



# **FlexPod Hybrid Cloud mit Cloud Volumes ONTAP für Epic**

FlexPod

NetApp  
August 28, 2024

# Inhalt

- FlexPod Hybrid Cloud mit Cloud Volumes ONTAP für Epic . . . . . 1
  - TR-4960: FlexPod Hybrid Cloud with Cloud Volumes ONTAP for Epic . . . . . 1
  - Lösungskomponenten . . . . . 3
  - Installation und Konfiguration . . . . . 8
  - SAN-Konfiguration . . . . . 13
  - Lösungvalidierung . . . . . 26
  - Schlussfolgerung . . . . . 36
  - Wo Sie weitere Informationen finden . . . . . 37

# FlexPod Hybrid Cloud mit Cloud Volumes ONTAP für Epic

## TR-4960: FlexPod Hybrid Cloud with Cloud Volumes ONTAP for Epic



In Zusammenarbeit mit:

Kamini Singh, NetApp

Der Schlüssel zu einer digitalen Transformation liegt darin, einfach mehr Daten zu nutzen. Krankenhäuser generieren große Datenmengen, um ihr Unternehmen zu betreiben und ihre Patienten effektiv zu versorgen. Die Daten werden bei der Behandlung von Patienten und bei der Verwaltung von Terminplänen und medizinischen Ressourcen des Personals erfasst und verarbeitet.

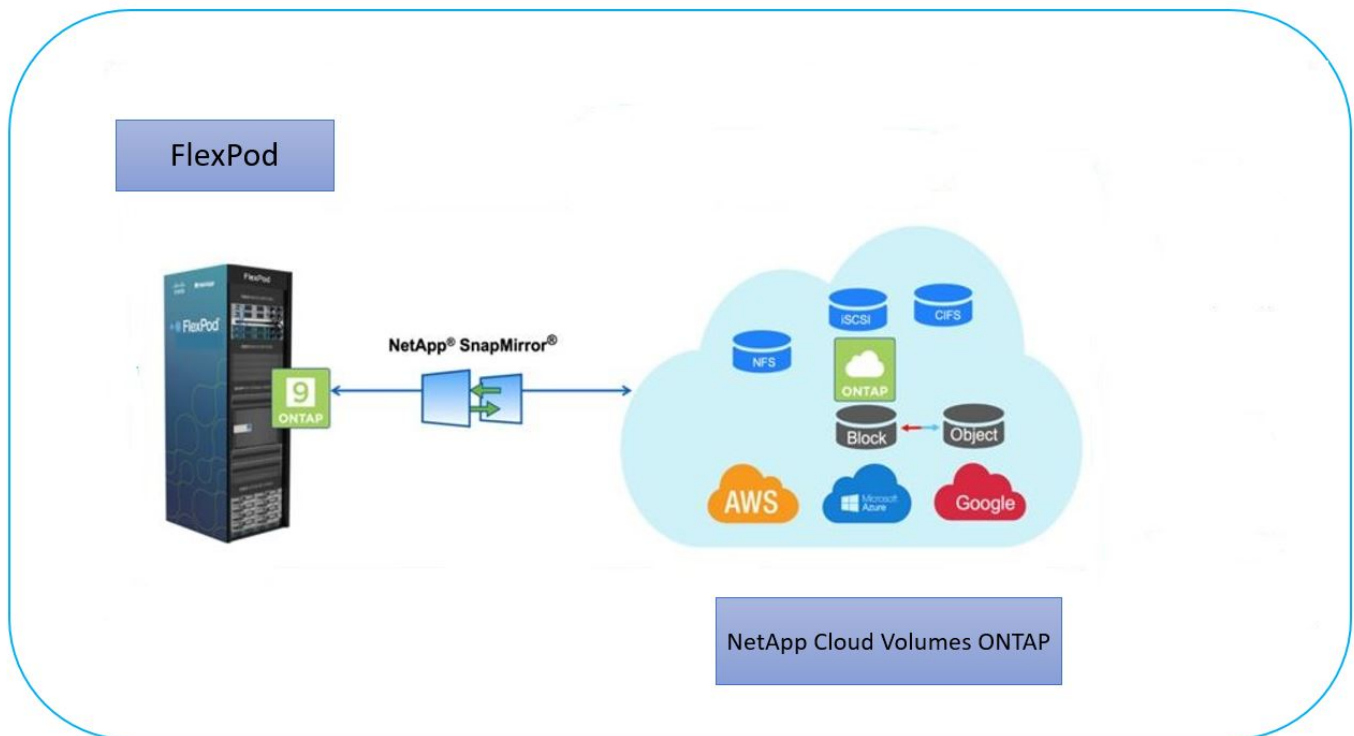
Durch die stetig wachsende Datenmenge im Gesundheitswesen und die wertvollen Einblicke, die diese Daten bieten, werden Datenservices und Datensicherung im Gesundheitswesen zu einer wichtigen und schwierigen Herausforderung. Erstens müssen Daten im Gesundheitswesen sowohl verfügbar als auch geschützt sein, um Datenwiederherstellungsanforderungen, medizinische Business Continuity oder Compliance-Anforderungen zu erfüllen.

Zweitens müssen Gesundheitsdaten zur Analyse bereitstehen. Häufig kommen bei dieser Analyse Ansätze auf der Basis von künstlicher Intelligenz (KI) und ml (Machine Learning) zum Einsatz, um medizinische Unternehmen bei der Verbesserung ihrer Lösungen und der Schaffung von geschäftlichen Werten zu unterstützen.

Drittens müssen die Datenserviceinfrastrukturen und die Datensicherungsmethoden das Wachstum der Gesundheitsdaten bewältigen, während das medizinische Unternehmen wächst. Darüber hinaus wird Datenmobilität immer wichtiger, da die Daten vom Edge dorthin verschoben werden müssen, wo sie erstellt werden, im Core-Bereich und in der Cloud, um die dort verfügbaren Ressourcen für Datenanalyse oder Archivierung zu nutzen.

NetApp bietet eine zentrale Datenmanagement-Lösung für Enterprise-Applikationen einschließlich Gesundheitswesen und wir können Krankenhäuser durch ihren Weg zur digitalen Transformation begleiten. NetApp Cloud Volumes ONTAP bietet eine Lösung für Datenmanagement im Gesundheitswesen, mit der Daten effizient von einem FlexPod Datacenter zu Cloud Volumes ONTAP repliziert werden können, die in einer Public Cloud wie AWS implementiert werden.

Cloud Volumes ONTAP nutzt kostengünstige und sichere Public Cloud-Ressourcen und verbessert die Cloud-basierte Disaster Recovery (DR) mit äußerst effizienter Datenreplikierung, integrierten Storage-Effizienzfunktionen und einfachen DR-Tests. Diese Systeme werden mit einheitlicher Steuerung und einfacher Drag-and-Drop-Funktion verwaltet, wodurch kosteneffektiver und absolut sicherer Schutz vor Fehlern, Ausfällen oder Notfällen gewährleistet wird. Cloud Volumes ONTAP bietet die NetApp SnapMirror Technologie als Lösung für die Datenreplikierung auf Block-Ebene, die das Ziel durch inkrementelle Updates auf dem neuesten Stand hält.



## Zielgruppe

Dieses Dokument richtet sich an Solution Engineers (SES) und Mitarbeiter von NetApp und Partner. NetApp geht davon aus, dass der Leser über folgende Hintergrundwissen verfügt:

- Ein solides Verständnis der SAN- und NAS-Konzepte
- Technische Vertrautheit mit NetApp ONTAP Storage-Systemen
- Technische Vertrautheit mit der Konfiguration und Administration der ONTAP Software

## Vorteile der Lösung

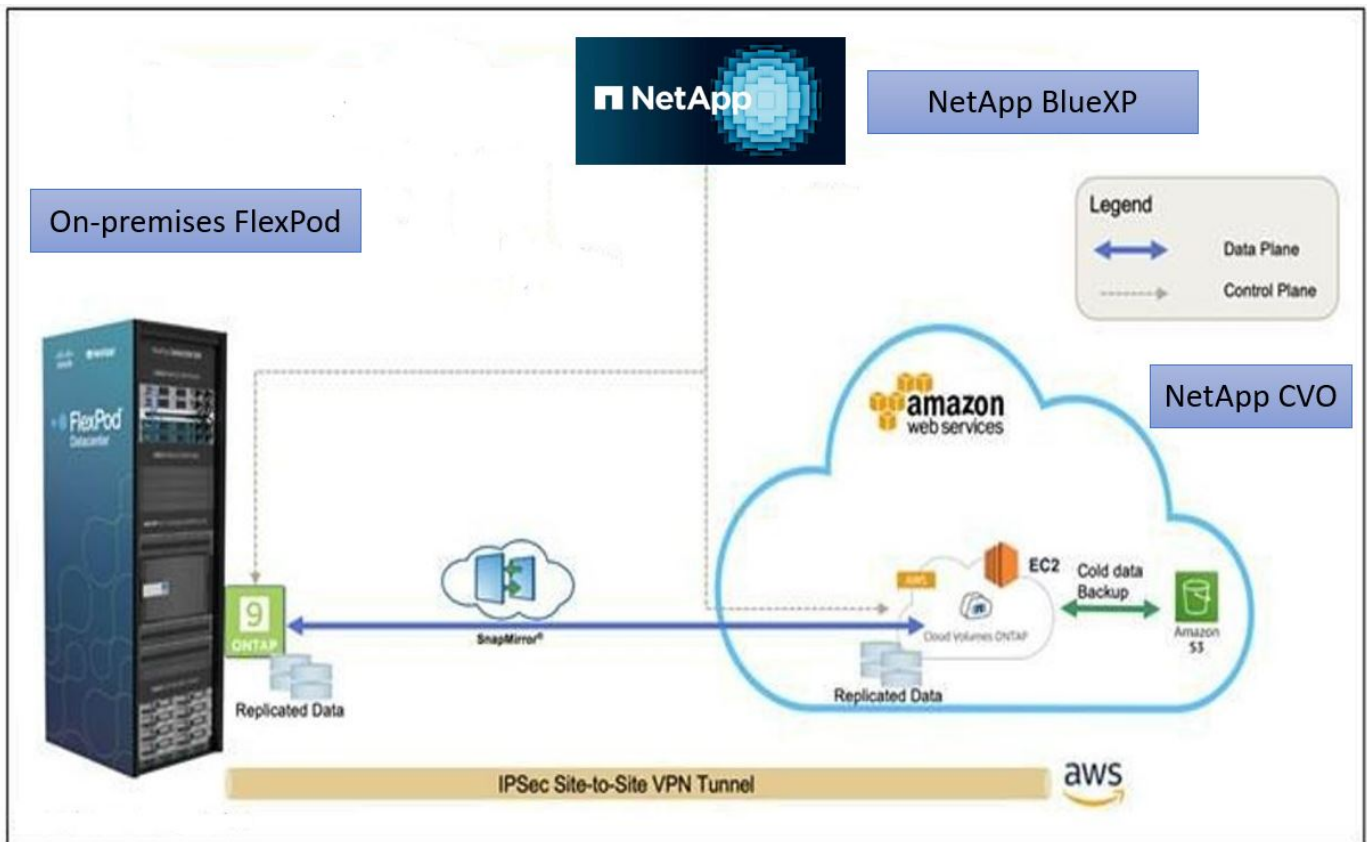
Eine Integration von FlexPod Datacenter mit NetApp Cloud Volumes ONTAP bietet folgende Vorteile für Workloads im Gesundheitswesen:

