Hybrid Cloud mit selbst gemanagten Komponenten (lokal/AWS/GCP/Azure)

NetApp Solutions

NetApp
April 26, 2024

Inhalt

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-als-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

- Multi-tenancy
- FlexVol & FlexGroup
- LUN
- Quotas
- ONTAP CLI & API
- System Manager & BlueXP

Performance & Scalability

- FlexCache
- FlexClone
- nconnect, session trunking, multipathing
- Scale-out clusters

Availability & Resilience

- Multi-AZ HA deployment (MetroCluster)
- SnapShot & SnapRestore
- SnapMirror
- SnapMirror Business Continuity
- SnapMirror Cloud

Access Protocols

- NFS –v3, v4, v4.1, v4.2
- SMB – v2, v3
- iSCSI
- Multi-protocol access

Storage Efficiency

- Deduplication & Compression
- Compaction
- Thin provisioning
- Data Tiering (Fabric Pool)

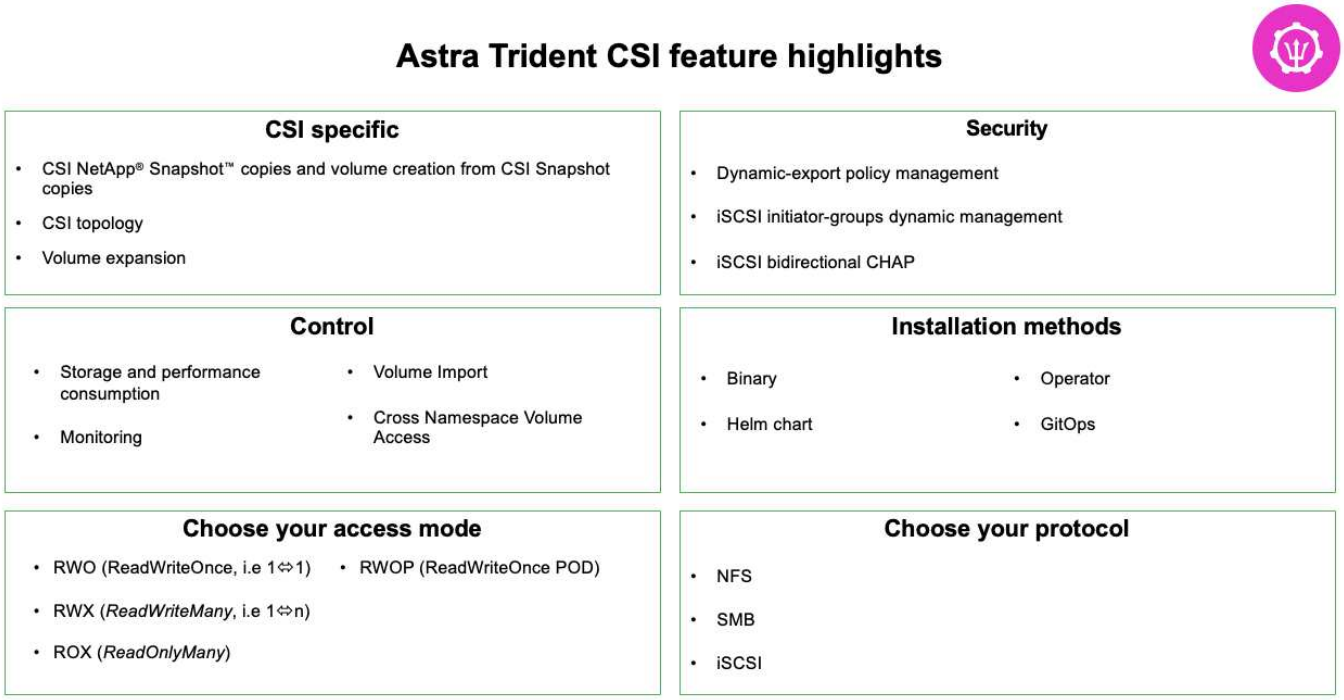
Security & Compliance

- 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.



