



Openshift für lokale Anwendungen

NetApp public and hybrid cloud solutions

NetApp
February 04, 2026

Inhalt

OpenShift für lokale Anwendungen	1
NetApp -Lösung mit Red Hat OpenShift Container-Plattform-Workloads auf VMware	1
Datenschutz- und Migrationslösung für OpenShift-Container-Workloads mit Trident Protect	1
Bereitstellen und Konfigurieren der Red Hat OpenShift Container-Plattform auf VMware	2
Datenschutz bei Astra	4
Schnappschuss mit ACC	4
Sichern und Wiederherstellen mit ACC	5
Anwendungsspezifische Ausführungs-Hooks	5
Beispiel-Ausführungs-Hook für den Pre-Snapshot einer Redis-Anwendung.	6
Replikation mit ACC	6
Geschäftskontinuität mit MetroCluster	7
Datenmigration mit Trident Protect	8
Datenmigration zwischen verschiedenen Kubernetes-Umgebungen	8

OpenShift für lokale Anwendungen

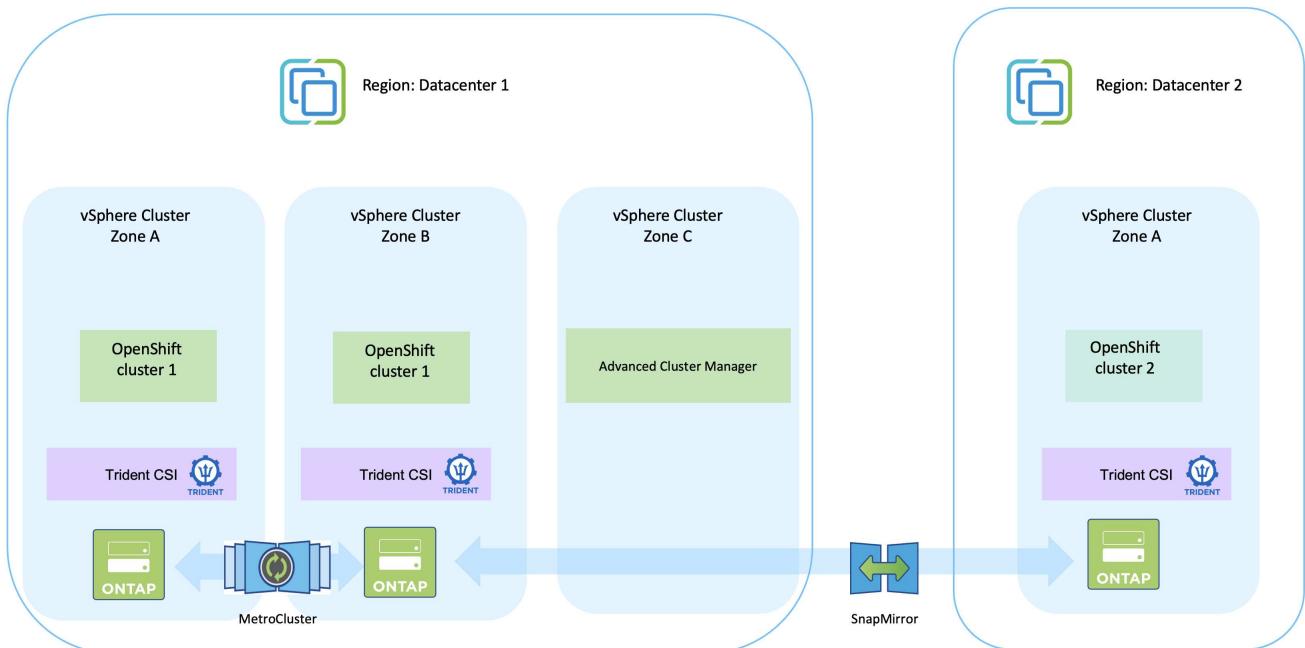
NetApp -Lösung mit Red Hat OpenShift Container-Plattform-Workloads auf VMware

Wenn Kunden ihre modernen containerisierten Anwendungen auf der Infrastruktur ihrer privaten Rechenzentren ausführen müssen, können sie dies tun. Sie sollten die Red Hat OpenShift-Containerplattform (OCP) für eine erfolgreiche produktionsbereite Umgebung zur Bereitstellung ihrer Container-Workloads planen und bereitstellen. Ihre OCP-Cluster können auf VMware oder Bare Metal bereitgestellt werden.