- **Customized Protection.** Cloud Volumes ONTAP bietet Datenreplikation auf Blockebene von ONTAP in die Cloud, sodass das Ziel durch inkrementelle Updates auf dem neuesten Stand bleibt. Benutzer können einen Synchronisierungszeitplan festlegen, der bestimmt, wann Änderungen an der Quelle übertragen werden. Damit bietet das System einen individuellen Schutz für alle Arten von Gesundheitsdaten.
- **Failover und Failback.** Wenn ein Notfall eintritt, können Storage-Administratoren schnell ein Failover auf die Cloud Volumes einrichten. Wenn der primäre Standort wiederhergestellt ist, werden die in der DR-Umgebung neu erstellten Daten zurück zu den Quell-Volumes synchronisiert. So kann die sekundäre Datenreplikierung wieder hergestellt werden. Auf diese Weise können Gesundheitsdaten problemlos und ohne Unterbrechung wiederhergestellt werden.
- **Effizienz.** der Speicherplatz und die Kosten für die sekundäre Cloud-Kopie werden durch Datenkomprimierung, Thin Provisioning und Deduplizierung optimiert. Gesundheitsdaten werden auf Blockebene komprimiert und dedupliziert übertragen, was die Übertragungsgeschwindigkeit erhöht. Darüber hinaus werden Daten automatisch auf kostengünstigen Objekt-Storage verschoben und lediglich bei Zugriffen auf hochperformanten Storage zurückgeführt, z. B. in einem DR-Szenario. So sinken die laufenden Storage-Kosten deutlich.

- **Ransomware-Schutz.** der Ransomware-Schutz von NetApp BlueXP scannt Datenquellen in On-Premises- und Cloud-Umgebungen, erkennt Sicherheitslücken und bietet ihren aktuellen Sicherheitsstatus sowie ihre Risikobewertung. Anschließend erhalten Sie umsetzbare Empfehlungen, die Sie weiter untersuchen und befolgen können, um Abhilfe zu schaffen. So können Sie Ihre kritischen Daten im Gesundheitswesen vor Ransomware-Angriffen schützen.

## Topologie der Lösung

In diesem Abschnitt wird die logische Topologie der Lösung beschrieben. Die folgende Abbildung zeigt die Lösungstopologie aus der On-Premises-Umgebung von FlexPod, der NetApp Cloud Volumes ONTAP (CVO) auf Amazon Web Services (AWS) und der NetApp BlueXP SaaS-Plattform.



Die Kontrollebenen und Datenebenen werden zwischen den Endpunkten klar angezeigt. Die Datenebene läuft über eine sichere Site-to-Site-VPN-Verbindung zwischen der ONTAP Instanz, die auf All-Flash FAS in FlexPod ausgeführt wird, und der NetApp CVO Instanz in AWS. Die Replizierung von Daten aus dem lokalen FlexPod Datacenter in die NetApp Cloud Volumes ONTAP erfolgt durch die NetApp SnapMirror Replizierung. Ein optionales Backup und Tiering von kalten Daten in der NetApp CVO-Instanz zu AWS S3 wird bei dieser Lösung ebenfalls unterstützt.

"Als Nächstes: Lösungskomponenten."

## Lösungskomponenten

"Zurück: Lösungsübersicht."

## FlexPod

FlexPod besteht aus vordefinierter Hardware und Software und bietet eine integrierte Grundlage für virtualisierte und nicht virtualisierte Lösungen. FlexPod umfasst NetApp ONTAP Storage, Cisco Nexus Netzwerkkomponenten, Cisco MDS Storage Netzwerke und das Cisco Unified Computing System (Cisco UCS).

Organisationen im Gesundheitswesen suchen nach einer Lösung, mit der sie ihren digitalen Wandel vereinfachen und die Patientenerfahrungen und -Ergebnisse verbessern können. Mit FlexPod erhalten Sie eine sichere, skalierbare Plattform, die die Effizienz steigert und Ihren Mitarbeitern ermöglicht, fundiertere Entscheidungen schneller zu treffen und somit die Patientenversorgung zu verbessern.

FlexPod ist die ideale Plattform für die Workload-Anforderungen im Gesundheitswesen, da sie folgende Vorteile bietet:

- Optimierung des Betriebs für schnellere Einblicke und bessere Behandlungsergebnisse
- Optimierung von Bildgebungsapplikationen mit einer skalierbaren, zuverlässigen Infrastruktur.
- Schnelle und effiziente Implementierung mit einem bewährten Ansatz für Applikationen im Gesundheitswesen, wie z. B. EHR.

## EHR

Electronic Health Records (EHRs) stellt Software für mittelgroße und große medizinische Gruppen, Krankenhäuser und integrierte Organisationen im Gesundheitswesen her. Zu den Kunden zählen auch kommunale Krankenhäuser, akademische Einrichtungen, Kinderorganisationen, Sicherheitsnetzbetreiber und Systeme mit mehreren Krankenhäusern. Die in die EHR integrierte Software umfasst klinische Funktionen sowie Zugriffs- und Umsatzfunktionen und kann auch zu Hause genutzt werden.

Unternehmen aus dem Gesundheitswesen stehen weiterhin unter dem Druck, den Nutzen aus ihren umfangreichen Investitionen in branchenführende EHRs zu maximieren. Wenn Kunden ihre Datacenter auf EHR-Lösungen und geschäftskritische Applikationen ausrichten, werden häufig die folgenden Ziele für die Datacenter-Architektur identifiziert:

- Hohe Verfügbarkeit der EHR-Anwendungen
- Hohe Performance
- Einfache Implementierung von EHR im Datacenter
- Agilität und Skalierbarkeit, um das Wachstum mit neuen EHR-Versionen oder -Applikationen zu ermöglichen
- Auch die Wirtschaftlichkeit kann sich sehen
- Managebarkeit, Stabilität und einfache Support-Bedienung
- Robuste Datensicherung, Backup, Recovery und Business Continuanace

FlexPod ist EHR-validiert und unterstützt eine Plattform mit Cisco UCS mit Intel Xeon Prozessoren, Red hat Enterprise Linux (RHEL) und Virtualisierung mit VMware ESXi. Diese Plattform kombiniert mit dem High Comfort Level Ranking von EHR für NetApp Storage mit ONTAP. Kunden können ihre Applikationen im Gesundheitswesen über FlexPod in einer vollständig gemanagten Private Cloud ausführen, die auch mit jedem der Public Cloud-Provider verbunden werden kann.

## NetApp BlueXP

BlueXP (ehemals NetApp Cloud Manager) ist eine SaaS-basierte Managementplattform der Enterprise-Klasse, mit der IT-Experten und Cloud-Architekten ihre Hybrid-Multi-Cloud-Infrastruktur mithilfe von NetApp Cloud-Lösungen zentral managen können. Es stellt ein zentrales System für die Anzeige und das Management von lokalem und Cloud-Storage bereit und unterstützt Hybrid- und Cloud-Umgebungen mit unterschiedlichen Cloud-Providern und Konten. Weitere Informationen finden Sie unter "[BlueXP](#)".

### Stecker

Mithilfe einer Connector-Instanz kann BlueXP Ressourcen und Prozesse in einer Public Cloud-Umgebung managen. Connector ist für viele der Funktionen von BlueXP erforderlich und kann in der Cloud oder im On-Premises-Netzwerk implementiert werden.

Der Anschluss wird an folgenden Orten unterstützt:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- On-Premises

Weitere Informationen zu Connector finden Sie im "[Anschlusseite](#)".

## NetApp Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP ist ein Software-Defined-Storage-Angebot, auf dem die ONTAP Datenmanagement-Software in der Cloud ausgeführt wird. Sie bietet fortschrittliches Datenmanagement für Datei- und Block-Workloads. Mit Cloud Volumes ONTAP können Sie Ihre Cloud Storage-Kosten optimieren, die Applikations-Performance steigern und gleichzeitig den Schutz, die Sicherheit und die Compliance verbessern.

Die wichtigsten Vorteile:

- **Storage-Effizienz** Nutzen Sie integrierte Datendeduplizierung, Datenkomprimierung, Thin Provisioning und sofortiges Klonen, um die Storage-Kosten zu minimieren.
- **Hohe Verfügbarkeit.** Zuverlässigkeit der Enterprise-Klasse und unterbrechungsfreier Betrieb bei Ausfällen in der Cloud-Umgebung.
- **Datensicherung** Cloud Volumes ONTAP nutzt SnapMirror, die branchenführende NetApp Replizierungstechnologie, um On-Premises-Daten in die Cloud zu replizieren. So ist es einfach, sekundäre Kopien für verschiedene Anwendungsfälle zur Verfügung zu haben. Cloud Volumes ONTAP lässt sich auch in Cloud Backup integrieren, um Backup- und Restore-Funktionen zum Schutz und zur langfristigen Archivierung Ihrer Cloud-Daten zu bieten.
- **Daten-Tiering.** Wechseln Sie nach Bedarf zwischen hoch- und Low-Performance-Speicherpools, ohne Anwendungen offline zu schalten.
- **Applikationskonsistenz.** sorgen für die Konsistenz der NetApp Snapshot Kopien mit NetApp SnapCenter Technologie.
- **Datensicherheit.** Cloud Volumes ONTAP unterstützt Datenverschlüsselung und bietet Schutz vor Viren und Ransomware.
- **Datenschutz-Compliance-Kontrollen.** die Integration mit Cloud Data Sense hilft Ihnen, Datenkontext zu verstehen und sensible Daten zu identifizieren.

