



# **On-Premises**

## **NetApp Solutions**

NetApp  
April 26, 2024

This PDF was generated from <https://docs.netapp.com/de-de/netapp-solutions/rhhc/rhhc-op-solution.html> on April 26, 2024. Always check docs.netapp.com for the latest.

# Inhalt

- NetApp Hybrid-Multi-Cloud-Lösungen für Container-Workloads mit Red hat OpenShift . . . . . 1
  - Überblick . . . . . 1
  - NetApp Lösung mit Container-Plattform-Workloads von Red hat OpenShift auf VMware . . . . . 3
  - Bereitstellung und Konfiguration der Container-Plattform Red hat OpenShift unter VMware . . . . . 4
  - Datensicherung mit Astra . . . . . 7
  - Datenmigration über Astra Control Center . . . . . 12

# 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



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

**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



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

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

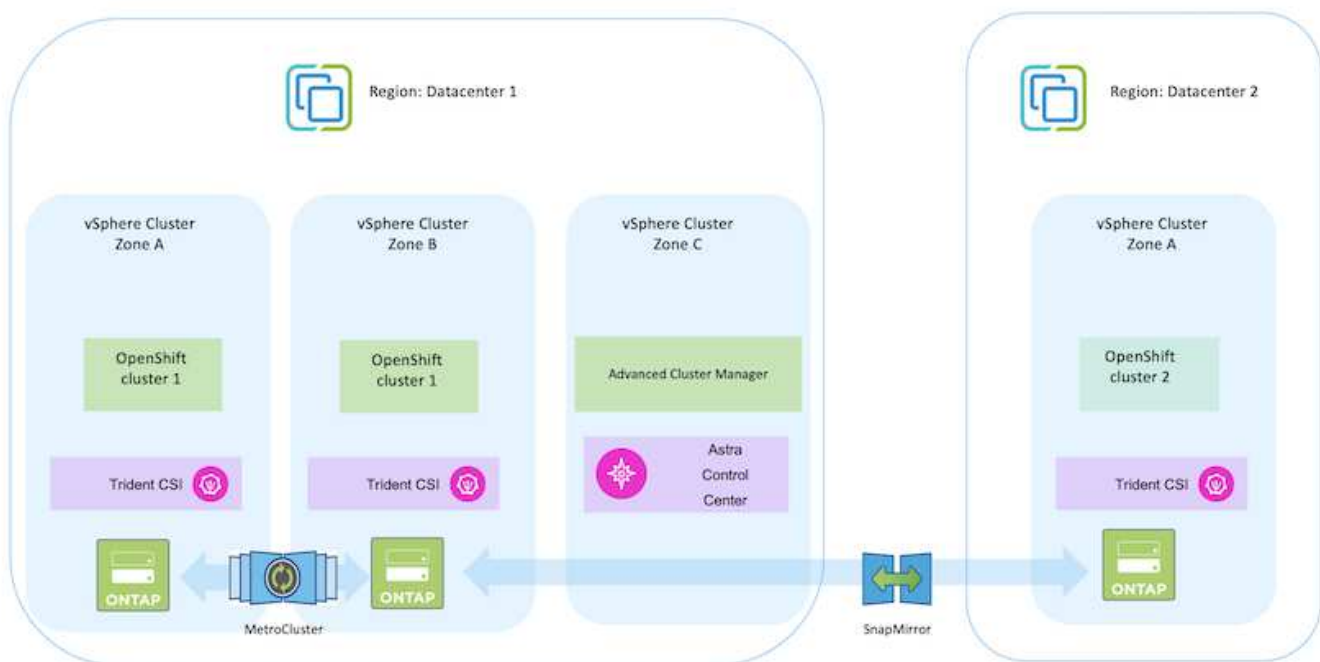
produktionsbereite Umgebung für die Bereitstellung ihrer Container-Workloads zu schaffen. Die OCP Cluster können auf VMware oder Bare Metal bereitgestellt werden.

