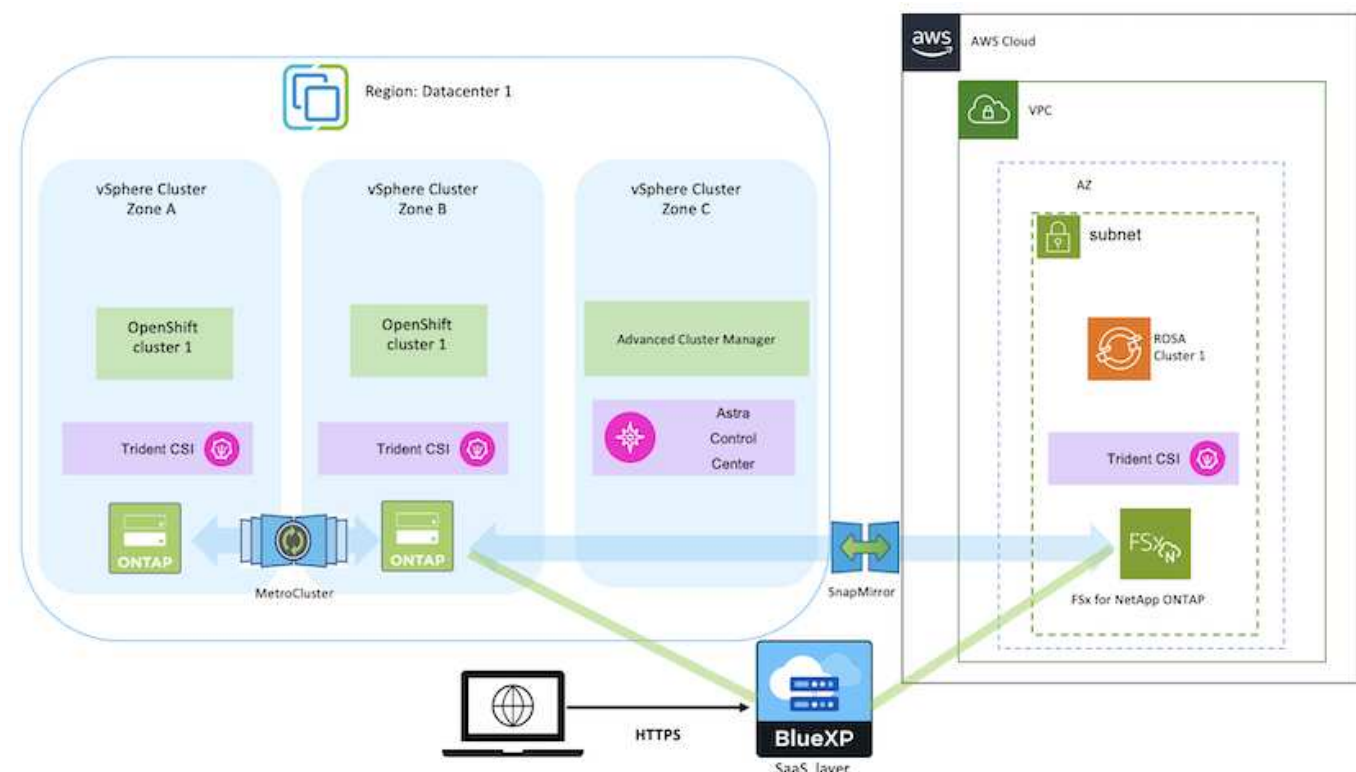
FSX for NetApp ONTAP bietet Datensicherung, Zuverlässigkeit und Flexibilität für Container-Implementierungen in AWS. Astra Trident dient als dynamische Storage-bereitstellung zur Nutzung des persistenten FSxN Storage für zustandsbehaftete Applikationen von Kunden.

DA ROSA im HA-Modus mit Knoten der Kontrollebene über mehrere Verfügbarkeitszonen hinweg implementiert werden kann, kann FSX ONTAP auch mit Multi-AZ-Option bereitgestellt werden, die hohe Verfügbarkeit bietet und AZ-Ausfälle schützt.



Beim Zugriff auf ein Amazon FSX Filesystem aus der bevorzugten Verfügbarkeitszone (AZ) des Filesystems fallen keine Datenübertragungsgebühren an. Weitere Informationen zur Preisgestaltung finden Sie unter ["Hier"](#).

Datensicherungs- und Migrationslösung für OpenShift-Container-Workloads

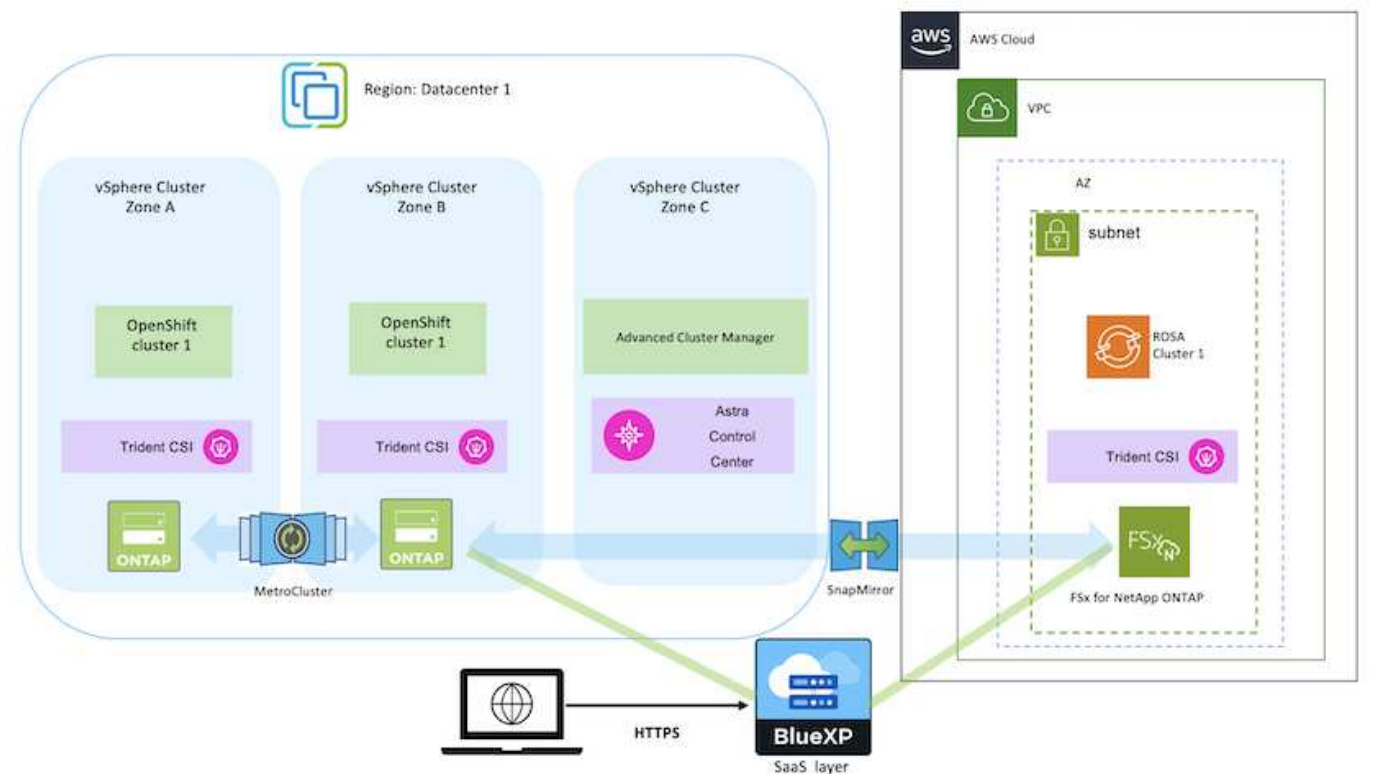


Implementierung und Konfiguration der gemanagten Container-Plattform Red hat OpenShift auf AWS

In diesem Abschnitt wird ein High-Level-Workflow zur Einrichtung der verwalteten Red hat OpenShift-Cluster auf AWS(ROSA) beschrieben. Es zeigt die Nutzung von Managed FSX for NetApp ONTAP (FSxN) als Storage-Backend von Astra Trident zur Bereitstellung

persistenter Volumes. Es werden Details zur Implementierung von FSxN auf AWS mithilfe von BlueXP bereitgestellt. Außerdem werden Einzelheiten zur Verwendung von BlueXP und OpenShift GitOps (Argo CD) bereitgestellt, um Datensicherungs- und Migrationsaktivitäten für die zustandsbehafteten Applikationen auf ROSA Clustern durchzuführen.