NetApp ONTAP Speicher bietet Datenschutz, Zuverlässigkeit und Flexibilität für Containerbereitstellungen. Trident dient als dynamischer Speicherbereitsteller, um persistenten ONTAP Speicher für zustandsbehaftete Anwendungen der Kunden zu nutzen. NetApp Trident Protect kann für die zahlreichen Datenverwaltungsanforderungen von Stateful-Anwendungen wie Datenschutz, Migration und Geschäftskontinuität verwendet werden.

Mit VMware vSphere bieten NetApp ONTAP -Tools ein vCenter-Plugin, das zum Bereitstellen von Datenspeichern verwendet werden kann. Wenden Sie Tags an und verwenden Sie sie mit OpenShift zum Speichern der Knotenkonfiguration und -daten. NVMe-basierter Speicher bietet geringere Latenz und hohe Leistung.

Datenschutz- und Migrationslösung für OpenShift-Container-Workloads mit Trident Protect



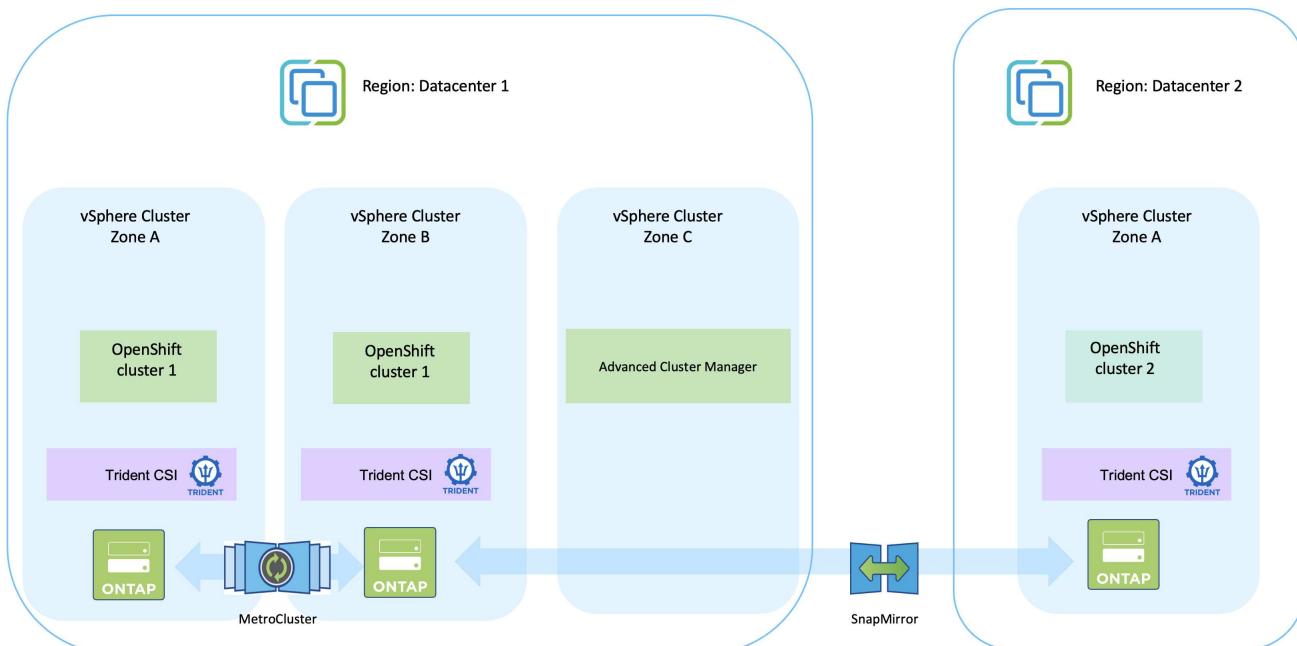
Bereitstellen und Konfigurieren der Red Hat OpenShift Container-Plattform auf VMware

In diesem Abschnitt wird ein allgemeiner Workflow zum Einrichten und Verwalten von OpenShift-Clustern und zum Verwalten von statusbehafteten Anwendungen darauf beschrieben. Es zeigt die Verwendung von NetApp ONTAP Speicherarrays mit Hilfe von Trident zur Bereitstellung persistenter Volumes.