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

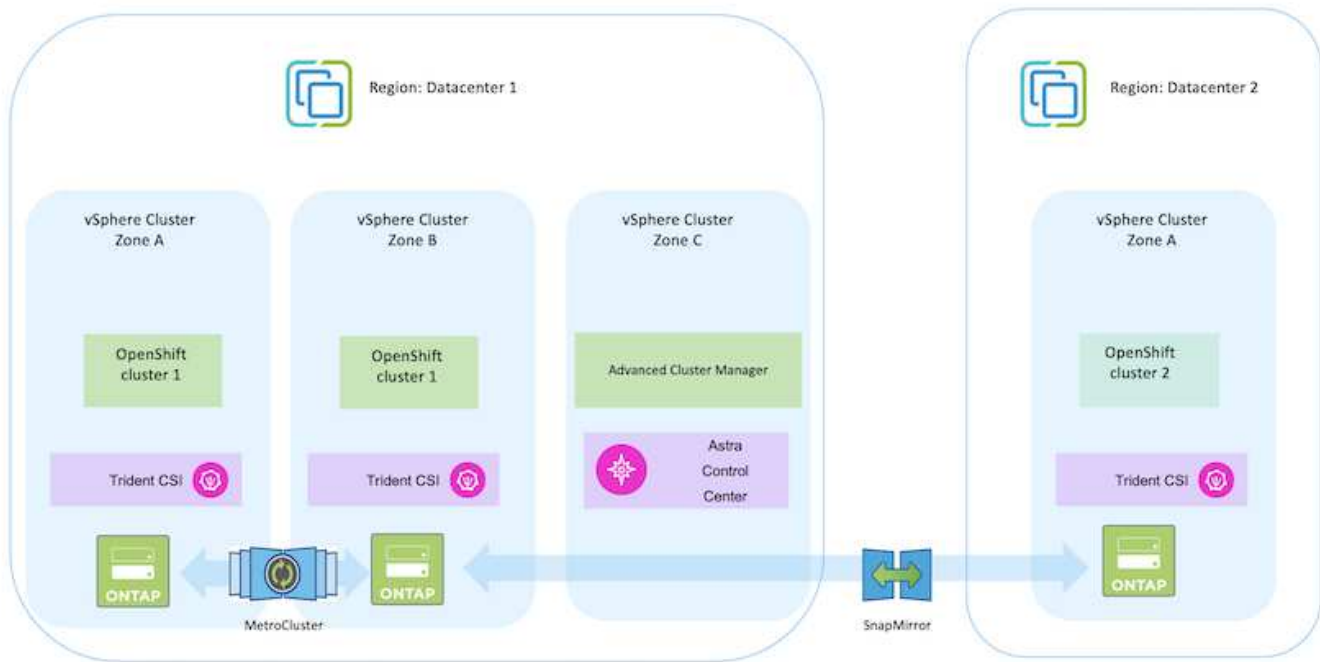
Dieser Abschnitt beschreibt einen allgemeinen Workflow, in dem erläutert wird, wie OpenShift-Cluster eingerichtet und gemanagt und zustandsbehaftete Anwendungen auf ihnen verwaltet werden. Es zeigt die Nutzung von NetApp ONTAP Storage-Arrays mit Hilfe von Astra Trident zur Bereitstellung persistenter 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 Datenschutzoptionen 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 Disaster 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.