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

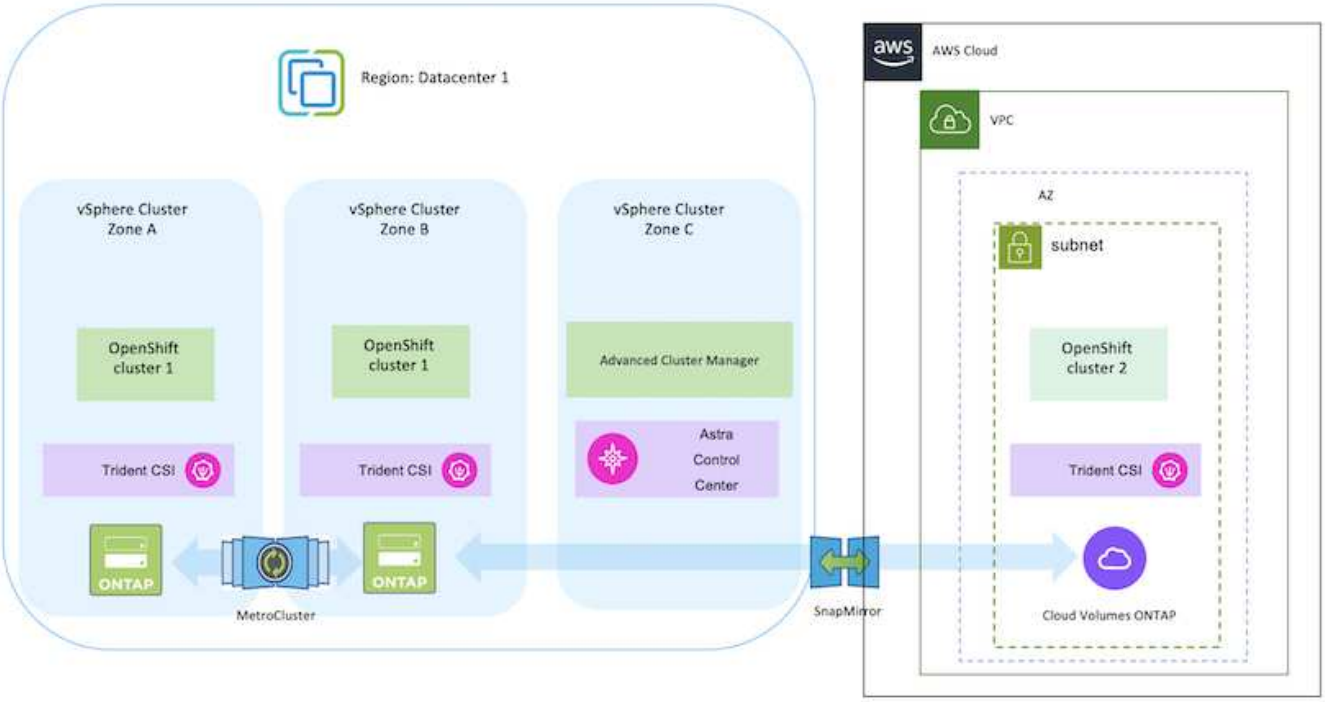
Kunden sind möglicherweise an einem Punkt ihrer Modernisierungsstrategie, wenn sie einige ausgewählte Workloads oder alle Workloads aus ihren Datacentern in die Cloud verschieben möchten. Sie können aus verschiedenen Gründen dafür entscheiden, selbst

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.