Weitere Informationen finden Sie unter ["Cloud Volumes ONTAP"](#).

## NetApp Active IQ Unified Manager

Mit NetApp Active IQ Unified Manager können Sie Ihre ONTAP Storage-Cluster über eine zentrale, neu gestaltete und intuitive Benutzeroberfläche überwachen, die wertvolle Erkenntnisse aus Community-Wissen und KI-Analysen liefert. Es bietet umfassende betriebliche, performante und proaktive Einblicke in die Storage-Umgebung und die darauf ausgeführten Virtual Machines. Wenn bei der Storage-Infrastruktur ein Problem auftritt, informiert Sie Unified Manager über die Fehlerdetails, um die Ursache des Problems zu identifizieren. Das Dashboard der Virtual Machine bietet einen Überblick über die Performance-Statistiken der VM, sodass Sie den gesamten I/O-Pfad vom vSphere Host über das Netzwerk und schließlich den Storage ermitteln können.

Einige Ereignisse bieten auch Abhilfemaßnahmen, die zur Behebung des Problems ergriffen werden können. Sie können benutzerdefinierte Warnmeldungen für Ereignisse konfigurieren, sodass Sie bei Auftreten von Problemen über E-Mail und SNMP-Traps benachrichtigt werden. Mit Active IQ Unified Manager können Sie die Storage-Anforderungen Ihrer Anwender planen, indem Sie Kapazitäten und Nutzungstrends prognostizieren, um aktuelle Probleme zu vermeiden und so kurzfristige Entscheidungen zu vermeiden, die langfristig zu zusätzlichen Problemen führen können.

Weitere Informationen finden Sie unter ["Active IQ Unified Manager"](#).

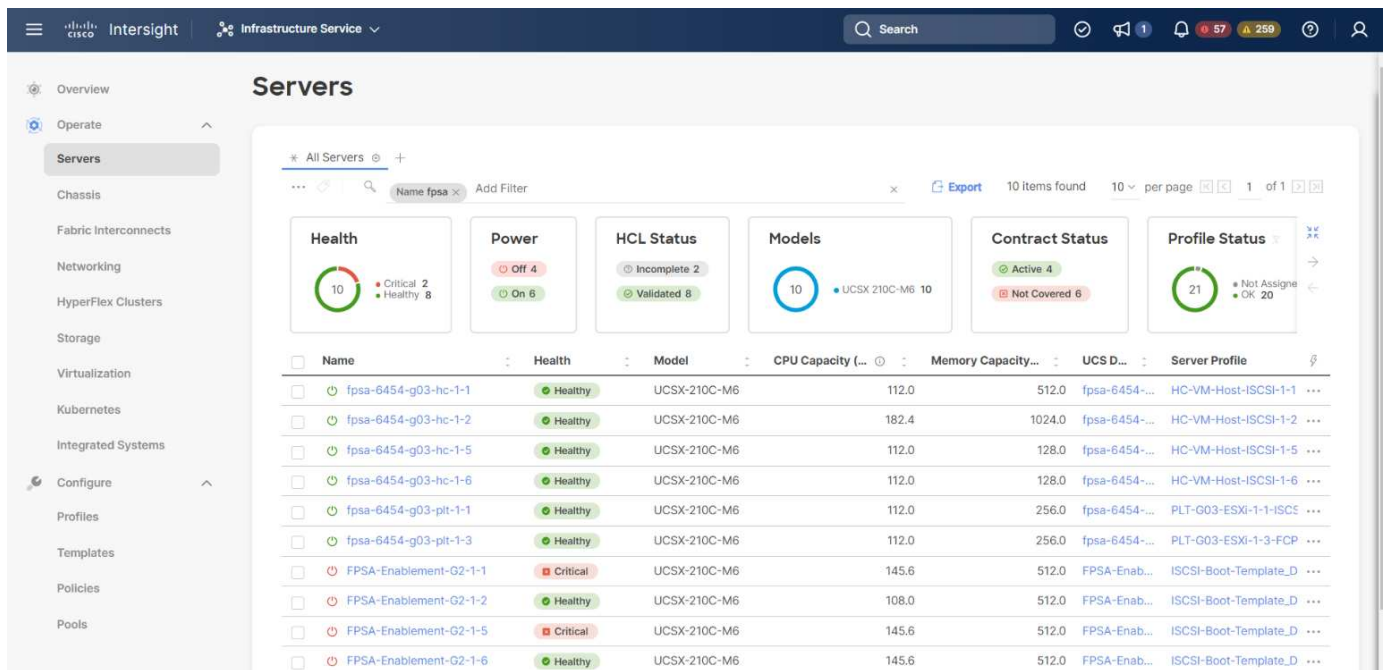
## Cisco Intersight

Cisco Intersight ist eine SaaS-Plattform, die intelligente Automatisierung, Beobachtbarkeit und Optimierung für herkömmliche und Cloud-native Applikationen und Infrastrukturen bietet. Die Plattform fördert den Wandel mit IT-Teams und bietet ein Betriebsmodell für Hybrid Clouds. Cisco Intersight bietet folgende Vorteile:

- **Schnellere Lieferung.** Intersight wird als Service aus der Cloud oder im Rechenzentrum des Kunden mit häufigen Updates und fortgesetzten Innovationen durch ein agiles Software-Entwicklungsmodell bereitgestellt. So kann sich der Kunde auf die Unterstützung wichtiger geschäftlicher Anforderungen konzentrieren.
- **Vereinfachter Betrieb.** Intersight vereinfacht den Betrieb durch die Verwendung eines einzigen, sicheren SaaS-bereitgestellten Tools mit gemeinsamer Inventarisierung, Authentifizierung und APIs für den gesamten Stack und an allen Standorten, sodass Silos in allen Teams vermieden werden. Damit können Sie physische Server und Hypervisoren vor Ort, auf VMs, K8s, serverlos, Automatisierung, Optimierung und Kostenkontrolle sowohl vor Ort als auch in Public Clouds.
- **Kontinuierliche Optimierung.** Sie können Ihre Umgebung kontinuierlich optimieren, indem Sie die Intelligenz von Cisco Intersight auf allen Ebenen sowie von Cisco TAC nutzen. Diese Informationen werden in empfohlene und automatisierte Aktionen umgewandelt, damit Sie sich in Echtzeit an Änderungen anpassen können: Vom Verschieben von Workloads und der Überwachung des Zustands physischer Server bis hin zu Empfehlungen zur Kostenreduzierung für die Public Clouds, mit denen Sie zusammenarbeiten.

Cisco Intersight ermöglicht zwei verschiedene Managementmodi: UCSM Managed Mode (UMM) und Intersight Managed Mode (IMM). Während des ersten Setups der Fabric Interconnects können Sie den nativen UCSM Managed Mode (UMM) oder Intersight Managed Mode (IMM) für Fabric-Attached Cisco UCS-Systeme auswählen. In dieser Lösung wird natives IMM verwendet. Die folgende Abbildung zeigt das Cisco Intersight Dashboard.





## VMware vSphere 7.0

VMware vSphere ist eine Virtualisierungsplattform, mit der sich große Mengen an Infrastrukturen (einschließlich CPUs, Storage und Netzwerke) als eine nahtlose, vielseitige und dynamische Betriebsumgebung verwalten lassen. Im Gegensatz zu herkömmlichen Betriebssystemen, die eine einzelne Maschine verwalten, aggregiert VMware vSphere die Infrastruktur eines gesamten Rechenzentrums zu einem einzigen Kraftpaket mit Ressourcen, die schnell und dynamisch jeder benötigten Anwendung zugewiesen werden können.

Weitere Informationen über VMware vSphere und seine Komponenten finden Sie unter ["VMware vSphere"](#).

## VMware vCenter Server

VMware vCenter Server ermöglicht einheitliches Management aller Hosts und VMs über eine einzige Konsole und aggregiert die Performance-Überwachung von Clustern, Hosts und VMs. VMware vCenter Server bietet Administratoren einen detaillierten Einblick in Status und Konfiguration von Computing-Clustern, Hosts, VMs, Storage, Gastbetriebssystem Und anderen geschäftskritischen Komponenten einer virtuellen Infrastruktur. VMware vCenter verwaltet die umfassenden Funktionen, die in einer VMware vSphere Umgebung verfügbar sind.

Ausführliche Informationen finden Sie unter ["VMware vCenter"](#).

## Hardware- und Software-Versionen

Diese Hybrid Cloud-Lösung kann auf jede FlexPod Umgebung erweitert werden, auf der unterstützte Versionen von Software, Firmware und Hardware ausgeführt werden, wie in definiert ["NetApp Interoperabilitäts-Matrix-Tool"](#), ["UCS Hardware- und Softwarekompatibilität"](#), und ["VMware Compatibility Guide"](#).

In der folgenden Tabelle sind die lokalen FlexPod Hardware- und Softwareversionen aufgeführt.

Komponente	Produkt	Version
Computing	Cisco UCS X210c M6	5.0(1b)
	Cisco UCS Fabric Interconnects 6454	4.2(2a)
Netzwerk	Cisco Nexus 9336C-FX2 NX-OS	9.3 (9)
Storage	NetApp AFF A400	ONTAP 9.11.1P2
	NetApp ONTAP Tools für VMware vSphere	9.11
	NetApp NFS Plug-in für VMware VAAI	2.0
	NetApp Active IQ Unified Manager	9.11P1
Software	VMware vSphere	7.0 (U3)
	VMware ESXi Nenic Ethernet-Treiber	1.0.35.0
	VMware vCenter Appliance	7.0.3
	Cisco Intersight Assist Virtual Appliance	1.0.9-342

In der folgenden Tabelle sind die Versionen von NetApp BlueXP und Cloud Volumes ONTAP aufgeführt.