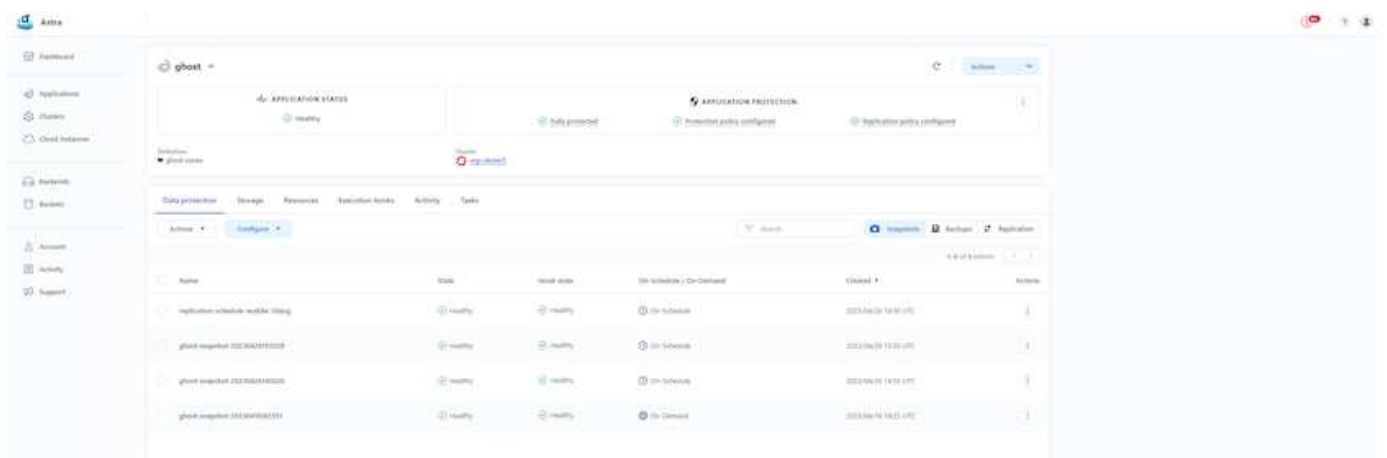
Die Datensicherung in ONTAP kann über Ad-hoc oder richtliniengesteuert erfolgen - **Snapshot - Backup und Restore**

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

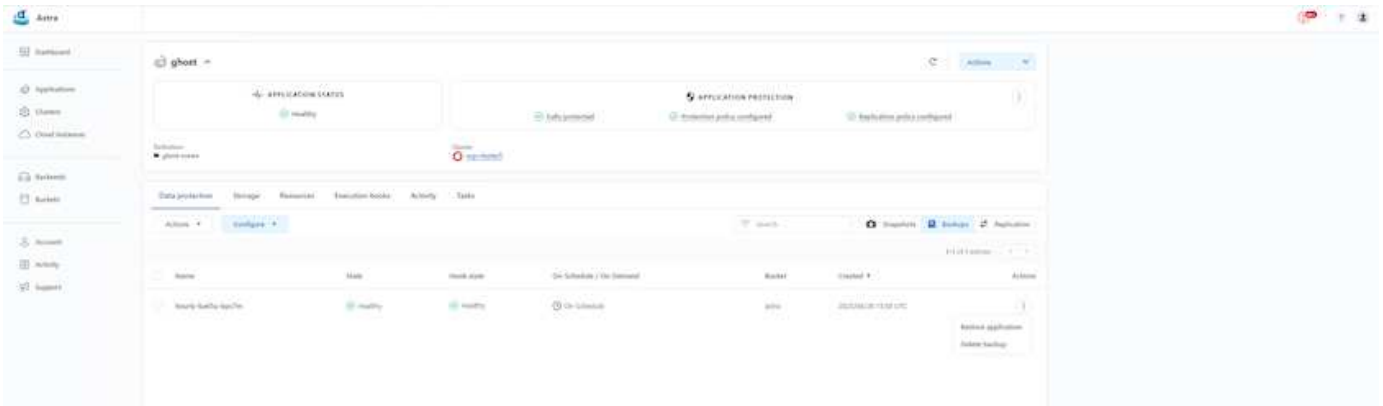


## Sichern und Wiederherstellen mit ACC

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 ✕ ?