Das folgende Diagramm zeigt die AUF AWS implementierten ROSA-Cluster, die FSxN als Back-End-Storage verwenden.



Diese Lösung wurde mit zwei ROSA-Clustern in zwei VPCs in AWS verifiziert. Jeder ROSA Cluster wurde mithilfe von Astra Trident in FSxN integriert. ES gibt mehrere Möglichkeiten, ROSA-Cluster und FSxN in AWS bereitzustellen. Diese allgemeine Beschreibung des Setups enthält Dokumentations-Links für die spezifische verwendete Methode. Weitere Methoden finden Sie in den entsprechenden Links im ["Ressourcen"](#).

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

INSTALLIEREN SIE ROSA Cluster

- Erstellung von zwei VPCs und Einrichtung der VPC-Peering-Konnektivität zwischen den VPCs.
- Siehe ["Hier"](#) Für Anweisungen zur Installation VON ROSA Clustern.

Installieren Sie FSxN

- Installieren Sie FSxN auf den VPCs von BlueXP. Siehe "[Hier](#)" Für die Erstellung von BlueXP Konten und weitere Schritte. Siehe "[Hier](#)" Zur Installation von FSxN. Siehe "[Hier](#)" Zum Erstellen eines Connectors in AWS zum Verwalten des FSxN.
- Implementieren Sie FSxN mithilfe von AWS. Siehe "[Hier](#)" Für die Implementierung über die AWS-Konsole.

Trident auf ROSA Clustern installieren (mit Helm-Diagramm)

- Verwenden Sie Helm-Diagramm, um Trident auf ROSA Clustern zu installieren. url für das Helm-Diagramm: <https://netapp.github.io/trident-helm-chart>

Integration von FSxN mit Astra Trident für ROSA Cluster



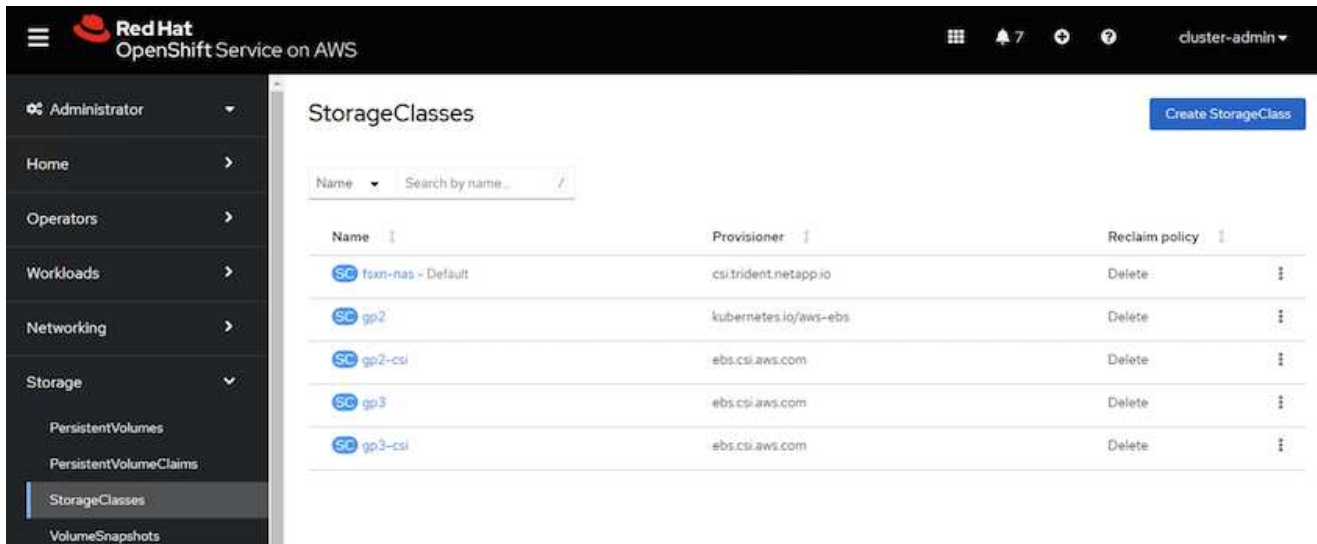
OpenShift GitOps kann zur Implementierung von Astra Trident CSI für alle gemanagten Cluster verwendet werden, wenn sie über ApplicationSet auf ArgoCD registriert werden.

```
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: trident-operator
spec:
  generators:
  - clusters: {}
    # selector:
    #   matchLabels:
    #     tridentversion: '23.04.0'
  template:
    metadata:
      name: '{{nameNormalized}}-trident'
    spec:
      destination:
        namespace: trident
        server: '{{server}}'
      source:
        repoURL: 'https://netapp.github.io/trident-helm-chart'
        targetRevision: 23.04.0
        chart: trident-operator
        project: default
        syncPolicy:
          syncOptions:
            - CreateNamespace=true
```



Back-End- und Storage-Klassen mit Trident (für FSxN) erstellen

- Siehe "[Hier](#)" Für Details zum Erstellen von Back-End und Storage-Klasse.
- Erstellen Sie die für FSxN erstellte Storage-Klasse mit Trident CSI standardmäßig aus der OpenShift-Konsole. Siehe Abbildung unten:



Anwendung mit OpenShift GitOps (Argo CD) bereitstellen

- Installieren Sie den OpenShift GitOps Operator auf dem Cluster. Siehe Anweisungen "[Hier](#)".
- Richten Sie eine neue Argo-CD-Instanz für den Cluster ein. Siehe Anweisungen "[Hier](#)".

Öffnen Sie die Konsole von Argo CD und stellen Sie eine App bereit. Als Beispiel können Sie eine Jenkins-App mithilfe einer Argo-CD mit einem Helm-Diagramm bereitstellen. Beim Erstellen der Anwendung wurden folgende Details angegeben: Projekt: Standardcluster:

<https://kubernetes.default.svc> Namensraum: Jenkins die url für das Helm-Diagramm:
<https://charts.bitnami.com/bitnami>

Helm-Parameter: Global.storageClass: FsxN-nas

Datensicherung

Auf dieser Seite werden die Datensicherungsoptionen für gemanagte Red hat OpenShift auf AWS (ROSA) Clustern unter Verwendung des Astra Control Service angezeigt. Astra Control Service (ACS) bietet eine intuitive grafische Benutzeroberfläche, mit der Sie Cluster hinzufügen, darauf laufende Applikationen definieren und applikationsorientierte Datenmanagement-Aktivitäten durchführen können. ACS-Funktionen können auch über eine API aufgerufen werden, die die Automatisierung von Workflows ermöglicht.