Es gibt mehrere Möglichkeiten, Red Hat OpenShift Container-Plattformcluster bereitzustellen. Diese allgemeine Beschreibung des Setups enthält Dokumentationslinks für die jeweils verwendete Methode. Weitere Methoden finden Sie in den entsprechenden Links im "Ressourcenbereich".

Hier ist ein Diagramm, das die auf VMware in einem Rechenzentrum bereitgestellten Cluster darstellt.



Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

Bereitstellen und Konfigurieren einer CentOS-VM

- Es wird in der VMware vSphere-Umgebung bereitgestellt.
- Diese VM wird zum Bereitstellen einiger Komponenten wie NetApp Trident und NetApp Trident Protect für die Lösung verwendet.
- Während der Installation wird auf dieser VM ein Root-Benutzer konfiguriert.

Bereitstellen und Konfigurieren eines OpenShift Container Platform-Clusters auf VMware vSphere (Hub-Cluster)

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

Denken Sie an Folgendes: – Erstellen Sie einen öffentlichen und privaten SSH-Schlüssel, um ihn dem Installationsprogramm bereitzustellen. Diese Schlüssel werden bei Bedarf zum Anmelden bei den Master- und Worker-Knoten verwendet. – Laden Sie das Installationsprogramm vom unterstützten Installationsprogramm 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 Mindestanforderungen an CPU, Speicher und Festplatte erfüllen. (Siehe die VM-Erstellungsbefehle auf "[Das](#)" Seite für den Master und die Worker-Knoten, die diese Informationen bereitstellen) – Die DiskUUID sollte auf allen VMs aktiviert sein. – Erstellen Sie mindestens 3 Knoten für den Master und 3 Knoten für den Worker. – Sobald sie vom Installationsprogramm erkannt wurden, aktivieren Sie den Umschaltknopf für die VMware vSphere-Integration.



Installieren Sie Advanced Cluster Management auf dem Hub-Cluster

Dies wird mithilfe des Advanced Cluster Management Operator auf dem Hub-Cluster installiert. Beachten Sie die Anweisungen "[hier](#),".

Installieren Sie zwei zusätzliche OCP-Cluster (Quelle und Ziel).

- Die zusätzlichen Cluster können mithilfe des ACM auf dem Hub-Cluster bereitgestellt werden.
- Beachten Sie die Anweisungen "[hier](#),".

Konfigurieren des NetApp ONTAP -Speichers

- Installieren Sie einen ONTAP Cluster mit Konnektivität zu den OCP-VMs in der VMWare-Umgebung.
- Erstellen Sie eine SVM.
- Konfigurieren Sie NAS-Datenlebensdauer, um auf den Speicher in SVM zuzugreifen.

Installieren Sie NetApp Trident auf den OCP-Clustern

- Installieren Sie NetApp Trident auf allen drei Clustern: Hub-, Quell- und Zielcluster
- Beachten Sie die Anweisungen "[hier](#),".
- Erstellen Sie ein Speicher-Backend für ontap-nas.
- Erstellen Sie eine Speicherklasse für ontap-nas.
- Siehe Anweisungen "[hier](#),".

Bereitstellen einer Anwendung auf dem Quellcluster

Verwenden Sie OpenShift GitOps, um eine Anwendung bereitzustellen. (z. B. Postgres, Ghost)

Der nächste Schritt besteht darin, Trident Protect für den Datenschutz und die Datenmigration vom Quell- zum Zielcluster zu verwenden. Verweisen "hier," Anweisungen hierzu finden Sie unter.