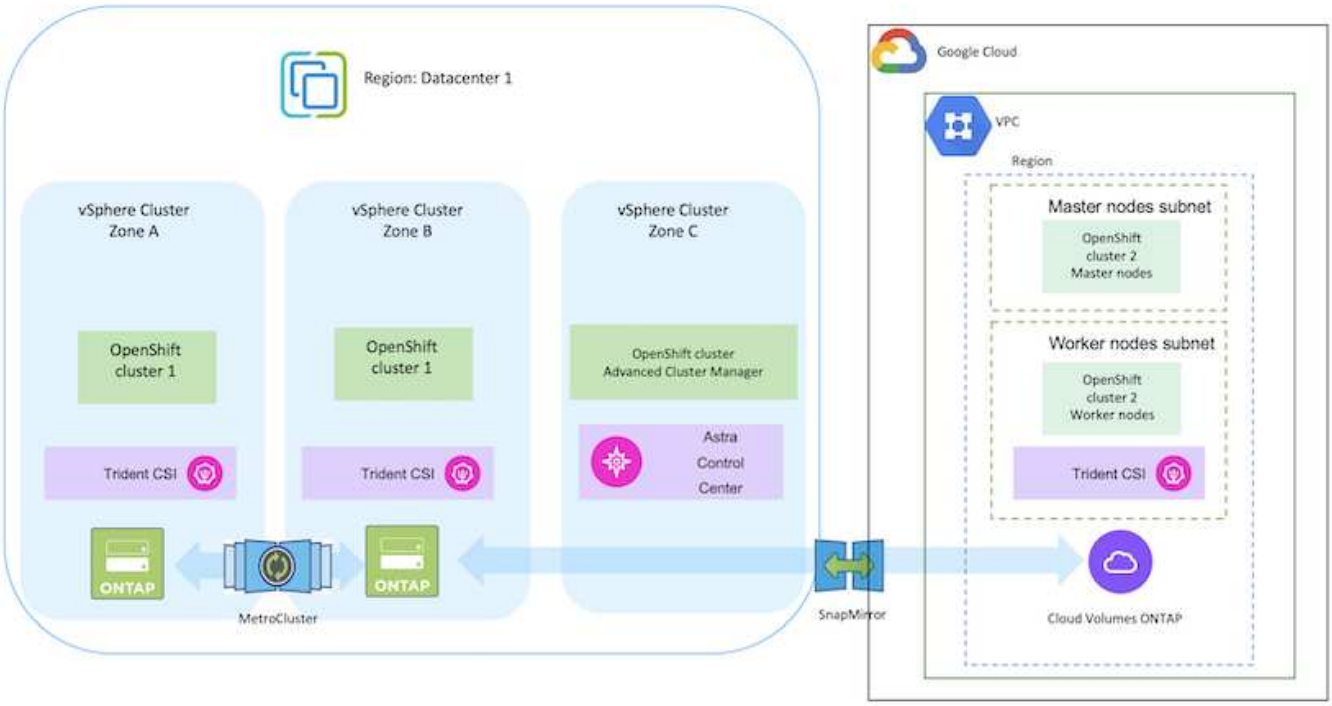
NetApp Cloud Volumes ONTAP Storage bietet Datensicherung, Zuverlässigkeit und Flexibilität für Container-Implementierungen in AWS, Azure und Google Cloud. Astra Trident dient als dynamische Storage-bereitstellung zur Nutzung des persistenten Cloud Volumes ONTAP Storage für zustandsbehaftete Applikationen 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