Anbieter	Produkt	Version
NetApp	BlueXP	3.9.24
	Cloud Volumes ONTAP	ONTAP 9.11

["Weiter: Installation und Konfiguration."](#)

## Installation und Konfiguration

["Früher: Lösungskomponenten."](#)

### NetApp Cloud Volumes ONTAP Implementierung

Führen Sie die folgenden Schritte aus, um Ihre Cloud Volumes ONTAP-Instanz zu konfigurieren:

#### 1. Vorbereitung der Public-Cloud-Service-Provider-Umgebung

Für die Lösungskonfiguration müssen Sie die Umgebungsdetails Ihres Public Cloud-Service-Providers erfassen. Zur Vorbereitung der Amazon Web Services (AWS)-Umgebung benötigen Sie beispielsweise den AWS-Zugriffsschlüssel, den AWS-Geheimschlüssel und weitere Netzwerkdetails wie Region, VPC, Subnetz usw.

#### 2. Konfigurieren Sie das VPC-Endpunkt-Gateway.

Um die Verbindung zwischen der VPC und dem AWS S3-Service zu ermöglichen, ist ein VPC-Endpunkt-Gateway erforderlich. Damit wird die Sicherung auf CVO, einem Endpunkt mit dem Gateway-Typ, aktiviert.

### 3. Greifen Sie auf NetApp BlueXP zu.

Um auf NetApp BlueXP und andere Cloud-Services zugreifen zu können, müssen Sie sich anmelden "[NetApp BlueXP](#)". Zum Einrichten von Workspaces und Benutzern im BlueXP Konto klicken Sie auf "[Hier](#)". Sie benötigen ein Konto, das über die Berechtigung verfügt, den Connector bei Ihrem Cloud-Provider direkt von BlueXP zu implementieren. Sie können die BlueXP Richtlinie von herunterladen "[Hier](#)".

### 4. Connector Bereitstellen.

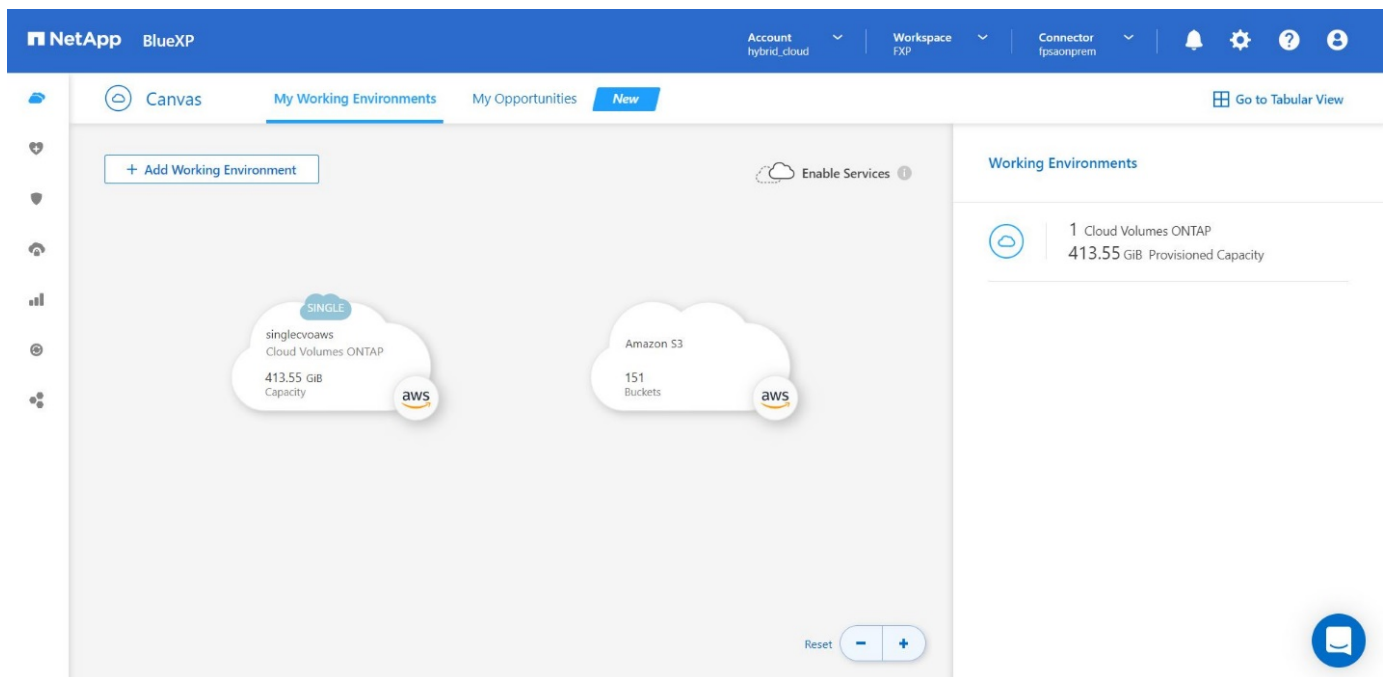
Bevor Sie eine Arbeitsumgebung von Cloud Volume ONTAP hinzufügen können, müssen Sie Connector bereitstellen. BlueXP fordert Sie auf, Ihre erste Cloud Volumes ONTAP Arbeitsumgebung ohne Connector zu erstellen. Wenn Sie Connector in AWS von BlueXP implementieren möchten, sehen Sie dies "[Verlinken](#)".

### 5. Starten Sie Cloud Volumes ONTAP in AWS.

Sie können Cloud Volumes ONTAP in einer Einzelsystemkonfiguration oder als HA-Paar in AWS starten. "[Lesen Sie die Schritt-für-Schritt-Anleitung](#)".

Ausführliche Informationen zu diesen Schritten finden Sie im "[Schnellstartanleitung für Cloud Volumes ONTAP in AWS](#)".

In dieser Lösung haben wir ein Cloud Volumes ONTAP System mit einem Node in AWS implementiert. Die folgende Abbildung zeigt das NetApp BlueXP Dashboard mit einer CVO-Instanz mit einem Node.



## Lokale FlexPod-Implementierung

Informationen über die Designdetails von FlexPod with UCS X-Series, VMware and NetApp ONTAP finden Sie im "[FlexPod Datacenter mit Cisco UCS X-Serie](#)" Designleitfaden. Dieses Dokument enthält Anleitungen zum Design, wie Sie die von Cisco Intersight gemanagte Plattform der UCS X-Serie in die FlexPod Datacenter-Infrastruktur integrieren können.

Informationen zur Bereitstellung der lokalen FlexPod-Instanz finden Sie unter "[Implementierungsleitfaden](#)".

Dieses Dokument enthält Anleitungen zur Implementierung, wie Sie die von Cisco Intersight gemanagte Plattform der UCS X-Serie in eine FlexPod Datacenter-Infrastruktur integrieren können. Das Dokument behandelt sowohl Konfigurationen als auch Best Practices für eine erfolgreiche Implementierung.

FlexPod kann sowohl im UCS Managed Mode als auch im Cisco Intersight Managed Mode (IMM) implementiert werden. Wenn Sie FlexPod im verwalteten UCS-Modus bereitstellen, finden Sie dies ["Designleitfaden"](#) Und das ["Implementierungsleitfaden"](#).

Die FlexPod-Implementierung kann mit „Infrastructure-as-Code“ über Ansible automatisiert werden. Nachfolgend finden Sie die Links zu GitHub Repositories für eine End-to-End FlexPod Implementierung:

- Ansible-Konfiguration von FlexPod mit Cisco UCS im UCS Managed Mode, NetApp ONTAP und VMware vSphere sind sichtbar ["Hier"](#).
- Ansible-Konfiguration von FlexPod mit Cisco UCS in IMM, NetApp ONTAP und VMware vSphere sind sichtbar ["Hier"](#).

## On-Premises-ONTAP Storage-Konfiguration

In diesem Abschnitt werden einige der wichtigen für diese Lösung spezifischen ONTAP Konfigurationsschritte beschrieben.

1. Konfigurieren Sie eine SVM, auf der der iSCSI-Dienst ausgeführt wird.

```
1. vservers create -vservers Healthcare_SVM -rootvolume
Healthcare_SVM_root -aggregate aggr1_A400_G0312_01 -rootvolume-security-
style unix
2. vservers add-protocols -vservers Healthcare_SVM -protocols iscsi
3. vservers iscsi create -vservers Healthcare_SVM
```

To verify:

```
A400-G0312::> vservers iscsi show -vservers Healthcare_SVM
Vserver: Healthcare_SVM
Target Name:
iqn.1992-08.com.netapp:sn.1fbf00f438c111ed866cd039ea91fb56:vs.3
Target Alias: Healthcare_SVM
Administrative Status: up
```

Wenn die iSCSI-Lizenz während der Clusterkonfiguration nicht installiert wurde, müssen Sie die Lizenz installieren, bevor Sie den iSCSI-Dienst erstellen.

2. Erstellen Sie ein FlexVol-Volume.

```
1. volume create -vservers Healthcare_SVM -volume hc_iscsi_vol -aggregate
aggr1_A400_G0312_01 -size 500GB -state online -policy default -space
guarantee none
```

3. Fügen Sie Schnittstellen für iSCSI-Zugriff hinzu.

```

1. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01a
   -service-policy default-data-iscsi -home-node <st-node01> -home-port
   a0a-<infra-iscsi-a-vlan-id> -address <st-node01-infra-iscsi-a-ip>
   -netmask <infra-iscsi-a-mask> -status-admin up
2. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01b
   -service-policy default-data-iscsi -home-node <st-node01> -home-port
   a0a-<infra-iscsi-b-vlan-id> -address <st-node01-infra-iscsi-b-ip>
   -netmask <infra-iscsi-b-mask> -status-admin up
3. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02a
   -service-policy default-data-iscsi -home-node <st-node02> -home-port
   a0a-<infra-iscsi-a-vlan-id> -address <st-node02-infra-iscsi-a-ip>
   -netmask <infra-iscsi-a-mask> -status-admin up
4. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02b
   -service-policy default-data-iscsi -home-node <st-node02> -home-port
   a0a-<infra-iscsi-b-vlan-id> -address <st-node02-infra-iscsi-b-ip>
   -netmask <infra-iscsi-b-mask> -status-admin up

```

In dieser Lösung haben wir vier iSCSI Logical Interfaces (LIFs) erstellt, zwei auf jedem Node.