Astra Control (ACS oder ACC) wird von NetApp Astra Trident angetrieben. Astra Trident integriert mehrere Arten von Kubernetes Clustern wie Red hat OpenShift, EKS, AKS, SUSE Rancher, Anthos usw. mit verschiedenen Ausführungen von NetApp ONTAP-Storage wie FAS/All Flash FAS, ONTAP Select, CVO, Google Cloud Volumes Service, Azure NetApp Files und Amazon FSX for NetApp ONTAP.

Dieser Abschnitt enthält Details zu den folgenden Datenschutzoptionen, die ACS verwenden:

- Ein Video, das Backup und Restore einer ROSA-Anwendung zeigt, die in einer Region ausgeführt wird und in einer anderen Region wiederhergestellt wird.
- Ein Video, das Snapshot und Wiederherstellung einer ROSA-Anwendung zeigt.
- Schritt-für-Schritt-Details zur Installation eines ROSA-Clusters, Amazon FSX for NetApp ONTAP, Verwendung von NetApp Astra Trident zur Integration mit Storage-Backend, Installation einer postgresql-Anwendung auf ROSA-Cluster, Verwendung von ACS zur Erstellung eines Snapshot der Anwendung und Wiederherstellung der Anwendung von ihm.
- Ein Blog, der Schritt-für-Schritt-Details des Erstellens und Wiederherstellens aus einem Snapshot für eine mysql-Anwendung auf einem ROSA-Cluster mit FSX für ONTAP unter Verwendung von ACS zeigt.

Backup/Wiederherstellung aus Backup

Das folgende Video zeigt die Sicherung einer ROSA-Anwendung, die in einer Region ausgeführt wird und in einer anderen Region wiederhergestellt wird.

[FSX NetApp ONTAP für Red hat OpenShift Service auf AWS](#)

Snapshot/Wiederherstellung aus Snapshot

Das folgende Video zeigt, wie Sie einen Snapshot einer ROSA-Anwendung erstellen und danach aus dem Snapshot wiederherstellen.

[Snapshot/Wiederherstellung für Anwendungen auf Red hat OpenShift-Service auf AWS \(ROSA\)-Clustern mit Amazon FSX für NetApp ONTAP-Speicher](#)

Blog

- ["Nutzung von Astra Control Service zum Datenmanagement von Applikationen auf ROSA Clustern mit Amazon FSX Storage"](#)

Schritt-für-Schritt-Details zum Erstellen von Snapshot und Wiederherstellen von ihm

Vorbereitende Einrichtung

- ["AWS Konto"](#)
- ["Red hat OpenShift -Konto"](#)
- IAM-Benutzer mit ["Entsprechende Berechtigungen"](#) Um ROSA Cluster zu erstellen und darauf zuzugreifen
- ["AWS CLI"](#)
- ["ROSA CLI"](#)
- ["OpenShift-CLI"\(oc\)](#)
- VPC mit Subnetzen und entsprechenden Gateways und Routen
- ["ROSA Cluster installiert"](#) In die VPC
- ["Amazon FSX für NetApp ONTAP"](#) Erstellt in derselben VPC
- Zugriff auf den ROSA-Cluster von ["OpenShift Hybrid Cloud Console"](#)

Nächste Schritte

1. Erstellen Sie einen Admin-Benutzer und melden Sie sich beim Cluster an.
2. Erstellen Sie eine kubeconfig-Datei für den Cluster.
3. Installieren Sie Astra Trident auf dem Cluster.
4. Mit der CSI-provisionierung von Trident können Sie eine Back-End-, Storage-Klasse- und Snapshot-Klassenkonfiguration erstellen.
5. Implementieren Sie eine postgresql-Anwendung auf dem Cluster.
6. Erstellen Sie eine Datenbank und fügen Sie einen Datensatz hinzu.
7. Fügen Sie den Cluster zu ACS hinzu.
8. Definieren Sie die Anwendung in ACS.
9. Erstellen Sie einen Snapshot mit ACS.
10. Löschen Sie die Datenbank in der postgresql-Anwendung.
11. Wiederherstellen von einem Snapshot mit ACS.
12. Überprüfen Sie, ob Ihre App aus dem Snapshot wiederhergestellt wurde.

1. Erstellen Sie einen Admin-Benutzer und melden Sie sich beim Cluster an

Greifen Sie auf den ROSA-Cluster zu, indem Sie einen Admin-Benutzer mit dem folgenden Befehl erstellen: (Sie müssen einen Admin-Benutzer nur erstellen, wenn Sie zum Zeitpunkt der Installation keinen Administrator erstellt haben)

```
rosa create admin --cluster=<cluster-name>
```

Der Befehl liefert eine Ausgabe, die wie folgt aussieht. Melden Sie sich mit dem beim Cluster an `oc login` In der Ausgabe bereitgestellter Befehl.

```
W: It is recommended to add an identity provider to login to this cluster.
See 'rosa create idp --help' for more information.
I: Admin account has been added to cluster 'my-rosa-cluster'. It may take up
to a minute for the account to become active.
I: To login, run the following command:
oc login https://api.my-rosa-cluster.abcd.p1.openshiftapps.com:6443 \
--username cluster-admin \
--password FWGYL-2mkJI-00000-00000
```



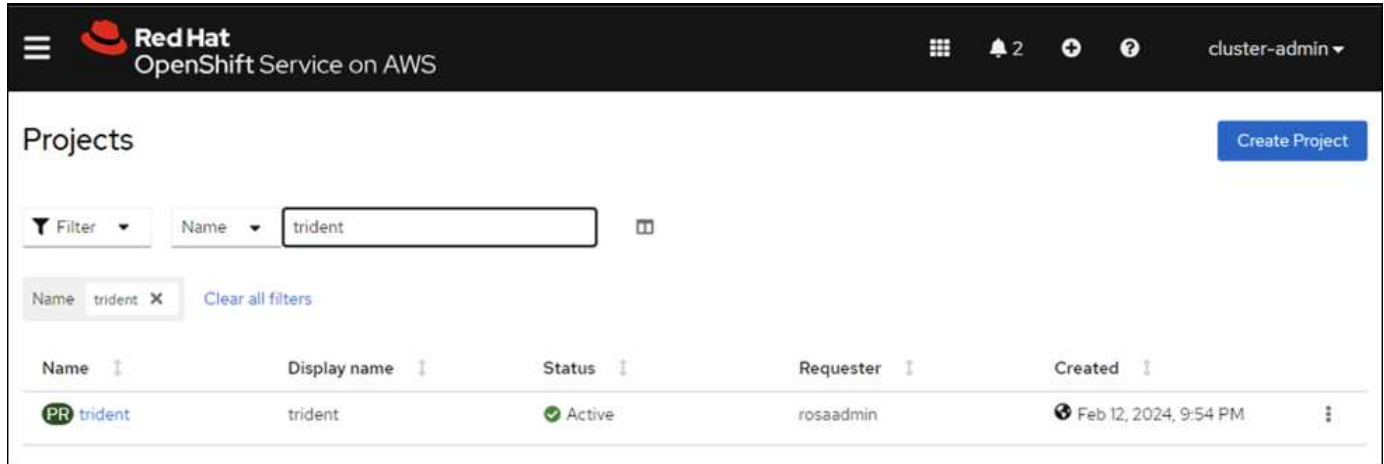
Sie können sich auch mit einem Token beim Cluster anmelden. Wenn Sie zum Zeitpunkt der Cluster-Erstellung bereits einen Admin-Benutzer erstellt haben, können Sie sich über die Red hat OpenShift Hybrid Cloud-Konsole mit den Anmeldedaten des Admin-Benutzers beim Cluster anmelden. Klicken Sie dann auf die obere rechte Ecke, wo der Name des angemeldeten Benutzers angezeigt wird, um den zu erhalten `oc login` Befehl (Token Login) für die Befehlszeile.