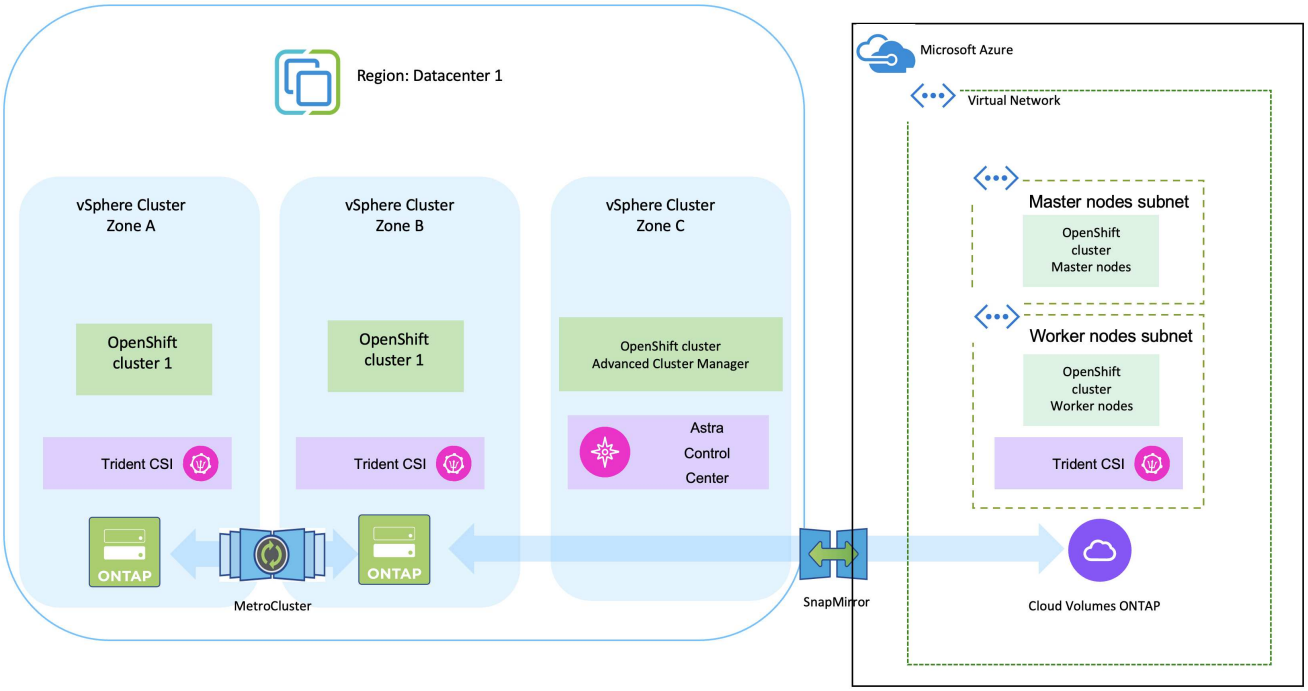


On-Premises und Google Cloud



On-Premises-Systeme und Azure Cloud

[redacted]



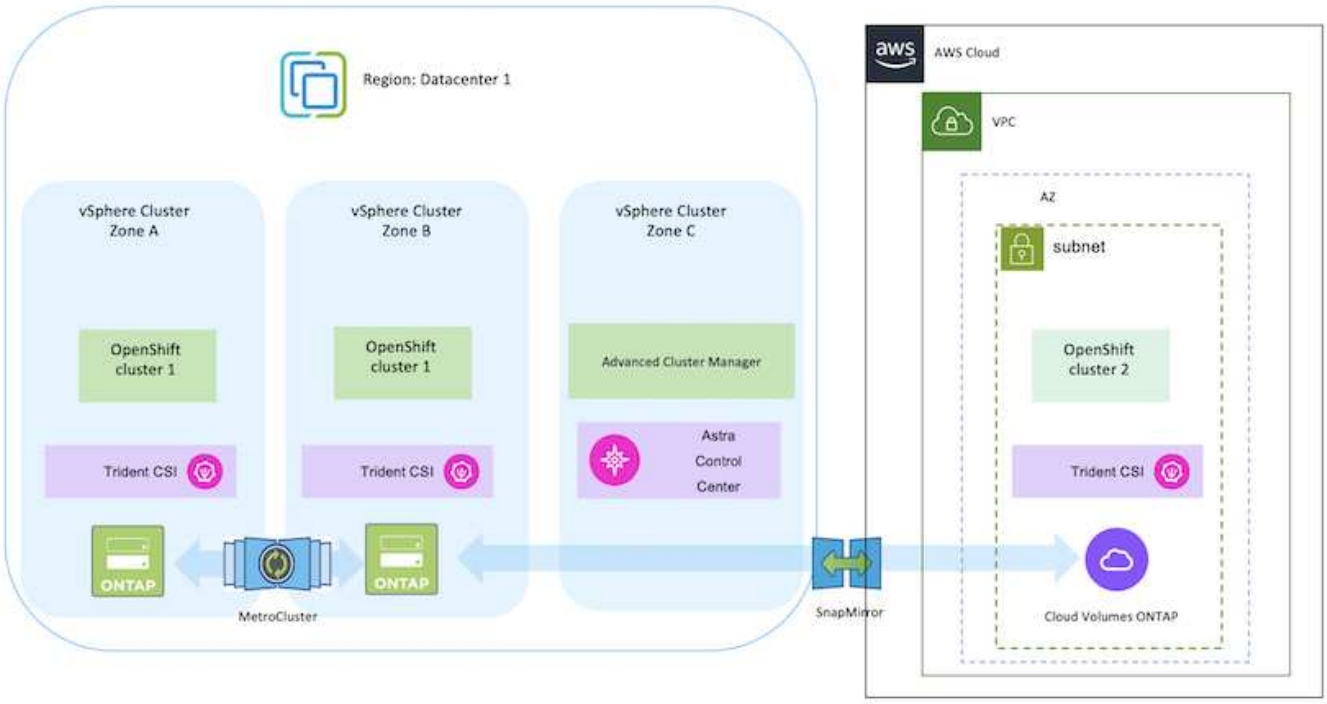
[redacted]

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.