Nachdem die FlexPod Instanz mit bereitgestelltem vCenter ausgeführt wurde und alle ESXi Hosts hinzugefügt wurden, müssen wir eine Linux VM implementieren, die als Server fungiert, der mit dem NetApp ONTAP Storage verbunden ist und auf diesen zugreift. In dieser Lösung haben wir eine CentOS 8-Instanz in vCenter installiert.

#### 4. Erstellen Sie eine LUN.

```

1. lun create -vserver Healthcare_SVM -path /vol/hc_iscsi_vol/iscsi_lun1
   -size 200GB -ostype linux -space-reserve disabled

```

Für eine ODB (EHR Operational Database), ein Journal und Applikations-Workloads empfiehlt EHR die Bereitstellung von Storage für Server als iSCSI-LUNs. NetApp unterstützt auch die Verwendung von FCP und NVMe/FC, wenn Sie Versionen von AIX und den RHEL Betriebssystemen verwenden können, wodurch die Performance verbessert wird. FCP und NVMe/FC können gleichzeitig im selben Fabric vorhanden sein.

#### 5. Erstellen einer Initiatorgruppe

```

1. igroup create -vserver Healthcare_SVM -igroup ehr -protocol iscsi
   -ostype linux -initiator iqn.1994-05.com.redhat:8e91e9769336

```

IGroups ermöglichen den Serverzugriff auf LUNs. Für Linux-Host kann der Server-IQN in der Datei gefunden werden `/etc/iscsi/initiatorname.iscsi`.

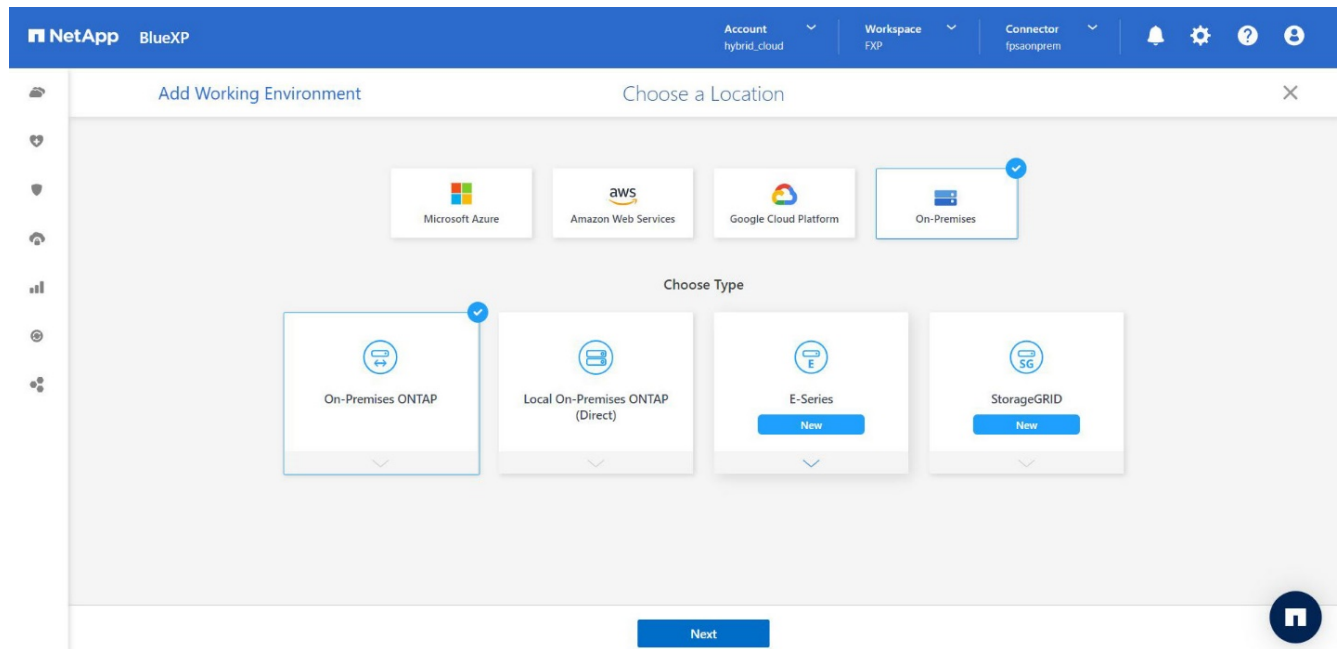
#### 6. Ordnen Sie die LUN der Initiatorgruppe zu.

```
1. lun mapping create -vserver Healthcare_SVM -path  
/vol/hc_iscsi_vol/iscsi_lun1 -igroup ehr -lun-id 0
```

## Fügen Sie lokalen FlexPod Storage zu BlueXP hinzu

Gehen Sie wie folgt vor, um Ihren FlexPod Storage mit NetApp BlueXP zur Arbeitsumgebung hinzuzufügen.

1. Wählen Sie im Navigationsmenü **Speicher > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und wählen Sie **On-Premises**.
3. Wählen Sie **On-Premise ONTAP**. Klicken Sie Auf **Weiter**.



4. Geben Sie auf der Seite ONTAP Cluster Details die Cluster-Management-IP-Adresse und das Kennwort für das Admin-Benutzerkonto ein. Klicken Sie dann auf **Hinzufügen**.

NetApp BlueXP

Account hybrid\_cloud Workspace FXP Connector fpxaonprem

Discover ONTAP Cluster ONTAP Cluster Details

Provide a few details about your ONTAP cluster so BlueXP can discover it.

Cluster Management IP Address

User Name  
admin

Password  
\*\*\*\*\*

Add

5. Geben Sie auf der Seite Details und Anmeldeinformationen einen Namen und eine Beschreibung für die Arbeitsumgebung ein, und klicken Sie dann auf **Go**.

BlueXP erkennt den ONTAP Cluster und fügt ihn als Arbeitsumgebung auf dem Canvas hinzu.

NetApp BlueXP

Account hybrid\_cloud Workspace FXP Connector fpxaonprem

Canvas My Working Environments My Opportunities New

+ Add Working Environment

Enable Services

Working Environments

- 1 Cloud Volumes ONTAP  
413.55 GiB Provisioned Capacity
- 1 On-Premises ONTAP  
2.98 TiB Provisioned Capacity

Ausführliche Informationen finden Sie auf der Seite ["Erkennen von ONTAP Clustern vor Ort"](#).

"Weiter: [SAN-Konfiguration](#)."

## SAN-Konfiguration

"Zurück: [Installation und Konfiguration](#)."

In diesem Abschnitt wird die Host-seitige Konfiguration beschrieben, die von EHR zur

optimalen Integration der Software in NetApp Storage erforderlich ist. In diesem Segment befassen wir uns insbesondere mit der Host-Integration für Linux-Betriebssysteme. Verwenden Sie die "[NetApp Interoperabilitäts-Matrix-Tool \(IMT\)](#)" Zur Validierung aller Versionen von Software und Firmware.



Die folgenden Konfigurationsschritte sind spezifisch für den CentOS 8-Host, der in dieser Lösung verwendet wurde.

## NetApp Host Utility Kit

NetApp empfiehlt die Installation des NetApp Host Utility Kit (Host Utilities) auf den Betriebssystemen der Hosts, die mit den NetApp Storage-Systemen verbunden sind und auf diese zugreifen. Native Microsoft Multipath-I/O (MPIO) wird unterstützt. Das Betriebssystem muss für Multipathing asymmetrisch (Asymmetric Logical Unit Access, ALUA) fähig sein. Durch das Installieren der Host Utilities werden die HBA-Einstellungen (Host Bus Adapter) für den NetApp Storage konfiguriert.

NetApp Host Utilities können heruntergeladen werden "[Hier](#)". In dieser Lösung haben wir Linux Host Utilities 7.1 auf dem Host installiert.

```
[root@hc-cloud-secure-1 ~]# rpm -ivh netapp_linux_unified_host_utilities-7-1.x86_64.rpm
```

## ONTAP Storage entdecken

Stellen Sie sicher, dass der iSCSI-Dienst ausgeführt wird, wenn die Anmeldungen erfolgen sollen. Um den Anmelde-Modus für ein bestimmtes Portal auf einem Ziel oder für alle Portale auf einem Ziel festzulegen, verwenden Sie die `iscsiadm` Befehl.

```
[root@hc-cloud-secure-1 ~]# rescan-scsi-bus.sh
[root@hc-cloud-secure-1 ~]# iscsiadm -m discovery -t sendtargets -p
<iscsi-lif-ip>
[root@hc-cloud-secure-1 ~]# iscsiadm -m node -L all
```

Jetzt können Sie verwenden `sanlun` Um Informationen über die mit dem Host verbundenen LUNs anzuzeigen. Stellen Sie sicher, dass Sie als root auf dem Host angemeldet sind.



```
[root@hc-cloud-secure-1 ~]# sanlun lun show
controller(7mode/E-Series)/
```

	device	host	lun
vserver(cDOT/FlashRay) lun-pathname filename adapter protocol size			
product			
-----			
Healthcare_SVM	/dev/sdb	host33	iSCSI 200g
cDOT	/vol/hc_iscsi_vol/iscsi_lun1		
Healthcare_SVM	/dev/sdc	host34	iSCSI 200g
cDOT	/vol/hc_iscsi_vol/iscsi_lun1		

## Konfigurieren Sie Multipathing

Device Mapper Multipathing (DM-Multipath) ist ein natives Multipathing-Dienstprogramm in Linux. Es kann für Redundanz und zur Verbesserung der Leistung verwendet werden. Die Software aggregiert oder kombiniert die zahlreichen I/O-Pfade zwischen Servern und Storage und erstellt somit ein einziges Gerät auf Betriebssystemebene.