Datenschutz bei Astra

Auf dieser Seite werden die Datenschutzoptionen für auf Red Hat OpenShift Container basierende Anwendungen angezeigt, die mit Trident Protect (ACC) auf VMware vSphere ausgeführt werden.

Wenn Benutzer ihre Anwendungen mit Red Hat OpenShift modernisieren, sollte eine Datenschutzstrategie vorhanden sein, um sie vor versehentlichem Löschen oder anderen menschlichen Fehlern zu schützen. Oft ist auch aus regulatorischen oder Compliance-Gründen eine Schutzstrategie erforderlich, um die Daten vor einer Katastrophe zu schützen.

Die Anforderungen an den Datenschutz variieren von der Rückkehr zu einer Point-in-Time-Kopie bis hin zum automatischen Failover auf eine andere Fehlerdomäne ohne menschliches Eingreifen. Viele Kunden wählen ONTAP als bevorzugte Speicherplattform für ihre Kubernetes-Anwendungen aufgrund der umfangreichen Funktionen wie Mandantenfähigkeit, Multiprotokoll, hohe Leistung und Kapazitätsangebote, Replikation und Caching für mehrere Standorte, Sicherheit und Flexibilität.

Datenschutz in ONTAP kann durch Ad-hoc- oder richtliniengesteuerte **Snapshots - Backups und Wiederherstellungen** erreicht werden.

Sowohl Snapshot-Kopien als auch Backups schützen die folgenden Datentypen: - **Die Anwendungsmetadata**, die den Status der Anwendung darstellen - **Alle mit der Anwendung verknüpften persistenten Datenvolumes** - **Alle zur Anwendung gehörenden Ressourcenartefakte**

Schnappschuss mit ACC

Mithilfe von Snapshot mit ACC kann eine zeitpunktbezogene Kopie der Daten erfasst werden. Die Schutzrichtlinie definiert die Anzahl der aufzubewahrenen Snapshot-Kopien. Die Mindestzeitplanoption ist stündlich. Manuelle Snapshot-Kopien auf Abruf können jederzeit und in kürzeren Abständen als geplante Snapshot-Kopien erstellt werden. Snapshot-Kopien werden auf demselben bereitgestellten Volume wie die App gespeichert.

Snapshot mit ACC konfigurieren

The screenshot shows the Astra Control web interface. On the left, there's a sidebar with navigation links like Dashboard, Applications, Clusters, Cloud Instances, Workflows, Buckets, Account, Activity, and Support. The main area is titled 'ghost' and contains sections for 'APPLICATION STATUS' (showing healthy), 'APPLICATION PROTECTION' (with 'Protect level' set to 'Fully protected' and 'Protection policy' as 'Not configured'), and 'Data protection' (listing four scheduled backups). The 'Data protection' table has columns for Name, Mode, Health state, On Schedule / On Demand, and Created.

Name	Mode	Health state	On Schedule / On Demand	Created
replication-schedule weekly 00:00	healthy	healthy	On Schedule	2023/09/05 14:56 (UTC)
ghost-backup-20230905T100000	healthy	healthy	On Schedule	2023/09/05 14:56 (UTC)
ghost-backup-20230905T100000	healthy	healthy	On Schedule	2023/09/05 14:56 (UTC)
ghost-backup-20230905T100000	healthy	healthy	On Demand	2023/09/05 14:56 (UTC)

Sichern und Wiederherstellen mit ACC

Eine Sicherung basiert auf einem Snapshot. Trident Protect kann mithilfe von CSI Snapshot-Kopien erstellen und mithilfe der zeitpunktbezogenen Snapshot-Kopie eine Sicherung durchführen. Das Backup wird in einem externen Objektspeicher gespeichert (jeder S3-kompatible, einschließlich ONTAP S3 an einem anderen Standort). Für geplante Sicherungen und die Anzahl der aufzubewahrenen Sicherungsversionen können Schutzrichtlinien konfiguriert werden. Das minimale RPO beträgt eine Stunde.