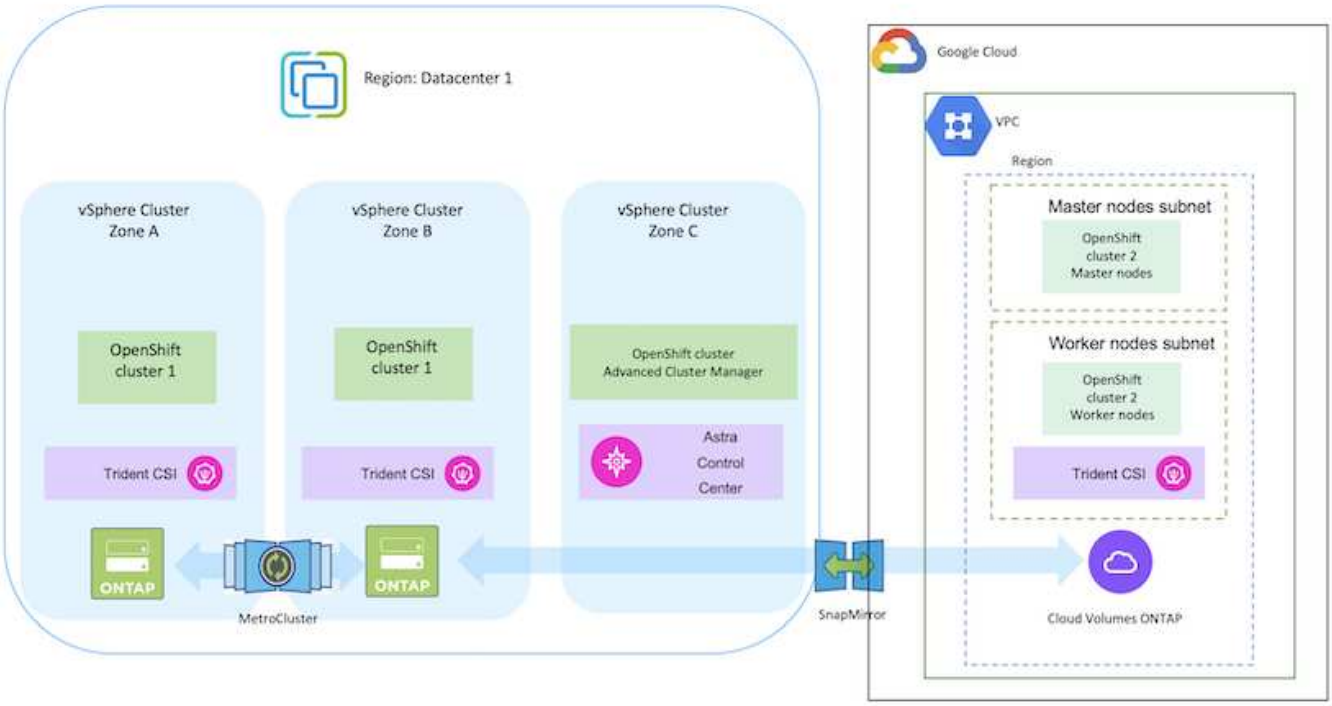
Kubernetes unterstützt zwei Volume-Bindungsmodi: - Wenn ***VolumeBindingMode* auf *Immediate*** (Standard) eingestellt ist, erstellt Astra Trident das Volume ohne Topologieorientierung. Persistente Volumes werden erstellt, ohne dass sie von den Planungsanforderungen des anfragenden Pods abhängig sind. - 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