1. Bevor Sie DM-Multipath auf Ihrem System einrichten, stellen Sie sicher, dass Ihr System aktualisiert wurde und den enthält `device-mapper-multipath` Paket.

```
[root@hc-cloud-secure-1 ~]# rpm -qa|grep multipath
device-mapper-multipath-libs-0.8.4-31.el8.x86_64
device-mapper-multipath-0.8.4-31.el8.x86_64
```

2. Die Konfigurationsdatei ist die `/etc/multipath.conf` Datei: Aktualisieren Sie die Konfigurationsdatei wie unten gezeigt.

```
[root@hc-cloud-secure-1 ~]# cat /etc/multipath.conf
defaults {
    path_checker      readsector0
    no_path_retry     fail
}
devices {
    device {
        vendor        "NETAPP  "
        product        "LUN.*"
        no_path_retry  queue
        path_checker    tur
    }
}
```

### 3. Aktivieren und starten Sie die Multipath-Services.

```
[root@hc-cloud-secure-1 ~]# systemctl enable multipathd.service
[root@hc-cloud-secure-1 ~]# systemctl start multipathd.service
```

### 4. Fügen Sie das ladbare Kernelmodul hinzu dm-multipath Und starten Sie den Multipath-Dienst neu. Überprüfen Sie abschließend den Multipathing-Status.

```
[root@hc-cloud-secure-1 ~]# modprobe -v dm-multipath
insmod /lib/modules/4.18.0-408.el8.x86_64/kernel/drivers/md/dm-
multipath.ko.xz

[root@hc-cloud-secure-1 ~]# systemctl restart multipathd.service

[root@hc-cloud-secure-1 ~]# multipath -ll
3600a09803831494c372b545a4d786278 dm-2 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
|+- policy='service-time 0' prio=50 status=active
|  `-- 33:0:0:0 sdb 8:16 active ready running
`+- policy='service-time 0' prio=10 status=enabled
  `-- 34:0:0:0 sdc 8:32 active ready running
```



Ausführliche Informationen zu diesen Schritten finden Sie unter ["Hier"](#).

## Erstellen eines physischen Volumes

Verwenden Sie die `pvcreeate` Befehl zum Initialisieren eines Blockgeräts, das als physisches Volume verwendet werden soll. Die Initialisierung ist analog zur Formatierung eines Dateisystems.

```
[root@hc-cloud-secure-1 ~]# pvcreate /dev/sdb
Physical volume "/dev/sdb" successfully created.
```

## Volume-Gruppe erstellen

Um eine Volume-Gruppe aus einem oder mehreren physischen Volumes zu erstellen, verwenden Sie die `vgcreate` Befehl. Mit diesem Befehl wird eine neue Volume-Gruppe nach Namen erstellt und ihr mindestens ein physisches Volume hinzugefügt.

```
[root@hc-cloud-secure-1 ~]# vgcreate datavg /dev/sdb
Volume group "datavg" successfully created.
```

Der `vgdisplay` Mit dem Befehl können die Eigenschaften der Volume-Gruppe (z. B. Größe, Extents, Anzahl physischer Volumes usw.) in einem festen Format angezeigt werden.

```
[root@hc-cloud-secure-1 ~]# vgdisplay datavg
--- Volume group ---
VG Name                datavg
System ID
Format                 lvm2
Metadata Areas         1
Metadata Sequence No   1
VG Access               read/write
VG Status               resizable
MAX LV                 0
Cur LV                 0
Open LV                 0
Max PV                 0
Cur PV                 1
Act PV                 1
VG Size                 <200.00 GiB
PE Size                 4.00 MiB
Total PE                51199
Alloc PE / Size         0 / 0
Free PE / Size          51199 / <200.00 GiB
VG UUID                 C7jmI0-J0SS-Cq91-t6b4-A9xw-nTfi-RXcy28
```

## Erstellung eines logischen Volumes

Wenn Sie ein logisches Volume erstellen, wird das logische Volume mithilfe der freien Extents auf den physischen Volumes, aus denen die Volume-Gruppe besteht, aus einer Volume-Gruppe erstellt.

```
[root@hc-cloud-secure-1 ~]# lvcreate -l 100%FREE -n datalv datavg
Logical volume "datalv" created.
```

Mit diesem Befehl wird ein logisches Volume mit dem Namen erstellt `datalv`. Dies belegt den gesamten nicht zugewiesenen Speicherplatz in der Volume-Gruppe `datavg`.

## Erstellen Sie ein Dateisystem

```
[root@hc-cloud-secure-1 ~]# mkfs.xfs -K /dev/datavg/datalv
meta-data=/dev/datavg/datalv      isize=512    agcount=4, agsize=13106944
blks
        =                        sectsz=4096   attr=2, projid32bit=1
        =                        crc=1          finobt=1, sparse=1, rmapbt=0
        =                        reflink=1      bigtime=0 inobtcount=0
data      =                        bsize=4096   blocks=52427776, imaxpct=25
        =                        sunit=0       swidth=0 blks
naming    =version 2              bsize=4096   ascii-ci=0, ftype=1
log        =internal log          bsize=4096   blocks=25599, version=2
        =                        sectsz=4096   sunit=1 blks, lazy-count=1
realtime   =none                  extsz=4096   blocks=0, rtextents=0
```

## Ordner zum Mounten erstellen

```
[root@hc-cloud-secure-1 ~]# mkdir /file1
```

## Mounten Sie das Dateisystem

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1
```

```
[root@hc-cloud-secure-1 ~]# df -k
```

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
devtmpfs	8072804	0	8072804	0%	/dev
tmpfs	8103272	0	8103272	0%	/dev/shm
tmpfs	8103272	9404	8093868	1%	/run
tmpfs	8103272	0	8103272	0%	/sys/fs/cgroup
/dev/mapper/cs-root	45496624	5642104	39854520	13%	/
/dev/sda2	1038336	258712	779624	25%	/boot
/dev/sda1	613184	7416	605768	2%	/boot/efi
tmpfs	1620652	12	1620640	1%	/run/user/42
tmpfs	1620652	0	1620652	0%	/run/user/0
/dev/mapper/datavg-datalv	209608708	1494520	208114188	1%	/file1

Ausführliche Informationen zu diesen Aufgaben finden Sie auf der Seite ["LVM-Administration mit CLI-Befehlen"](#).

## Datengenerierung

`Dgen.pl` Ist ein Perl-Skript-Datengenerator für EHR I/O-Simulator (GenerateIO). Daten innerhalb der LUNs werden mit der EHR erzeugt  
`Dgen.pl` Skript: Das Skript wurde entwickelt, um Daten zu erstellen, die den Daten in einer EHR-Datenbank ähneln.

```
[root@hc-cloud-secure-1 ~]# cd GenerateIO-1.17.3/

[root@hc-cloud-secure-1 GenerateIO-1.17.3]# ./dgen.pl --directory /file1
--jobs 80

[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37
dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38
dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39
dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40
dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80