2. Erstellen Sie eine kubeconfig-Datei für den Cluster

Befolgen Sie die Anweisungen ["Hier"](#) Um eine Kubeconfig-Datei für den ROSA-Cluster zu erstellen. Diese kubeconfig-Datei wird später verwendet, wenn Sie den Cluster zu ACS hinzufügen.

3. Installieren Sie Astra Trident auf dem Cluster

Installieren Sie Astra Trident (neueste Version) im ROSA Cluster. Um dies zu tun, können Sie eine der angegebenen Verfahren befolgen ["Hier"](#). Um Trident über das Helm von der Cluster-Konsole zu installieren, erstellen Sie zuerst ein Projekt mit dem Namen Trident.



Erstellen Sie dann in der Entwickleransicht ein Helmdiagramm-Repository. Verwenden Sie für das URL-Feld `'https://netapp.github.io/trident-helm-chart'`. Erstellen Sie dann ein Helm Release für den Trident Operator.

Create Helm Chart Repository

Add helm chart repository.

Configure via: ☒ Form view ☐ YAML view

Scope type

☐ Namespaced scoped (ProjectHelmChartRepository)

Add Helm Chart Repository in the selected namespace.

☒ Cluster scoped (HelmChartRepository)

Add Helm Chart Repository at the cluster level and in all namespaces.

Name *

trident

A unique name for the Helm Chart repository.

Display name

Astra Trident

A display name for the Helm Chart repository.

Description

NetApp Astra Trident

A description for the Helm Chart repository.

☐ Disable usage of the repo in the developer catalog.

URL *

https://netapp.github.io/trident-helm-chart

Project: trident ▼

[Developer Catalog](#) > [Helm Charts](#)

Helm Charts

Browse for charts that help manage complex installations and upgrades. Cluster administrators can customize the catalog. Alternatively, developers can [try to configure their own custom Helm Chart repository](#).

All items

CI/CD

Languages

Other

Chart Repositories

☒ Astra Trident (1)

☐ OpenShift Helm Charts (87)

Source

☐ Community (33)


☐ Partner (42)

☐ Red Hat (12)

All items

Q Filter by keyword...

A-Z ▼

**Helm Charts**

Trident Operator

A Helm chart for deploying NetApp's Trident CSI storage provisioner using the Trident...

Überprüfen Sie, ob alle Stativpods ausgeführt werden, indem Sie zur Administratoransicht auf der Konsole zurückkehren und Pods im Dreizack-Projekt auswählen.

Red Hat
 OpenShift Service on AWS

Administrator

Home

Operators

Workloads

Pods

Deployments

DeploymentConfigs

StatefulSets

Secrets

ConfigMaps

CronJobs

Jobs

DaemonSets

ReplicaSets

ReplicationControllers

HorizontalPodAutoscalers

PodDisruptionBudgets

Networking

Project: trident

Pods

Filter Name Search by name...

Name	Status	Ready	Restarts	Owner	Mem
trident-controller-69cff44ddf-4dqnj	Running	6/6	0	trident-controller-69cff44ddf	-
trident-node-linux-4b6fm	Running	2/2	0	trident-node-linux	-
trident-node-linux-4sckw	Running	2/2	0	trident-node-linux	-
trident-node-linux-7142w	Running	2/2	0	trident-node-linux	-
trident-node-linux-dbhp4	Running	2/2	0	trident-node-linux	-
trident-node-linux-gj5km	Running	2/2	0	trident-node-linux	-
trident-node-linux-r79c8	Running	2/2	0	trident-node-linux	-
trident-node-linux-tzwdp	Running	2/2	0	trident-node-linux	-
trident-node-linux-vdvxt	Running	2/2	0	trident-node-linux	-
trident-operator-7f7fd45c68-6crqb	Running	1/1	0	trident-operator-7f7fd45c68	-

4. Erstellen Sie mit der Trident CSI-provisionierung eine Back-End-, Storage-Klasse- und Snapshot-Klassenkonfiguration

Verwenden Sie die unten abgebildeten yaml-Dateien, um ein dreigespanntes Backend-Objekt, ein Storage-Klasse-Objekt und das Volumesnapshot-Objekt zu erstellen. Stellen Sie sicher, dass Sie die Anmeldeinformationen für Ihr von Ihnen erstelltes Amazon FSX for NetApp ONTAP-Dateisystem, die Verwaltungs-LIF und den vserver-Namen Ihres Dateisystems in der Konfiguration yaml für das Backend angeben. Um diese Details anzuzeigen, wählen Sie in der AWS-Konsole für Amazon FSX das Dateisystem aus, und wechseln Sie zur Registerkarte Administration. Klicken Sie außerdem auf Aktualisieren, um das Kennwort für das festzulegen `fsxadmin` Benutzer:



Sie können die Objekte über die Befehlszeile erstellen oder mit den yaml-Dateien von der Hybrid Cloud-Konsole aus erstellen.

FSx > File systems > fs-049f9a23aac951429

fsx-for-rosa (fs-049f9a23aac951429)

▼ Summary

File system ID fs-049f9a23aac951429	SSD storage capacity 1024 GiB	Update	Availability Zones us-west-2b
Lifecycle state Available	Throughput capacity 128 MB/s	Update	Creation time 2024-02-12T20:15:23-05:00
File system type ONTAP	Provisioned IOPS 3072	Update	
Deployment type Single-AZ	Number of HA pairs 1		

Network & security | Monitoring & performance | **Administration** | Storage virtual machines | Volumes | Backups | Updates | Tags

ONTAP administration

Management endpoint - DNS name management.fs-049f9a23aac951429.fsx.us-west-2.amazonaws.com	Management endpoint - IP address 10.49.9.135	ONTAP administrator username fsxadmin
Inter-cluster endpoint - DNS name intercluster.fs-049f9a23aac951429.fsx.us-west-2.amazonaws.com	Inter-cluster endpoint - IP address 10.49.9.49	ONTAP administrator password Update
	10.49.9.251	

Trident Back-End-Konfiguration

```

apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-nas-secret
type: Opaque
stringData:
  username: fsxadmin
  password: <password>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: <management lif>
  backendName: ontap-nas
  svm: fsx
  credentials:
    name: backend-tbc-ontap-nas-secret

```

Storage-Klasse

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
allowVolumeExpansion: true

```

Snapshot-Klasse

```

apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Delete

```

Stellen Sie sicher, dass die Objekte von Backend, Storage-Klasse und Trident-snapshotclass mit den unten gezeigten Befehlen erstellt werden.