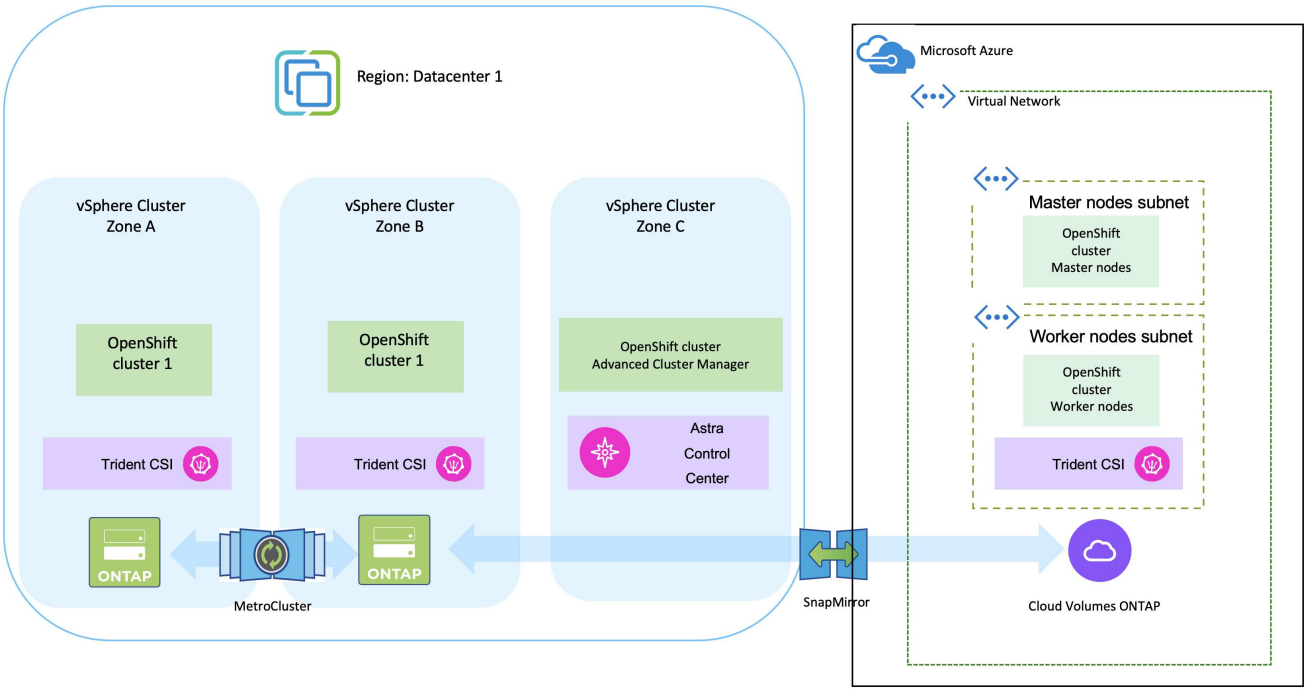
Importieren von OpenShift-Clustern in Astra Control Center

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.

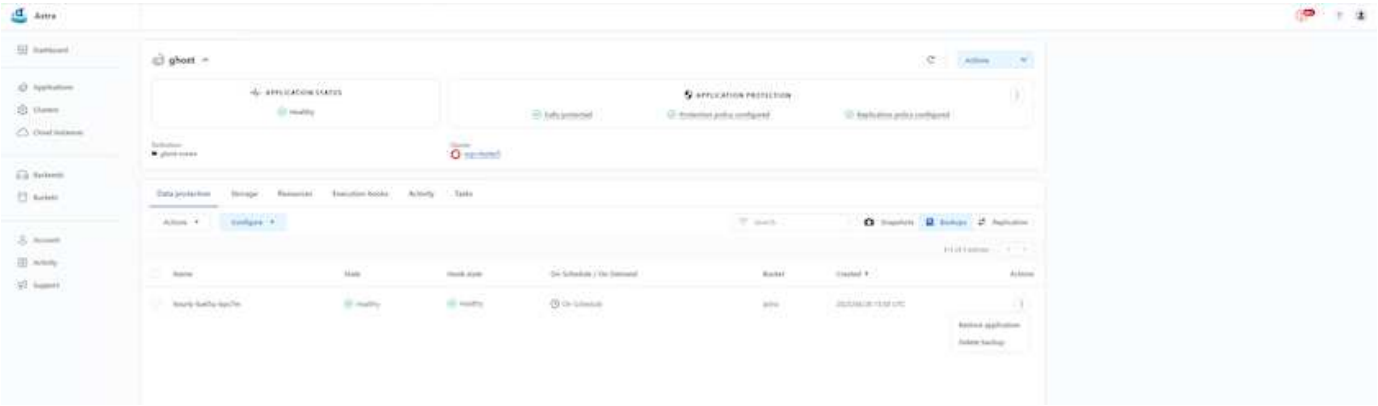
Die Anforderungen an die Datensicherung reichen von dem Zurücksetzen auf eine zeitpunktgenaue Kopie bis hin zum automatischen Failover auf eine andere Fehlerdomäne ohne menschliches Eingreifen. Viele Kunden entscheiden sich für ONTAP als bevorzugte Storage-Plattform für ihre Kubernetes-Applikationen, 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