[root@hc-cloud-secure-1 file1]# df -k .

```

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
/dev/mapper/datavg-datalv	209608708	178167156	31441552	85%	/file1

Während der Ausführung wird die angezeigt `Dgen.pl` Skript verwendet standardmäßig 85 % des Dateisystems für die Datengenerierung.

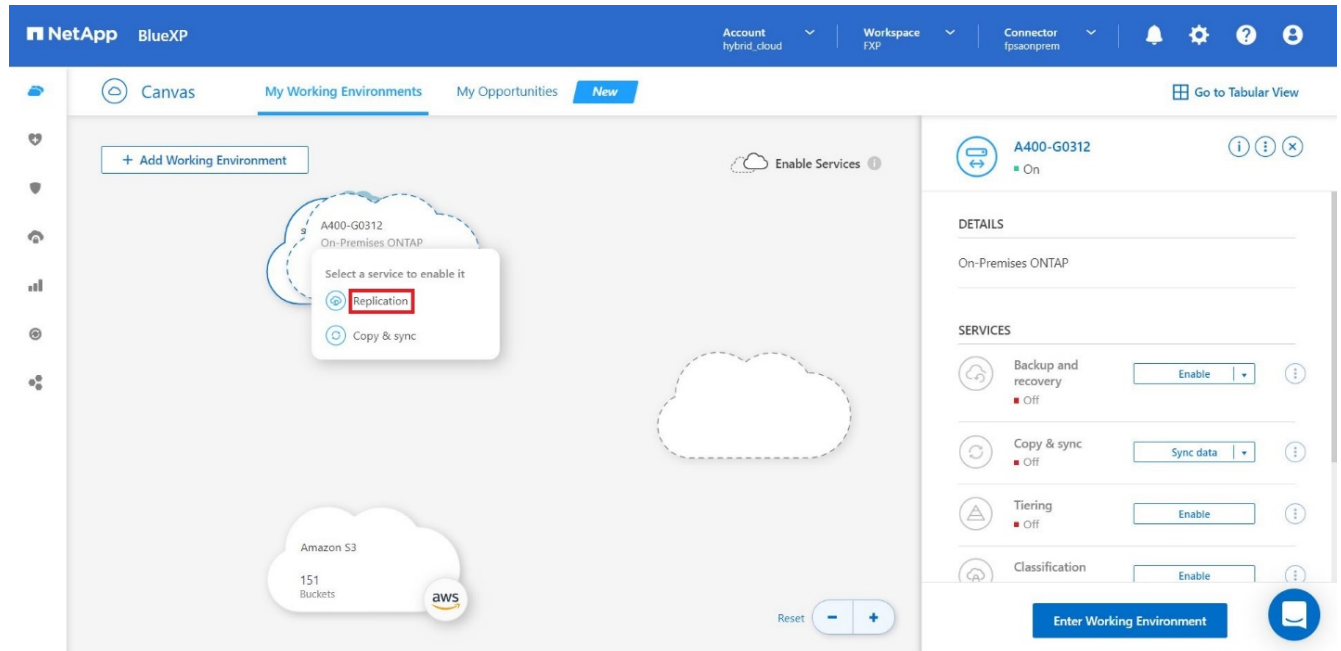
## Konfiguration der SnapMirror Replizierung zwischen lokalem ONTAP und Cloud Volumes ONTAP

NetApp SnapMirror repliziert Daten mit hohen Geschwindigkeiten über LAN oder WAN, so dass Sie in virtuellen und herkömmlichen Umgebungen hohe Datenverfügbarkeit und schnelle Datenreplizierung erhalten. Durch das Replizieren und ständige Aktualisieren der sekundären Daten auf NetApp Storage-Systemen sind die Daten immer aktuell und verfügbar. Es sind keine externen Replizierungsserver erforderlich.

Führen Sie die folgenden Schritte aus, um die SnapMirror Replizierung zwischen Ihrem lokalen ONTAP System und CVO zu konfigurieren.

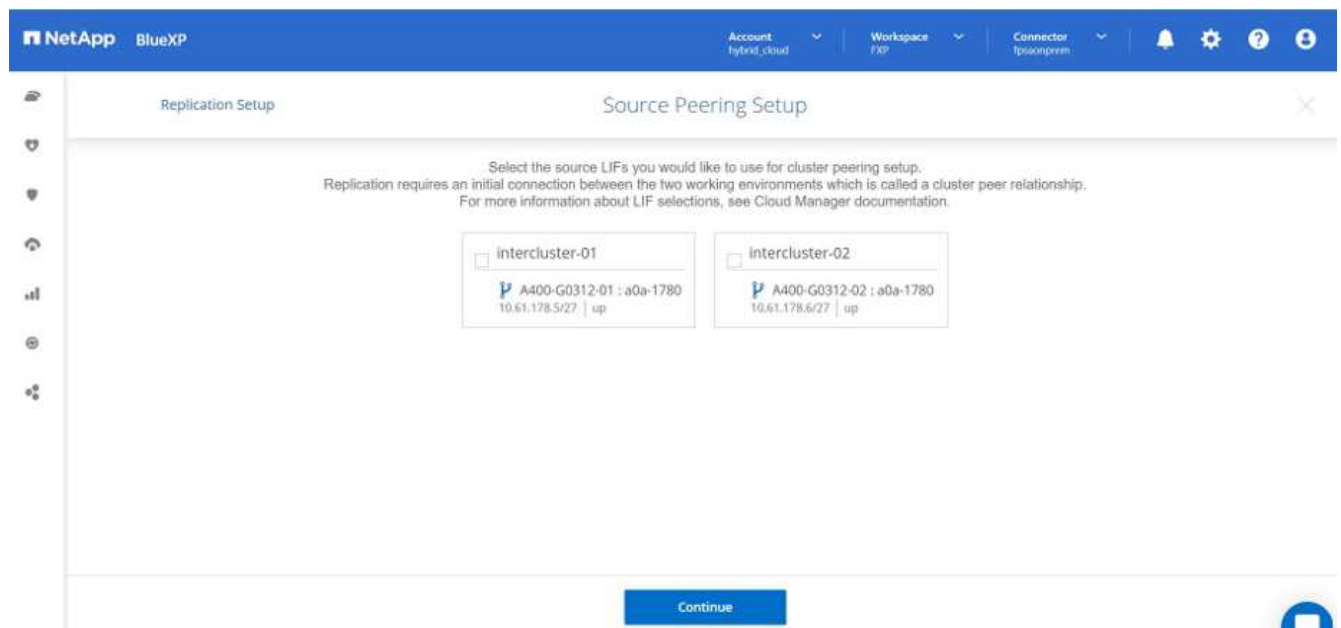
1. Wählen Sie im Navigationsmenü **Speicher > Leinwand**.

2. Wählen Sie in Canvas die Arbeitsumgebung aus, die das Quell-Volume enthält, ziehen Sie es in die Arbeitsumgebung, in die Sie das Volume replizieren möchten, und wählen Sie dann **Replikation** aus.

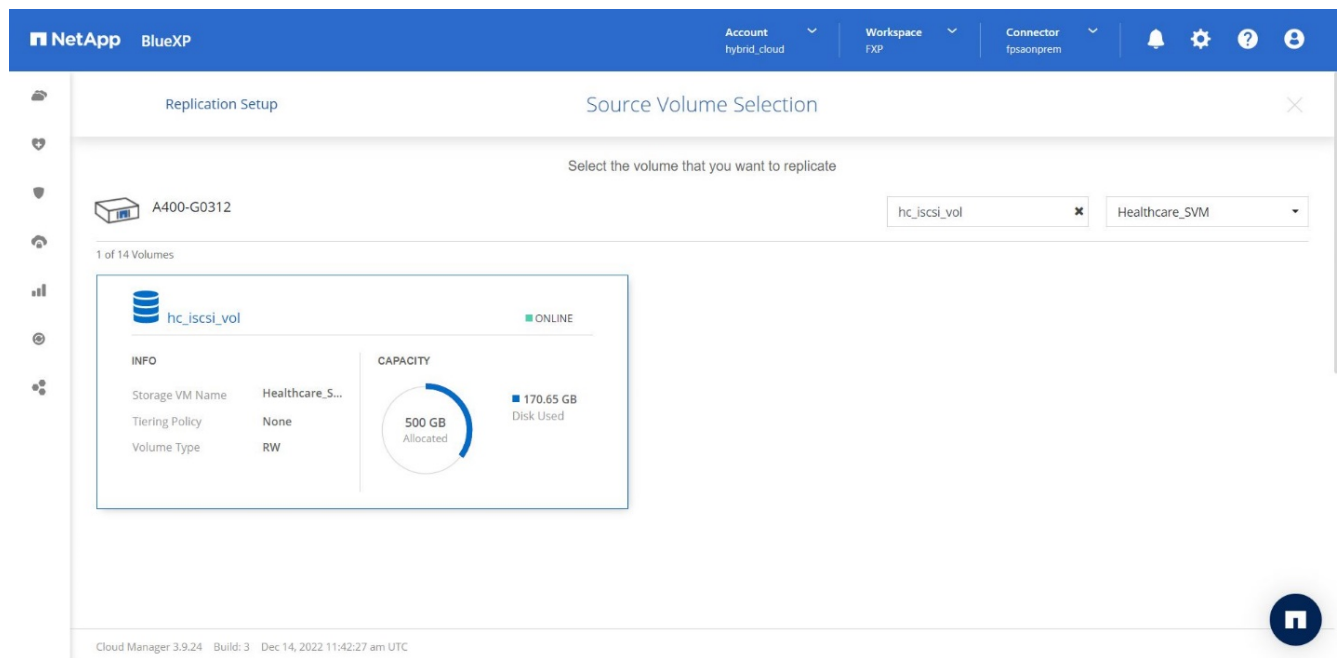


In den verbleibenden Schritten wird erläutert, wie eine synchrone Beziehung zwischen Cloud Volumes ONTAP und On-Premises-ONTAP-Clustern erstellt werden kann.

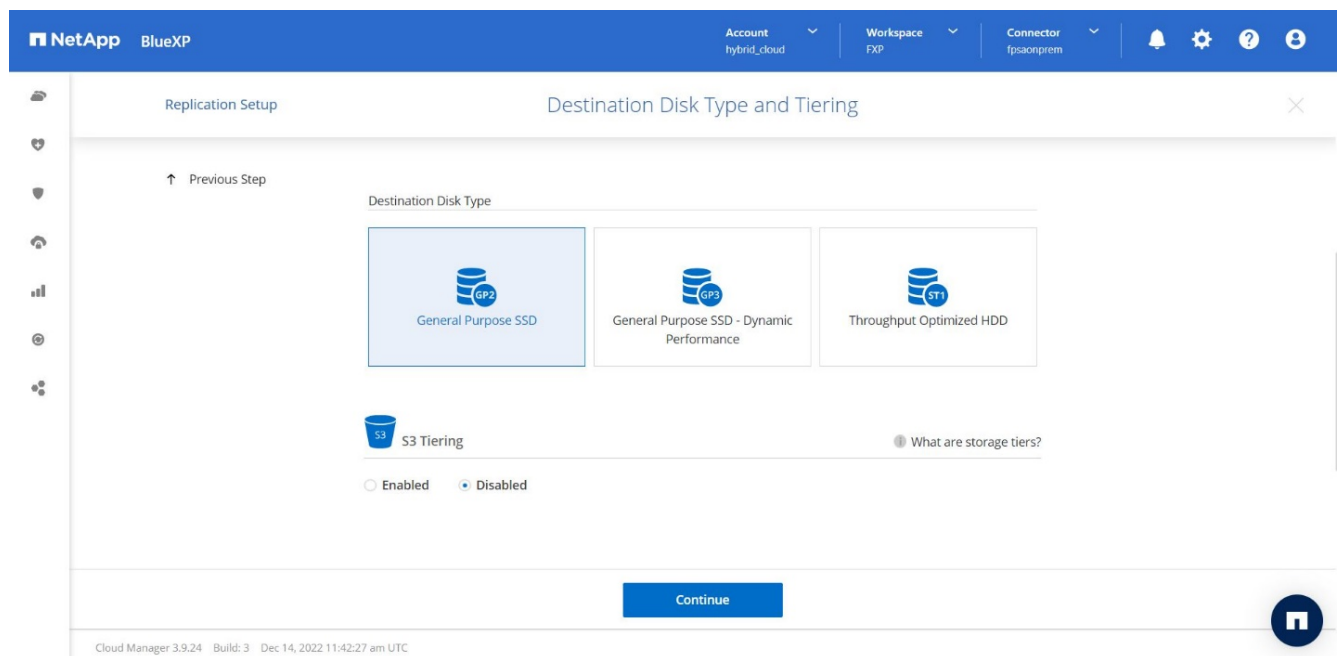
3. **Einrichtung von Quell- und Ziel-Peering.** Wenn diese Seite angezeigt wird, wählen Sie alle Cluster-LIFs für die Cluster-Peer-Beziehung aus.



4. **Auswahl des Quell-Volumes.** Wählen Sie das Volume aus, das Sie replizieren möchten.