```

[ec2-user@ip-10-49-11-132 storage]$ kubectl get tbc -n trident
NAME          BACKEND NAME      BACKEND UUID          PHASE    STATUS
ontap-nas     ontap-nas         8a5e4583-2dac-46bb-b01e-fa7c3816f121  Bound    Success
[ec2-user@ip-10-49-11-132 storage]$ kubectl get sc
NAME          PROVISIONER          RECLAIMPOLICY    VOLUMEBINDINGMODE    ALLOWVOLUMEEXPANSION    AGE
gp2           kubernetes.io/aws-ebs Delete            WaitForFirstConsumer  true                    3h23m
gp2-csi       ebs.csi.aws.com      Delete            WaitForFirstConsumer  true                    3h19m
gp3 (default) ebs.csi.aws.com      Delete            WaitForFirstConsumer  true                    3h23m
gp3-csi       ebs.csi.aws.com      Delete            WaitForFirstConsumer  true                    3h19m
ontap-nas     csi.trident.netapp.io Delete            Immediate             true                    141m
[ec2-user@ip-10-49-11-132 storage]$ kubectl get Volumesnapshotclass
NAME          DRIVER          DELETIONPOLICY    AGE
csi-aws-vsc   ebs.csi.aws.com Delete            3h19m
trident-snapshotclass csi.trident.netapp.io Delete            6m56s
[ec2-user@ip-10-49-11-132 storage]$

```

Zu diesem Zeitpunkt ist eine wichtige Änderung erforderlich, ontap-nas statt gp3 als Standard-Storage-Klasse einzustellen, damit die später zu implementierende postgresql-Applikation die Standard-Storage-Klasse verwenden kann. Wählen Sie in der OpenShift-Konsole Ihres Clusters unter Storage StorageClasses aus. Bearbeiten Sie die Annotation der aktuellen Standardklasse mit „false“ und fügen Sie die Annotation storageclass.kubernetes.io/is-default-class für die ontap-nas Storage-Klasse auf „true“ ein.

The screenshot shows the Red Hat OpenShift StorageClasses management interface. A modal titled "Edit annotations" is open, allowing the user to edit the annotations for a selected StorageClass. The modal contains two input fields: "Key" and "Value". The "Key" field is pre-filled with "storageclass.kubernetes.io/is-...", and the "Value" field contains "false". There is an "Add more" link below the input fields and "Cancel" and "Save" buttons at the bottom right of the modal. In the background, the StorageClasses list is visible, showing columns for Name, Provisioner, and Reclaim policy. The list includes StorageClasses like gp2, gp2-csi, gp3 - Default, gp3-csi, and ontap-nas.

StorageClasses

Create StorageClass

Name Search by name...

Name	Provisioner	Reclaim policy
SC gp2	kubernetes.io/aws-ebs	Delete
SC gp2-csi	ebs.csi.aws.com	Delete
SC gp3	ebs.csi.aws.com	Delete
SC gp3-csi	ebs.csi.aws.com	Delete
SC ontap-nas - Default	csi.trident.netapp.io	Delete

5. Implementieren Sie eine postgresql-Anwendung auf dem Cluster

Sie können die Anwendung über die Befehlszeile wie folgt bereitstellen:

```
helm install postgresql bitnami/postgresql -n postgresql --create-namespace
```

```
[ec2-user@ip-10-49-11-132 astra]$ helm install postgresql bitnami/postgresql -n postgresql --create-namespace
NAME: postgresql
LAST DEPLOYED: Tue Feb 13 14:46:16 2024
NAMESPACE: postgresql
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
BASIC CHART NAME: postgresql
BASIC CHART VERSION: 14.0.4
BASIC APP VERSION: 16.2.0

** Please be patient while the chart is being deployed **

PostgreSQL can be accessed via port 5432 on the following DNS names from within your cluster:

    postgresql.postgresql.svc.cluster.local - Read/Write connection

To get the password for "postgres" run:

    export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="{.data.postgres-password}" | base64 -d)

To connect to your database run the following command:

    kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" \
    --command -- psql --host postgresql -U postgres -d postgres -p 5432

    > NOTE: If you access the container using bash, make sure that you execute "/opt/bitnami/scripts/postgresql/entrypoint.sh /bin/bash" in order to avoid
    the error "psql: local user with ID 1001} does not exist"

To connect to your database from outside the cluster execute the following commands:

    kubectl port-forward --namespace postgresql svc/postgresql 5432:5432 &
    PGPASSWORD=$POSTGRES_PASSWORD psql --host 127.0.0.1 -U postgres -d postgres -p 5432

WARNING: The configured password will be ignored on new installation in case when previous PostgreSQL release was deleted through the helm command. In that
case, old PVC will have an old password, and setting it through helm won't take effect. Deleting persistent volumes (PVs) will solve the issue.
[ec2-user@ip-10-49-11-132 astra]$
```

Wenn die Anwendungspads nicht ausgeführt werden, kann es aufgrund von Einschränkungen im Sicherheitskontext zu einem Fehler kommen.

```
[ec2-user@ip-10-49-11-132 astra]$ kubectl get all -n postgresql
NAME                                TYPE          CLUSTER-IP    EXTERNAL-IP    PORT(S)    AGE
service/postgresql                  ClusterIP      172.30.245.50  <none>          5432/TCP    12m
service/postgresql-hl               ClusterIP      None           <none>          5432/TCP    12m

NAME                                READY    AGE
statefulset.apps/postgresql          0/1      12m
[ec2-user@ip-10-49-11-132 astra]$ kubectl get events -n postgresql
LAST SEEN   TYPE      REASON              OBJECT                                          MESSAGE
2m39s       Normal    WaitForFirstConsumer persistentvolumeclaim/data-postgresql-0        waiting for first consumer to be created before binding
12m         Normal    SuccessfulCreate     statefulset/postgresql                        create Claim data-postgresql-0 Pod postgresql-0 in StatefulSet postgresql success
107s        Warning   FailedCreate         statefulset/postgresql                        create Pod postgresql-0 in StatefulSet postgresql failed error: pods
"postgresql-0" is forbidden: unable to validate against any security context constraint: [provider "trident-controller": Forbidden: not usable by user or
serviceaccount, provider "anyuid": Forbidden: not usable by user or serviceaccount, provider restricted-v2: .spec.securityContext.fsGroup: Invalid value: [
1001010000], provider "restricted": Forbidden: not usable by user or serviceaccount, provider "nonroot-v2": Forbidden: not usable by user or serviceaccount, pr
ovider "nonroot": Forbidden: not usable by user or serviceaccount, provider "pcap-dedicated-admins": Forbidden: not usable by user or serviceaccount, pr
ovider "hostmount-anyuid": Forbidden: not usable by user or serviceaccount, provider "machine-api-termination-handler": Forbidden: not usable by user or servi
ceaccount, provider "hostnetwork-v2": Forbidden: not usable by user or serviceaccount, provider "hostnetwork": Forbidden: not usable by user or serviceacco
unt, provider "hostaccess": Forbidden: not usable by user or serviceaccount, provider "splunkforwarder": Forbidden: not usable by user or serviceaccount, p
rovider "trident-node-linux": Forbidden: not usable by user or serviceaccount, provider "node-exporter": Forbidden: not usable by user or serviceaccount, p
rovider "privileged": Forbidden: not usable by user or serviceaccount]
[ec2-user@ip-10-49-11-132 astra]$
```

Beheben Sie den Fehler, indem Sie den bearbeiten runAsUser Und fsGroup Felder in statefulset.apps/postgresql Objekt mit der UID, die sich in der Ausgabe des befindet oc get project Wie unten gezeigt.

```
[ec2-user@ip-10-49-11-132 astra]$ oc get project postgresql -o yaml | grep uid-range
openshift.io/sa.scc.uid-range: 1001010000/10000
[ec2-user@ip-10-49-11-132 astra]$ oc edit -n postgresql statefulset.apps/postgresql
statefulset.apps/postgresql edited
[ec2-user@ip-10-49-11-132 astra]$
```

die postgresql-App sollte ausgeführt werden und persistente Volumes verwenden, die von Amazon FSX für NetApp ONTAP-Storage unterstützt werden.