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

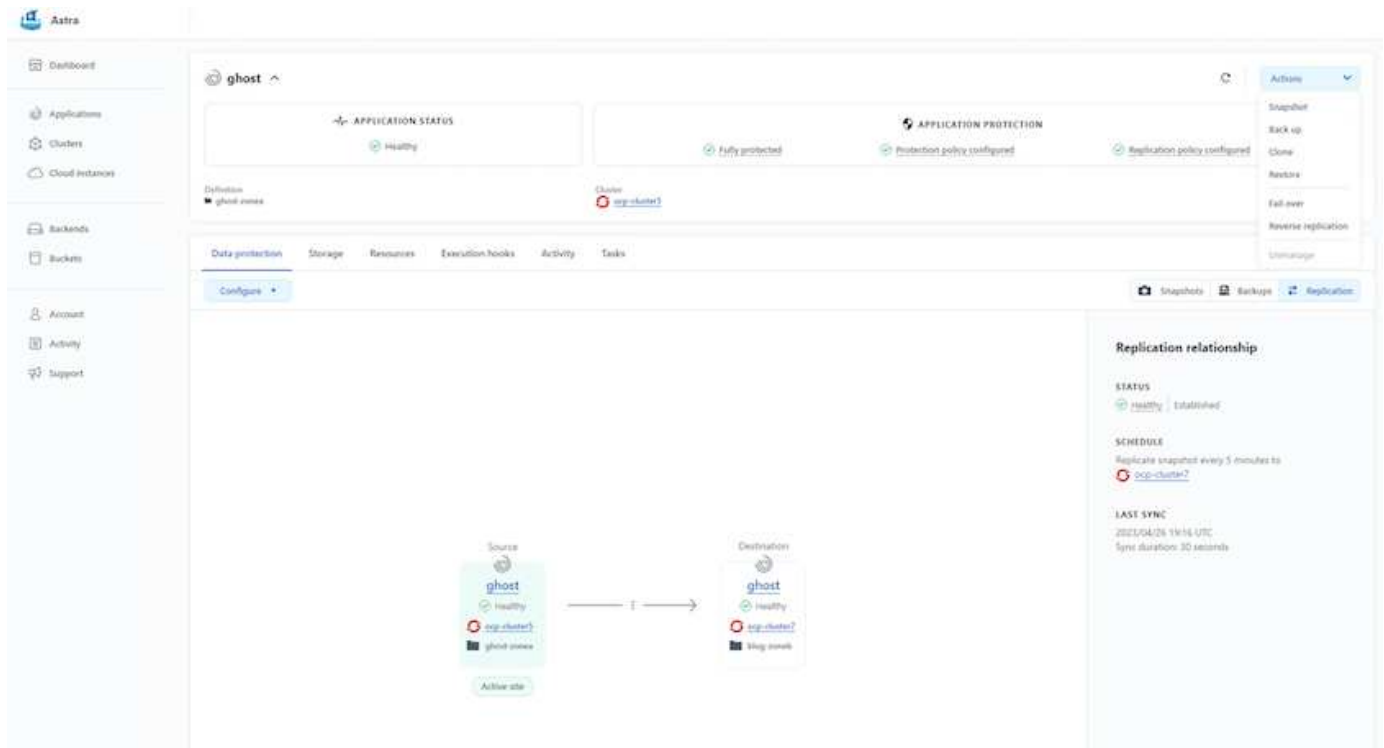
Für regionalen Schutz oder für eine Lösung mit niedriger RPO und RTO, kann eine Applikation auf eine andere Kubernetes-Instanz repliziert werden, die an einem anderen Standort, vorzugsweise in einer anderen Region, ausgeführt wird. ACC verwendet ONTAP Async SnapMirror mit einem Recovery Point Objective von nur 5 Minuten. 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