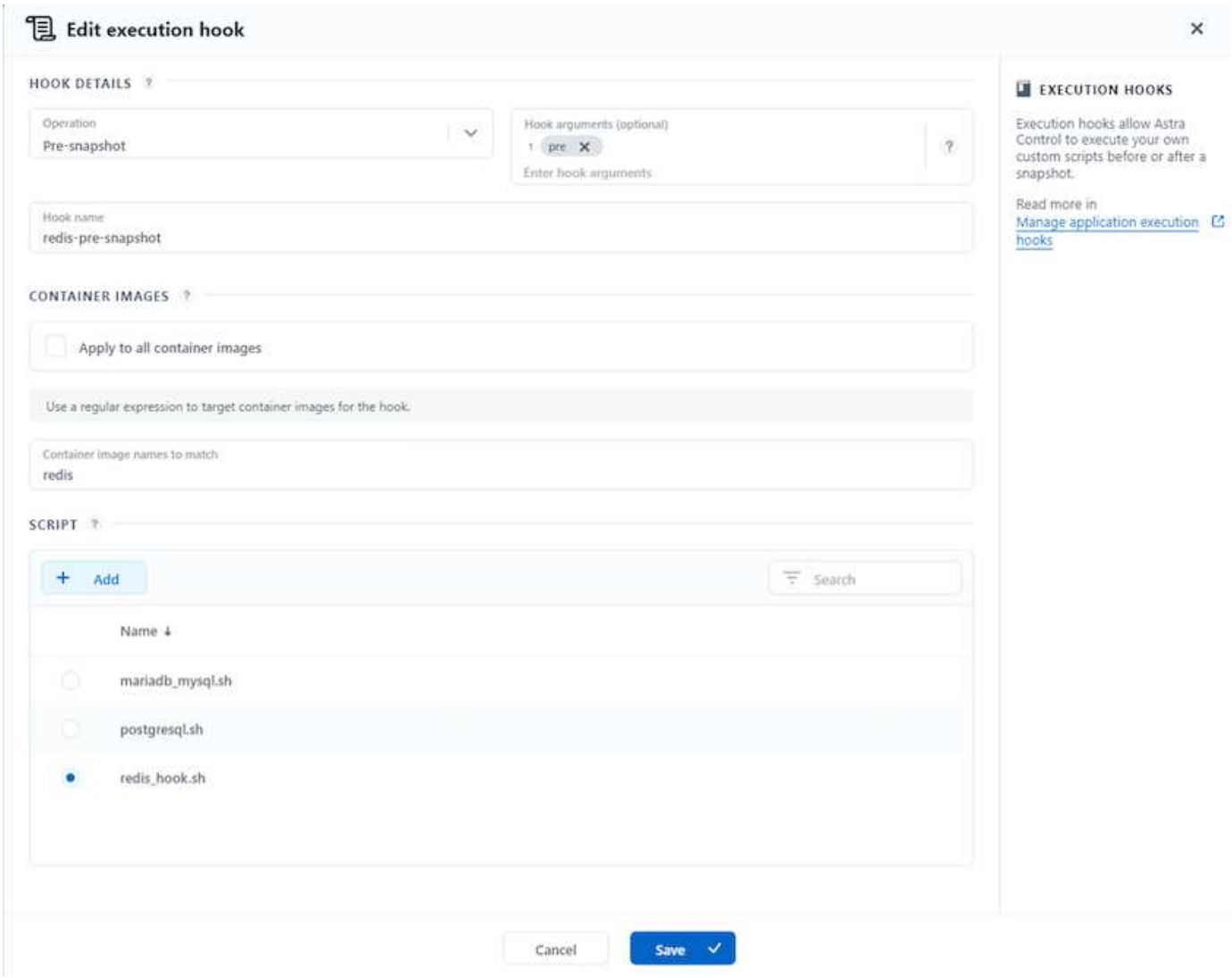


Anwendungsspezifische Ausführungshaken

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.

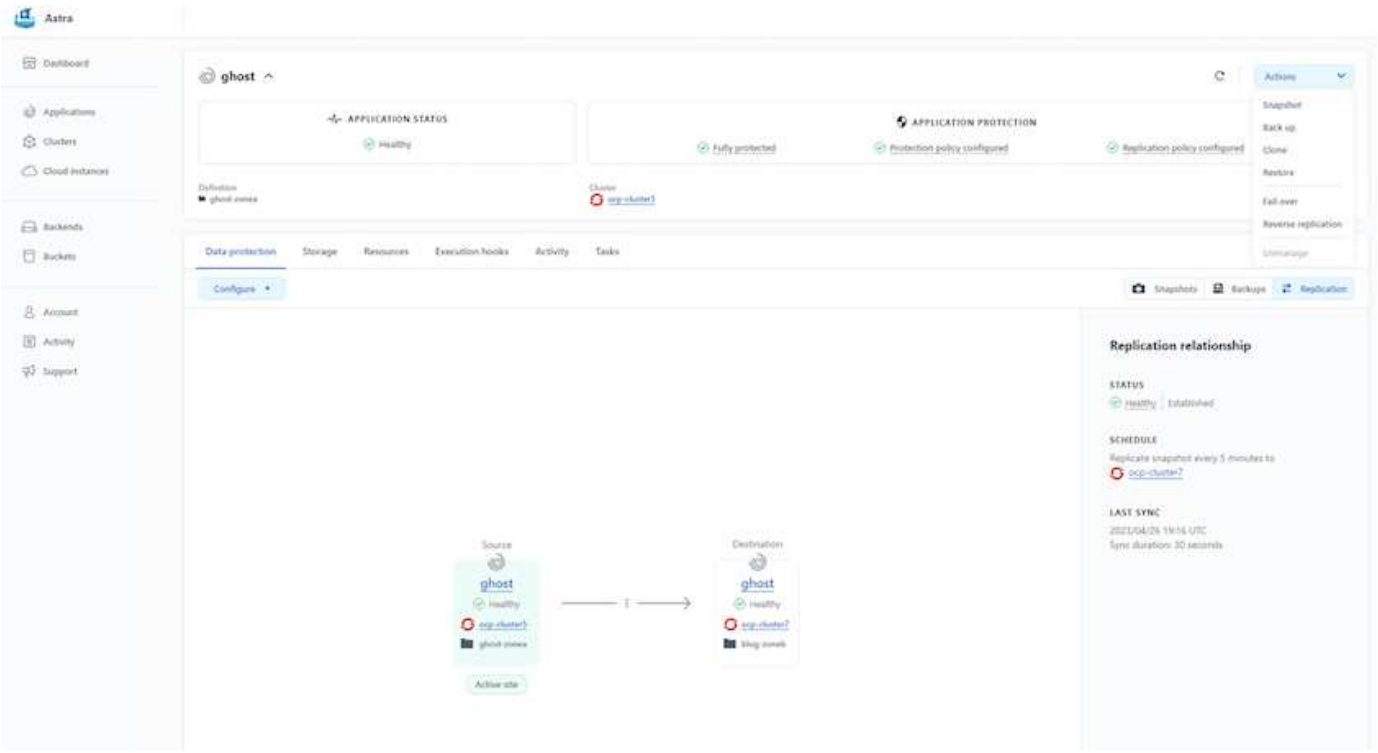
Beispiel-Ausführungshaken für Pre-Snapshot einer redis-Anwendung.



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



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