```
[ec2-user@ip-10-49-11-132 astra]$ oc get pods -n postgresql
```

NAME	READY	STATUS	RESTARTS	AGE
postgresql-0	1/1	Running	0	2m46s

```
[ec2-user@ip-10-49-11-132 astra]$
```

```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get pvc -n postgresql
```

NAME	STATUS	VOLUME	CAPACITY	ACCESS MODES	STORAGECLASS	AGE
data-postgresql-0	Bound	pvc-dd09524a-de75-4825-9424-03a9b91195ca	8Gi	RWO	ontap-nas	4m2s

```
[ec2-user@ip-10-49-11-132 storage]$
```

6. Erstellen Sie eine Datenbank und fügen Sie einen Datensatz hinzu

```
[ec2-user@ip-10-49-11-132 astra]$ export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="{.data.postgres-password}" | base64 -d)
[ec2-user@ip-10-49-11-132 astra]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" \
> --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must set securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "postgresql-client" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "postgresql-client" must set securityContext.seccompProfile.type to "RuntimeDefault" or "Localhost")
If you don't see a command prompt, try pressing enter.
```

```
postgres=# CREATE DATABASE erp;
CREATE DATABASE
postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# CREATE TABLE PERSONS(ID INT PRIMARY KEY NOT NULL, FIRSTNAME TEXT NOT NULL, LASTNAME TEXT NOT NULL);
CREATE TABLE
erp=# INSERT INTO PERSONS VALUES(1,'John','Doe');
INSERT 0 1
erp=# \dt
          List of relations
Schema | Name   | Type  | Owner
-----+-----+-----+-----
public | persons | table | postgres
(1 row)
```

```
erp=# SELECT * FROM persons;
 id | firstname | lastname
----+-----+-----
  1 | John     | Doe
(1 row)
```

7. Fügen Sie den Cluster zu ACS hinzu

Melden Sie sich bei ACS an. Wählen Sie Cluster aus, und klicken Sie auf Hinzufügen. Wählen Sie andere aus, und laden Sie die Datei kubeconfig hoch oder fügen Sie sie ein.

Add cluster

STEP 1/3: DETAILS

PROVIDER

Microsoft Azure

Google Cloud Platform

Amazon Web Services

Other

KUBECONFIG

Please ensure that the kubeconfig used for this cluster has a long-lived token associated with it.

Provide Astra Control access to your Kubernetes clusters by entering a kubeconfig credential. Follow these [instructions](#) on how to create a dedicated admin-role kubeconfig.

Upload file

Paste or type

```
XJu2XR1cy5phy9z2XJ2aWN1YWNjb3VudC9z2XJ2aWN1LWFjY291bnQubmFtZSI6ImFzdHJhY29udHJvbmC1z2XJ2aWN1LWFjY291bnQ1LCJrdWJ1cm5ldGVzLmlvL3N1cnZpY2VhY2NvdW50L3N1cnZpY2UtYWNjb3VudC51aWQ1O1I4NzFhOTI4MC0wMTEyLTZmYzAtOWFkNS0zZDI5NzA2N2NiN01iLCJzdWIiOiJzeXN0ZW06c2VydmljZWVjY291bnQ6ZGVmYXVedDphc3RyYWNvbnRyb2wtc2VydmljZS1hY2NvdW50In0.M7-IRxcaKOe7S-LkW-8ZDYOShQ5UolaSbJ-0SIdSrOEbvfcQ3tSf40VC72nM4BqYbN8cm0y0V8IpF3OG7tYA9XAIdwX98xAXJ00T2UOG2xbyLWfOqLCFDk3_us9uqU63t8LLmeenCBiOm9PaD3XWHF2ZcTXXpdKqtzWfmbLxYhuN1CzBMY7S55MvNB2WD_eikptN02alvaWmIZjrUQL0_q8Uj2Exe9vVH1KPkb0CxU4TvHncbathvL6mZ1N7Om
```

Cancel

Next →

Klicken Sie auf **Weiter** und wählen Sie **ontap-nas** als Standard-Storage-Klasse für ACS aus. Klicken Sie auf **Weiter**, überprüfen Sie die Details und **Hinzufügen** den Cluster.

Add cluster

STEP 2/3: STORAGE

STORAGE

☒
Assign a new default storage class

The following storage classes are available on the cluster.

Set default	Storage class	Storage provisioner	Reclaim policy	Binding mode	Eligibility
<input type="radio"/>	gp2	kubernetes.io/aws-ebs	Delete	waitForFirstConsumer	Ineligible
<input type="radio"/>	gp2-csi	ebs.csi.aws.com	Delete	WaitForFirstConsumer	Eligible
<input type="radio"/>	gp3	ebs.csi.aws.com	Delete	WaitForFirstConsumer	Eligible
<input type="radio"/>	gp3-csi	ebs.csi.aws.com	Delete	WaitForFirstConsumer	Eligible
<input checked="" type="radio"/>	ontap-nas <small>Default</small>	csi.trident.netapp.io	Delete	Immediate	Eligible


← Back

Next →


8. Definieren Sie die Anwendung in ACS

Definieren Sie die postgresql-Anwendung in ACS. Wählen Sie auf der Landing Page **Applications**, **define** aus und geben Sie die entsprechenden Details ein. Klicken Sie ein paar Mal auf **Weiter**, überprüfen Sie die Details


und klicken Sie auf **Definieren**. Die Anwendung wird zu ACS hinzugefügt.

 **Add cluster**






STEP 2/3: STORAGE





STORAGE

 Assign a new default storage class

The following storage classes are available on the cluster.

Set default	Storage class	Storage provisioner	Reclaim policy	Binding mode	Eligibility
<input type="radio"/>	gp2	kubernetes.io/aws-ebs	Delete	WaitForFirstConsumer	 Ineligible
<input type="radio"/>	gp2-csi	ebs.csi.aws.com	Delete	WaitForFirstConsumer	 Eligible
<input type="radio"/>	gp3	ebs.csi.aws.com	Delete	WaitForFirstConsumer	 Eligible
<input type="radio"/>	gp3-csi	ebs.csi.aws.com	Delete	WaitForFirstConsumer	 Eligible
<input checked="" type="radio"/>	ontap-nas <small>Default</small>	csi.trident.netapp.io	Delete	Immediate	 Eligible


 Back


Next 


9. Erstellen Sie einen Snapshot mit ACS


Es gibt viele Möglichkeiten, einen Snapshot in ACS zu erstellen. Sie können die Anwendung auswählen und einen Snapshot auf der Seite erstellen, auf der die Details der Anwendung angezeigt werden. Sie können auf Snapshot erstellen klicken, um einen On-Demand-Snapshot zu erstellen oder eine Schutzrichtlinie zu konfigurieren.


Erstellen Sie einen On-Demand-Snapshot, indem Sie einfach auf **Create Snapshot** klicken, einen Namen angeben, die Details überprüfen und auf **Snapshot** klicken. Nach Abschluss des Vorgangs ändert sich der Snapshot-Status in „funktionstüchtiger Zustand“.


 Dashboard


 Applications


 Clusters

 Cloud instances

 Buckets

 Account

 Activity

 Support

Data protection

Storage


Resources


Execution hooks


Activity


Tasks


Actions ▾




 Configure protection policy


 Search

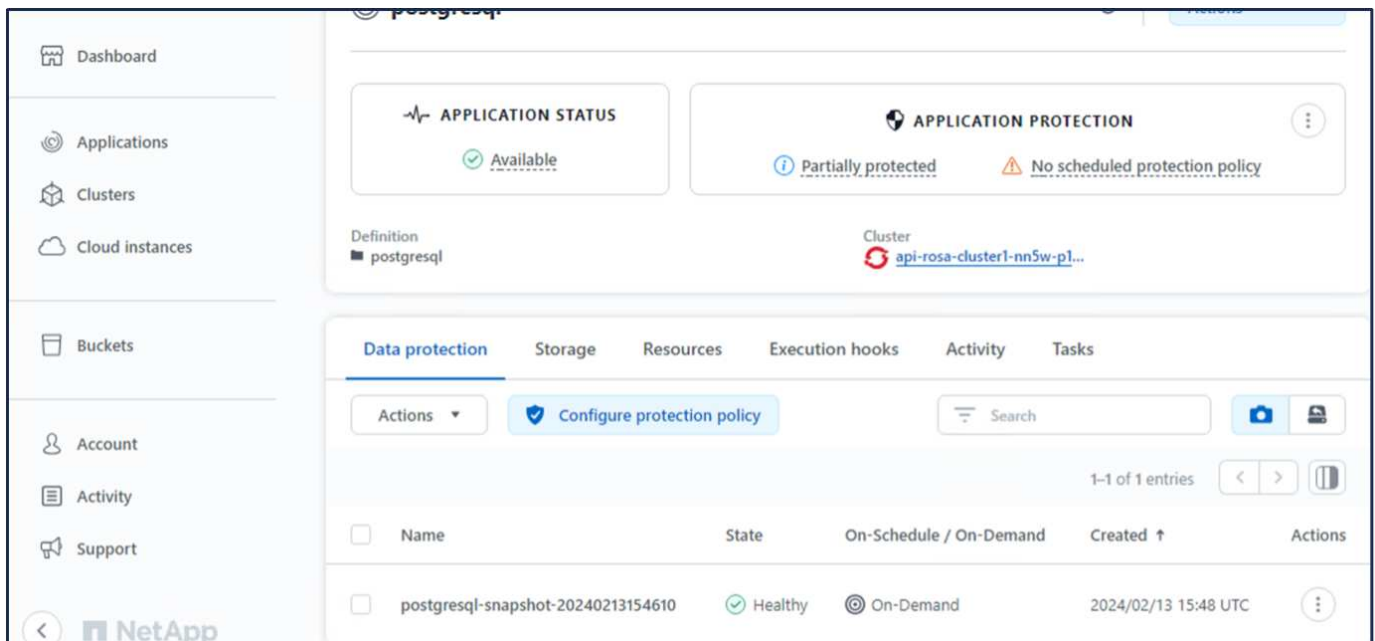
 Snapshots





0-0 of 0 entries   

<input type="checkbox"/>	Name	State	On-Schedule / On-Demand	Created ↑	Actions
<div><p>You don't have any snapshots</p><p>After you have created a snapshot, it will be listed here</p><div>Create snapshot</div></div>					



10. Löschen Sie die Datenbank in der postgresql-Anwendung

Melden Sie sich wieder bei postgresql an, Listen Sie die verfügbaren Datenbanken auf, löschen Sie die zuvor erstellte Datenbank und führen Sie sie erneut auf, um sicherzustellen, dass die Datenbank gelöscht wurde.