10



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

## Demovideo:

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

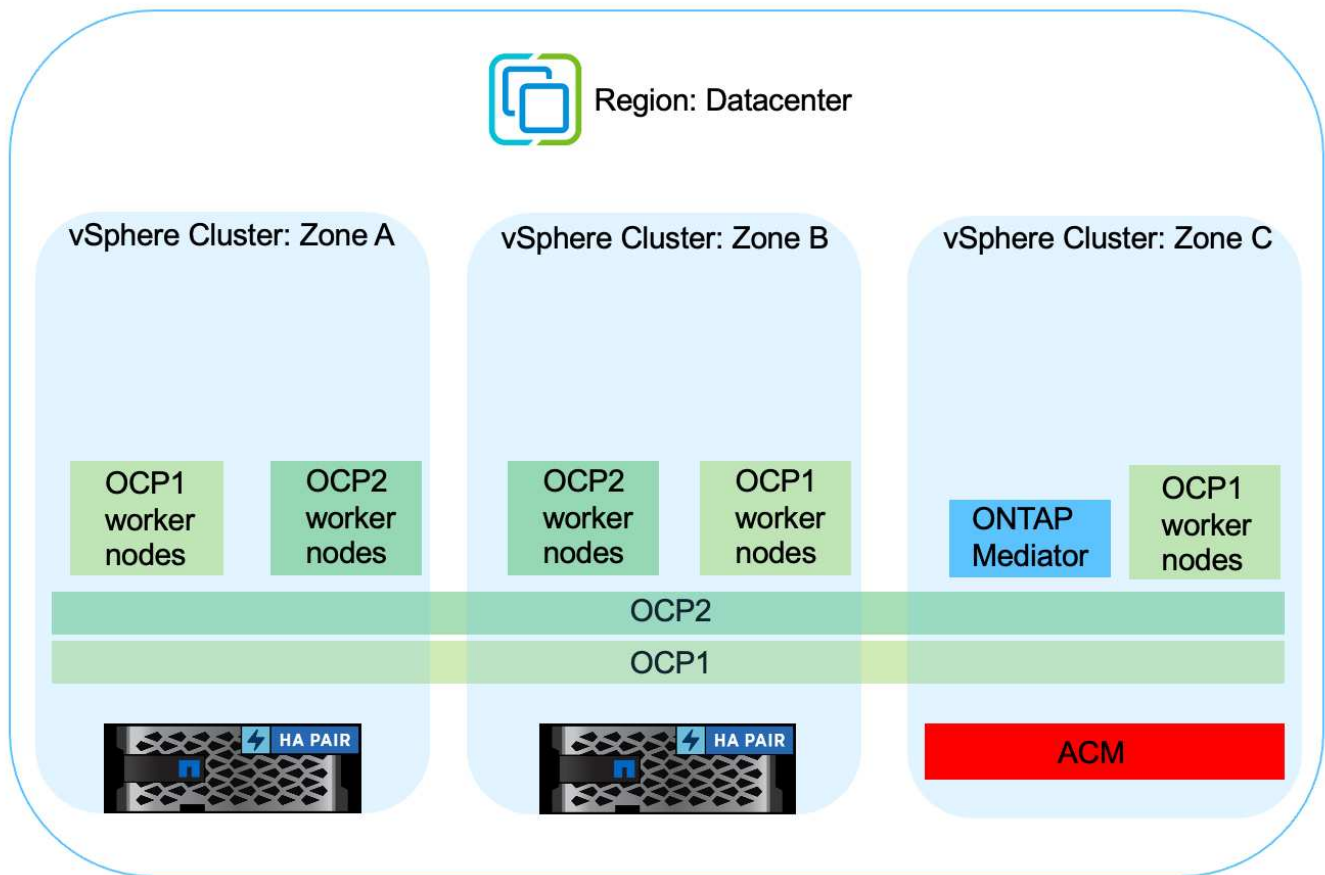
[Datensicherung mit Astra Control Center](#)

## 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 management console interface. On the left is a sidebar with navigation links: Dashboard, Applications, Clusters, Cloud instances, Backends, Buckets, Account, Activity, and Support. The main content area is titled 'ghost' and shows the 'APPLICATION STATUS' as 'Healthy'. Below this, it indicates 'Fully protected' and 'APPLICATION PROTECTION' with 'Protection policy configured' and 'Replication policy configured'. A 'Data protection' tab is selected, showing a 'Configure' button. A diagram illustrates the replication relationship between a 'Source' and a 'Destination', both labeled 'ghost' and 'Healthy', connected by a double-headed arrow. The 'Destination' also shows 'oci-cluster2' and 'Blog posts'. On the right, a 'Replication relationship' panel provides details: STATUS is 'Healthy' and 'Established'; SCHEDULE is 'Replicate snapshot every 5 minutes to oci-cluster2'; and LAST SYNC is '2023/04/26 19:16 UTC' with a 'Sync duration: 30 seconds'. An 'Actions' dropdown menu is visible on the far right, containing options like Snapshot, Back up, Clone, Restore, Fail over, Reverse replication, and Unmanage.

## 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, BEISPIELHAFT 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.