Wiederherstellen einer Anwendung aus einer Sicherung mit ACC

ACC stellt die Anwendung aus dem S3-Bucket wieder her, in dem die Backups gespeichert sind.

This screenshot is similar to the one above, showing the Astra Control interface for the 'ghost' application. The 'Data protection' table includes a new row for a scheduled backup named 'Security Audit Day Snapshot'. A context menu is open over this row, with options 'Revert application' and 'Delete backup' visible.

Anwendungsspezifische Ausführungs-Hooks

Darüber hinaus können Ausführungs-Hooks so konfiguriert werden, dass sie in Verbindung mit einem Datenschutzzugang einer verwalteten App ausgeführt werden. Obwohl Datenschutzfunktionen auf Speicher-Array-Ebene verfügbar sind, sind häufig zusätzliche Schritte erforderlich, um Backups und Wiederherstellungen anwendungskonsistent zu gestalten. Die app-spezifischen zusätzlichen Schritte könnten sein: – vor oder nach der Erstellung einer Snapshot-Kopie. - bevor oder nachdem ein Backup erstellt wurde. - nach der Wiederherstellung aus einer Snapshot-Kopie oder einem Backup.

Astra Control kann diese app-spezifischen Schritte ausführen, die als benutzerdefinierte Skripte, sogenannte Ausführungs-Hooks, codiert sind.

["NetApp Verda GitHub-Projekt"](#) bietet Ausführungs-Hooks für beliebte Cloud-native Anwendungen, um den Schutz von Anwendungen unkompliziert, robust und leicht orchestrierbar zu machen. Tragen Sie gerne zu diesem Projekt bei, wenn Sie über genügend Informationen für eine Anwendung verfügen, die nicht im

Repository enthalten ist.

Beispiel-Ausführungs-Hook für den Pre-Snapshot einer Redis-Anwendung.

The screenshot shows the configuration of an execution hook for a Redis application. In the 'HOOK DETAILS' section, the operation is set to 'Pre-snapshot' with the argument 'pre'. The 'CONTAINER IMAGES' section specifies the container image 'redis'. In the 'SCRIPT' section, the script 'redis_hook.sh' is selected. The right sidebar contains a general description of execution hooks and a link to 'Manage application execution hooks'.

Replikation mit ACC

Zum regionalen Schutz oder für eine Lösung mit niedrigem RPO und RTO kann eine Anwendung auf eine andere Kubernetes-Instanz repliziert werden, die an einem anderen Standort, vorzugsweise in einer anderen Region, ausgeführt wird. Trident Protect nutzt ONTAP async SnapMirror mit einem RPO von nur 5 Minuten. Die Replikation erfolgt durch Replikation auf ONTAP. Anschließend werden durch ein Failover die Kubernetes-Ressourcen im Zielcluster erstellt.

i Beachten Sie, dass sich die Replikation von der Sicherung und Wiederherstellung unterscheidet, bei der die Sicherung an S3 gesendet und die Wiederherstellung von S3 aus durchgeführt wird. Weitere Einzelheiten zu den Unterschieden zwischen den beiden Datenschutzarten finden Sie unter folgendem Link: [hier](#).

Verweisen "hier," für Anweisungen zur Einrichtung von SnapMirror .

SnapMirror mit ACC

The screenshot shows the Astra application management interface. On the left, there's a sidebar with options like Dashboard, Applications, Cloud Instances, Backends, Buckets, Account, Activity, and Support. The main area is titled 'ghost' and contains sections for Application Status (Healthy), Application Protection (Fully protected), and Data protection. It shows a replication relationship between a Source host ('ghost') and a Destination host ('ghost'). The Source host has a snapshot scheduled every 5 minutes to the Destination host. The last sync was at 2023/04/26 19:14 UTC with a duration of 30 seconds. The status is healthy and established.



Die Speichertreiber „san-economy“ und „nas-economy“ unterstützen die Replikationsfunktion nicht. Verweisen [hier](#), für weitere Einzelheiten.