```
postgres=# \l
      List of databases
  Name | Owner | Encoding | Locale Provider | Collate | Ctype | ICU Locale | ICU Rules | Access privileges
-----+-----+-----+-----+-----+-----+-----+-----+-----
erp    | postgres | UTF8 | libc | en_US.UTF-8 | en_US.UTF-8 | | | =c/postgres
postgres | postgres | UTF8 | libc | en_US.UTF-8 | en_US.UTF-8 | | | =c/postgres
template0 | postgres | UTF8 | libc | en_US.UTF-8 | en_US.UTF-8 | | | =c/postgres
template1 | postgres | UTF8 | libc | en_US.UTF-8 | en_US.UTF-8 | | | =c/postgres
(4 rows)

postgres=# DROP DATABASE erp;
DROP DATABASE
postgres=# \l
      List of databases
  Name | Owner | Encoding | Locale Provider | Collate | Ctype | ICU Locale | ICU Rules | Access privileges
-----+-----+-----+-----+-----+-----+-----+-----+-----
postgres | postgres | UTF8 | libc | en_US.UTF-8 | en_US.UTF-8 | | | =c/postgres
template0 | postgres | UTF8 | libc | en_US.UTF-8 | en_US.UTF-8 | | | =c/postgres
template1 | postgres | UTF8 | libc | en_US.UTF-8 | en_US.UTF-8 | | | =c/postgres
(3 rows)
```

11. Wiederherstellen von einem Snapshot mit ACS

Um die Anwendung von einem Snapshot wiederherzustellen, gehen Sie zur ACS-UI-Landing Page, wählen Sie

die Anwendung aus und wählen Sie Wiederherstellen. Sie müssen einen Snapshot oder ein Backup auswählen, von dem aus wiederhergestellt werden soll. (In der Regel würden auf Basis einer von Ihnen konfigurierten Richtlinie mehrere erstellt werden.) Treffen Sie in den nächsten Bildschirmanzeigen die richtige Auswahl und klicken Sie dann auf **Wiederherstellen**. Der Anwendungsstatus wechselt von Wiederherstellen zu verfügbar, nachdem er aus dem Snapshot wiederhergestellt wurde.

Dashboard

Applications

Clusters

Cloud instances

Buckets

Account

Activity

Support

postgresql ^

APPLICATION STATUS

Available

APPLICATION PROTECTION

Partially protected

No scheduled protect

Definition

postgresql

Cluster

api-rosa-cluster1-nn5w-p1-op...

Actions

Snapshot

Back up

Clone

Restore

Unmanage

Data protection

Storage

Resources

Execution hooks

Activity

Tasks

Actions

Configure protection policy

Search

1-1 of 1 entries

<input type="checkbox"/>	Name	State	On-Schedule / On-Demand	Created ↑	Actions
<input type="checkbox"/>	postgresql-snapshot-20240213164912	Healthy	On-Demand	2024/02/13 16:50 UTC	

RESTORE TYPE

Restore the application to new namespaces on any available cluster or to original namespaces on the original cluster.

☐ Restore to new namespaces

☒ Restore to original namespaces

RESTORE SOURCE

Select a snapshot or backup to restore the application to a previous state.

Time range

Filter

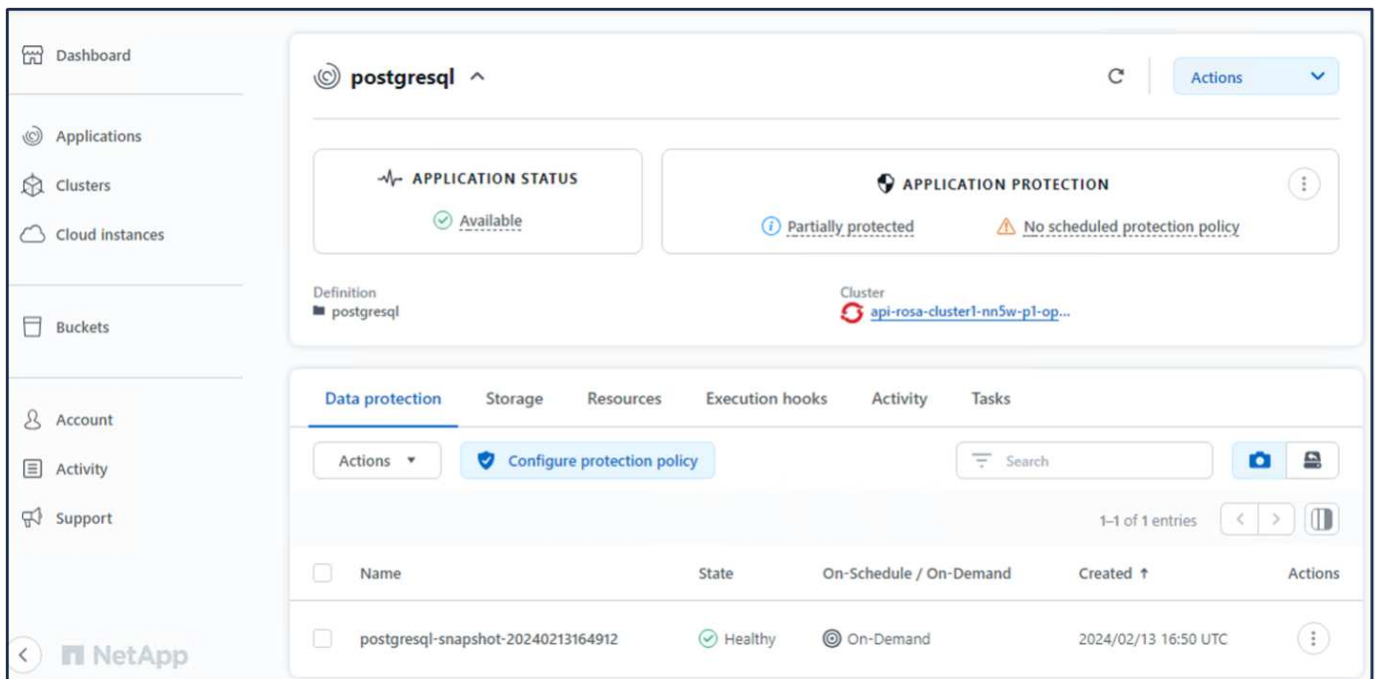
Snapshots

Backups

Application snapshot	Snapshot state	On-Schedule / On-Demand	Created ↑
<input checked="" type="radio"/> postgresql-snapshot-20240213164912	Healthy	On-Demand	2024/02/13 16:50 UTC

Cancel

Next →



12. Überprüfen Sie, ob Ihre App aus der Momentaufnahme wiederhergestellt wurde

Melden Sie sich beim postgresql-Client an und Sie sollten nun die Tabelle und den Datensatz in der Tabelle sehen, die Sie zuvor hatten. Das ist alles. Durch Klicken auf eine Schaltfläche wurde Ihre Anwendung in einen früheren Zustand zurückgesetzt. So einfach machen wir es unseren Kunden mit Astra Control.

```
[ec2-user@ip-10-49-11-132 ~]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:vl.24": allowPrivilegeEscalation != false (container "postgresql-client" must set securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "postgresql-client" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "postgresql-client" must set securityContext.seccompProfile.type to "RuntimeDefault" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgresql=# \l
      List of databases
  Name | Owner  | Encoding | Locale Provider | Collate | Ctype  | ICU Locale | ICU Rules | Access privileges
-----+-----+-----+-----+-----+-----+-----+-----+-----
erp    | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |              |           | =c/postgres +
postgres | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |              |           | postgres=CTc/postgres
template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |              |           | =c/postgres +
template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |              |           | postgres=CTc/postgres
(4 rows)

postgresql=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# \dt
      List of relations
 Schema | Name  | Type  | Owner
-----+-----+-----+-----
 public | persons | table | postgres
(1 row)

erp=# SELECT * from PERSONS;
 id | firstname | lastname
----+-----+-----
  1 | John      | Doe
(1 row)
```

Datenmigration

Auf dieser Seite werden die Datenmigrationsoptionen für Container-Workloads auf verwalteten Red hat OpenShift-Clustern unter Verwendung von FSX for NetApp ONTAP für persistenten Storage angezeigt.

Datenmigration

Red hat OpenShift-Service auf AWS sowie FSx for NetApp ONTAP (FSxN) sind Teil ihres Service-Portfolios von AWS. FSxN ist mit Single AZ- oder Multi-AZ-Optionen verfügbar. Die Multi-AZ-Option bietet Datenschutz bei Ausfall einer Verfügbarkeitszone. FSxN kann in Astra Trident integriert werden, um persistenten Storage für Applikationen auf ROSA Clustern bereitzustellen.

Integration von FSxN mit Trident mit Helm Chart

ROSA Cluster Integration mit Amazon FSX for ONTAP

Die Migration von Container-Applikationen umfasst Folgendes:

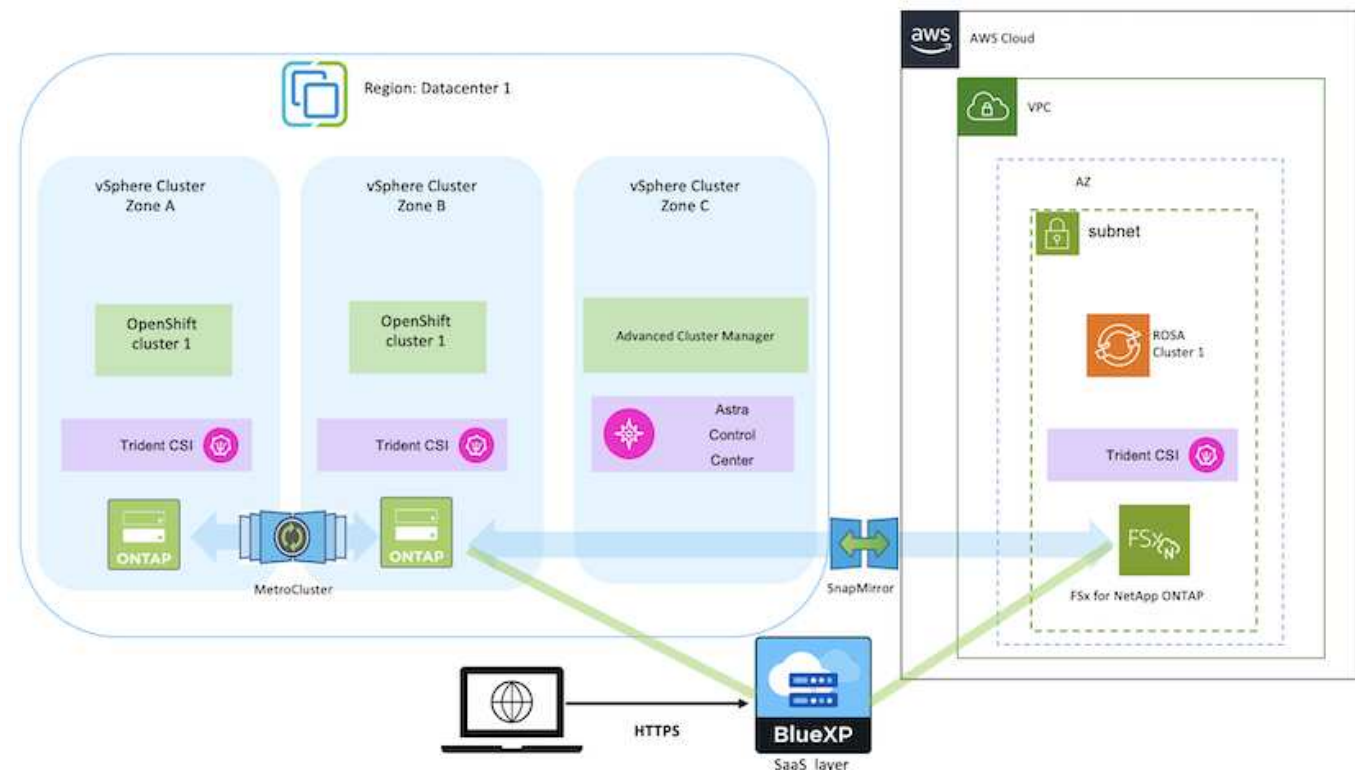
- Persistente Volumes: Dies ist mit BlueXP möglich. Eine weitere Option ist der Einsatz von Astra Control Center für die Migration von Container-Applikationen von On-Premises- in die Cloud-Umgebung. Automatisierung kann für den gleichen Zweck eingesetzt werden.
- Applikations-Metadaten: Dies kann mithilfe von OpenShift GitOps (Argo CD) erreicht werden.

Failover und Failback von Anwendungen auf ROSA-Cluster mit FSxN für persistenten Speicher

Das folgende Video zeigt eine Demonstration von Failover- und Failback-Szenarien mit BlueXP und der Argo CD.

Failover und Failback von Anwendungen auf ROSA Cluster

Datensicherungs- und Migrationslösung für OpenShift-Container-Workloads



Copyright-Informationen

Copyright © 2024 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 IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

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

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

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

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

Markeninformationen

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