Demo-Video:

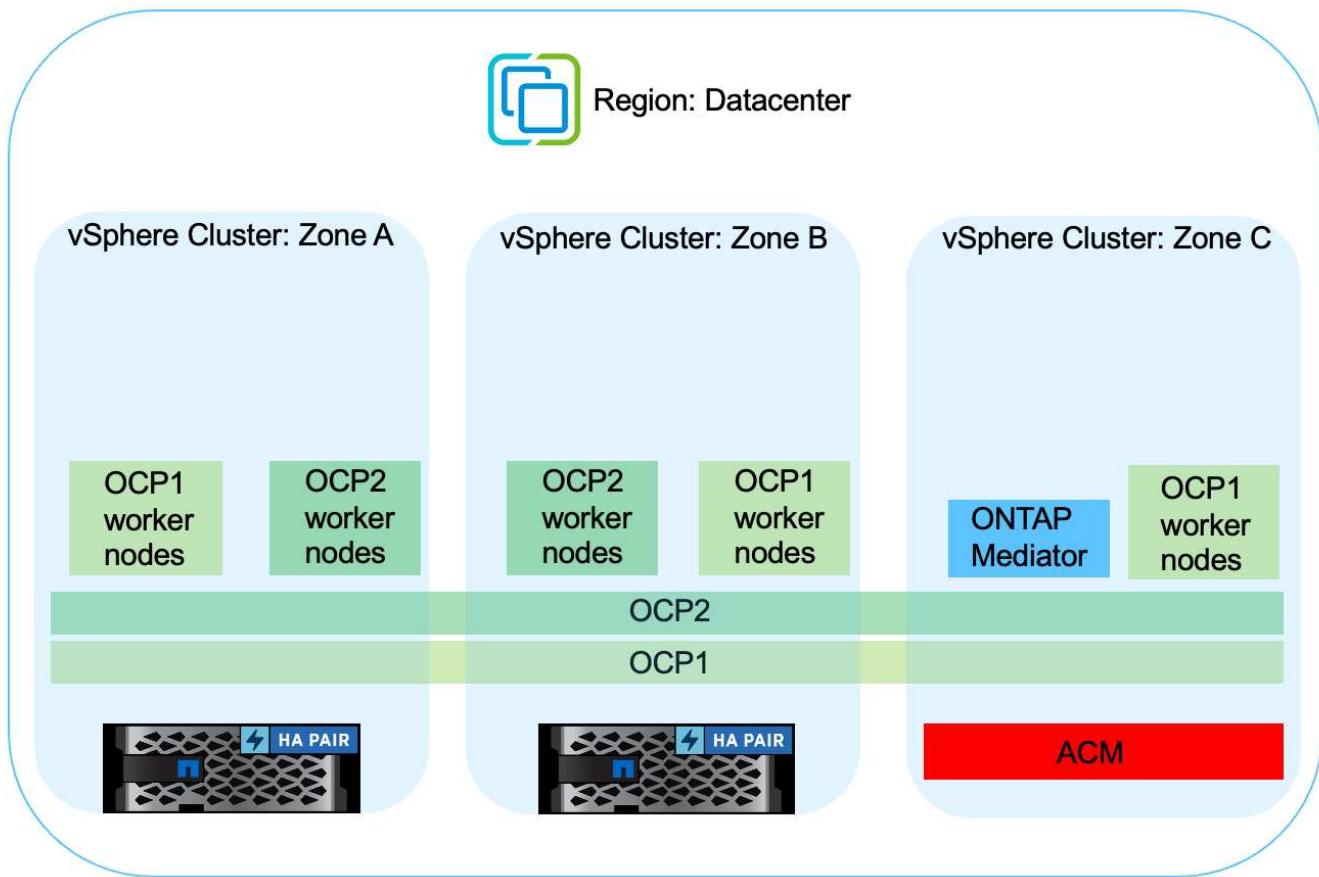
["Demonstrationsvideo zur Notfallwiederherstellung mit Trident Protect"](#)

Datenschutz mit Trident Protect

Die meisten unserer Hardwareplattformen für ONTAP verfügen über Hochverfügbarkeitsfunktionen zum Schutz vor Geräteausfällen, sodass keine Notfallwiederherstellung erforderlich ist. Zum Schutz vor Feuer oder anderen Katastrophen und um das Geschäft mit Null-RPO und niedrigem RTO fortzuführen, wird jedoch häufig eine MetroCluster Lösung verwendet.

Kunden, die derzeit über ein ONTAP -System verfügen, können es auf MetroCluster erweitern, indem sie unterstützte ONTAP -Systeme innerhalb der Entfernungsbeschränkungen hinzufügen, um eine Notfallwiederherstellung auf Zonenebene bereitzustellen. Trident, das CSI (Container Storage Interface), unterstützt NetApp ONTAP einschließlich MetroCluster -Konfiguration sowie andere Optionen wie Cloud Volumes ONTAP, Azure NetApp Files, AWS FSx ONTAP usw. Trident bietet fünf Speichertreiberoptionen für ONTAP und alle werden für die MetroCluster Konfiguration unterstützt. Verweisen [hier](#). Weitere Informationen zu den von Trident unterstützten ONTAP Speichertreibern finden Sie unter.

Die MetroCluster -Lösung erfordert eine Layer-2-Netzwerkerweiterung oder die Fähigkeit, von beiden Fehlerdomänen aus auf dieselbe Netzwerkadresse zuzugreifen. Sobald die MetroCluster Konfiguration eingerichtet ist, ist die Lösung für Anwendungsbesitzer transparent, da alle Volumes im MetroCluster -SVM geschützt sind und die Vorteile von SyncMirror (Null-RPO) nutzen.



Geben Sie für die Trident -Backend-Konfiguration (TBC) bei Verwendung der MetroCluster -Konfiguration nicht dataLIF und SVM an. Geben Sie die SVM-Verwaltungs-IP für managementLIF an und verwenden Sie die Anmeldeinformationen der Rolle vsadmin.

Details zu den Datenschutzfunktionen von Trident Protect sind verfügbar "[hier](#),"

Datenmigration mit Trident Protect

Diese Seite zeigt die Datenmigrationsoptionen für Container-Workloads auf Red Hat OpenShift-Clustern mit Trident Protect.

Kubernetes-Anwendungen müssen häufig von einer Umgebung in eine andere verschoben werden. Um eine Anwendung zusammen mit ihren persistenten Daten zu migrieren, kann NetApp Trident Protect verwendet 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 Informationen finden Sie unter "[hier](#)," .

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

- Replikation

- Sichern und Wiederherstellen

- Klon

Weitere Informationen finden Sie im "[Datenschutzbereich](#)" für die Optionen **Replikation und Sicherung und Wiederherstellung**.

Verweisen "[hier](#)," für weitere Details zum **Klonen**.

Durchführen der Datenreplikation mit ACC

The screenshot shows the Astra Cloud Control Center (ACC) interface. On the left, there's a sidebar with navigation links: Dashboard, Applications, Clusters, Cloud Instances, Backends, Buckets, Account, Activity, and Support. The main area is focused on the 'ghost' application. At the top, it displays 'APPLICATION STATUS' (Healthy) and 'APPLICATION PROTECTION' (Fully protected, Protection policy configured, Replication policy configured). Below this, there are tabs for Data protection, Storage, Resources, Execution hooks, Activity, and Tasks. The 'Data protection' tab is selected, showing a 'Configure' button and tabs for Snapshots, Backup, and Replication. The 'Replication relationship' section on the right shows a status of 'Established' with a green 'Healthy' icon. It indicates a scheduled replication every 5 minutes to 'occ-cluster2'. The last sync was at 2023/04/26 19:16 UTC with a duration of 30 seconds. Below this, there's a diagram showing the 'Source' (ghost cluster) replicating to the 'Destination' (ghost cluster), with an arrow pointing from Source to Destination.

Copyright-Informationen

Copyright © 2026 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 BESCHRÄNKKT 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, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT 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 IRGENDERINER 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.