5. **Zielfatentyp und Tiering.** Wenn es sich bei dem Ziel um ein Cloud Volumes ONTAP-System handelt, wählen Sie den Zielfatentyp aus und wählen, ob Sie Daten-Tiering aktivieren möchten.



6. **Zielfatenträger Name:** Geben Sie den Namen des Zielfatenträger an und wählen Sie das Zielaggregat. Wenn das Ziel ein ONTAP-Cluster ist, müssen Sie auch die Ziel-Storage-VM angeben.

Replication Setup

Destination Volume Name

↑ Previous Step

Destination Volume Name  
hc\_iscsi\_vol\_copy

Destination Aggregate  
Automatically select the best aggregate

Continue

Cloud Manager 3.9.24 Build: 3 Dec 14, 2022 11:42:27 am UTC

7. **Maximale Übertragungsrate.** Geben Sie die maximale Übertragungsrate (in Megabyte pro Sekunde) an.

Replication Setup

Max Transfer Rate

↑ Previous Step

You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your Internet performance.

☒ Limited to: 100 MB/s

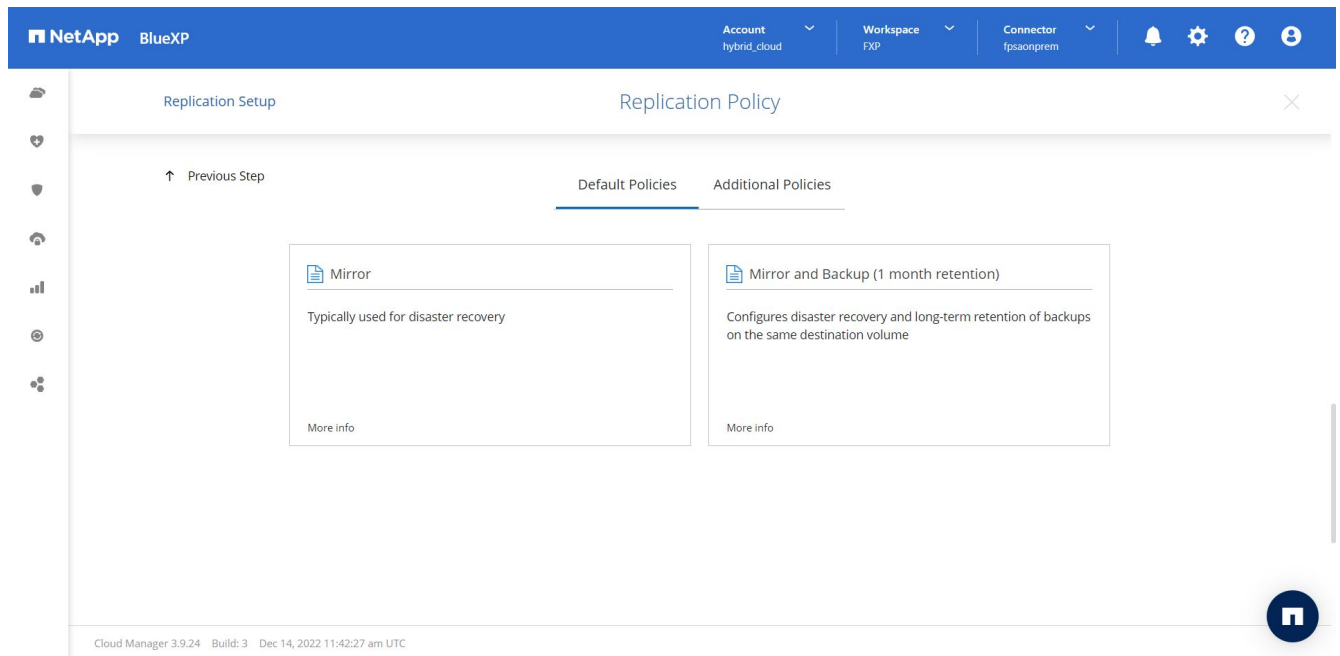
☐ Unlimited (recommended for DR only machines)

Continue

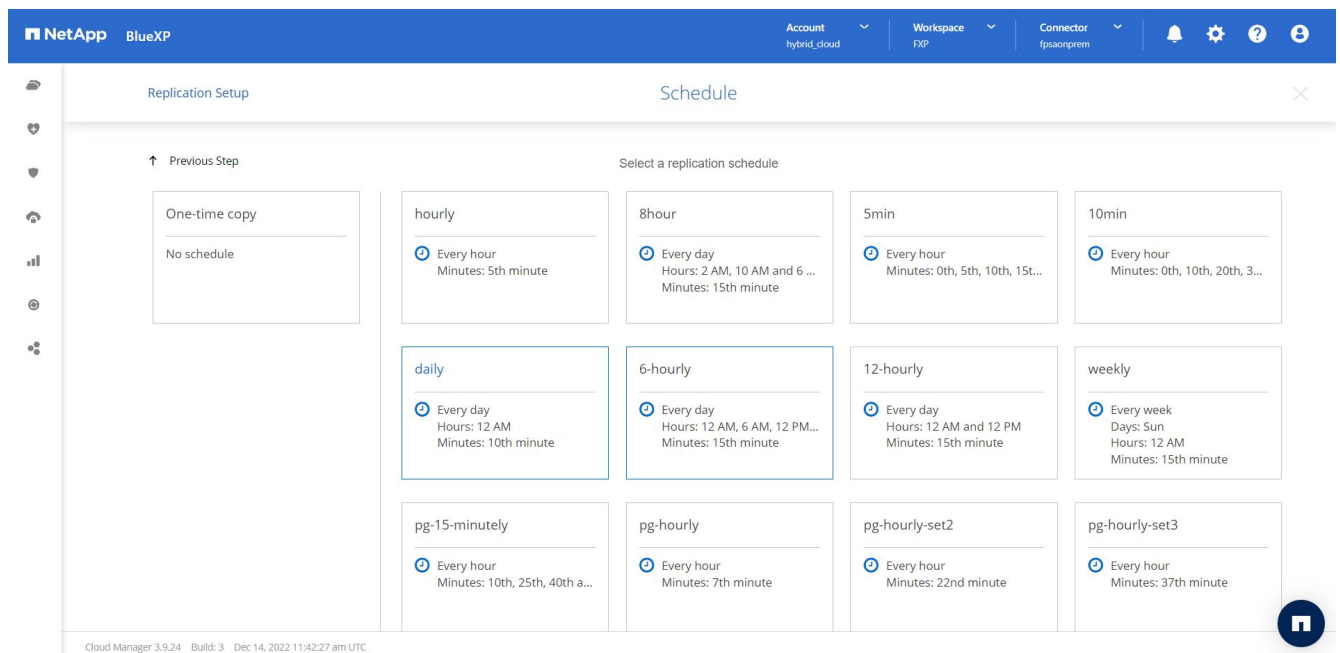
Cloud Manager 3.9.24 Build: 3 Dec 14, 2022 11:42:27 am UTC

8. **Replikationsrichtlinie.** Wählen Sie eine Standardrichtlinie oder klicken Sie auf **zusätzliche Richtlinien** und wählen Sie dann eine der erweiterten Richtlinien aus. Hilfe erhalten Sie unter: ["Weitere Informationen zu Replizierungsrichtlinien"](#).

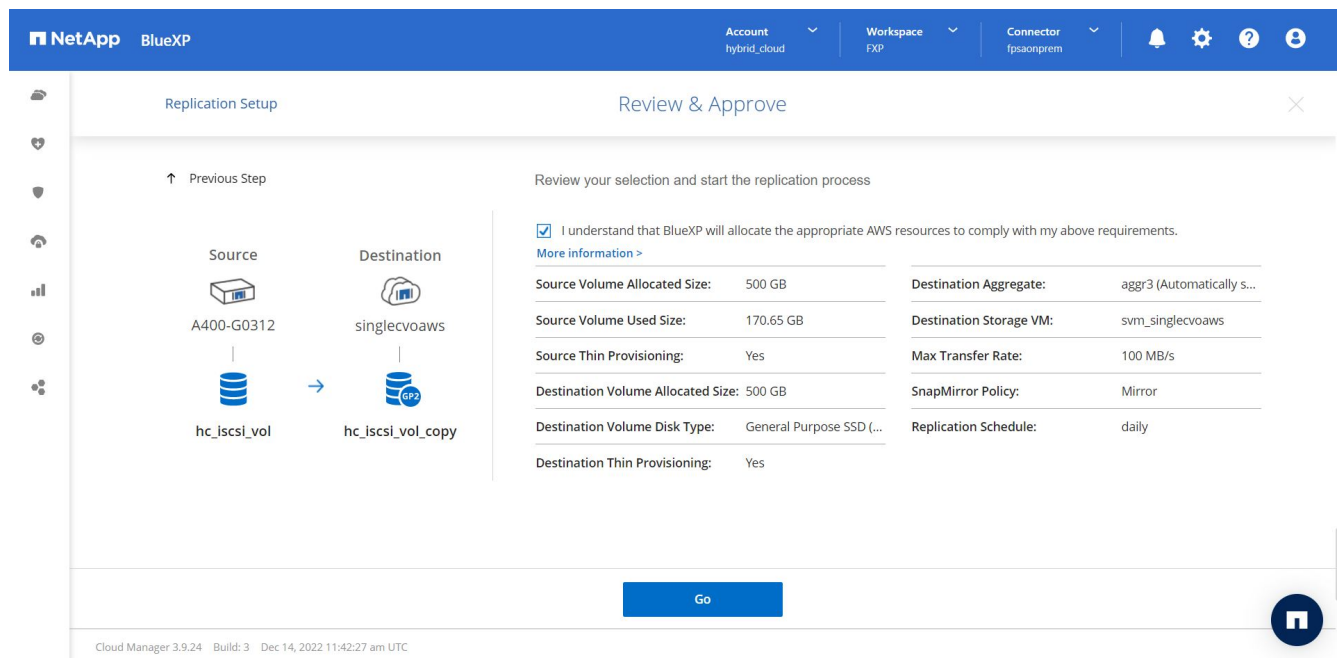




9. **Zeitplan.** Wählen Sie eine einmalige Kopie oder einen wiederkehrenden Zeitplan. Es stehen mehrere Standardzeitpläne zur Verfügung. Wenn Sie einen anderen Zeitplan benötigen, müssen Sie einen neuen Zeitplan auf der erstellen destination cluster Verwenden von System Manager.

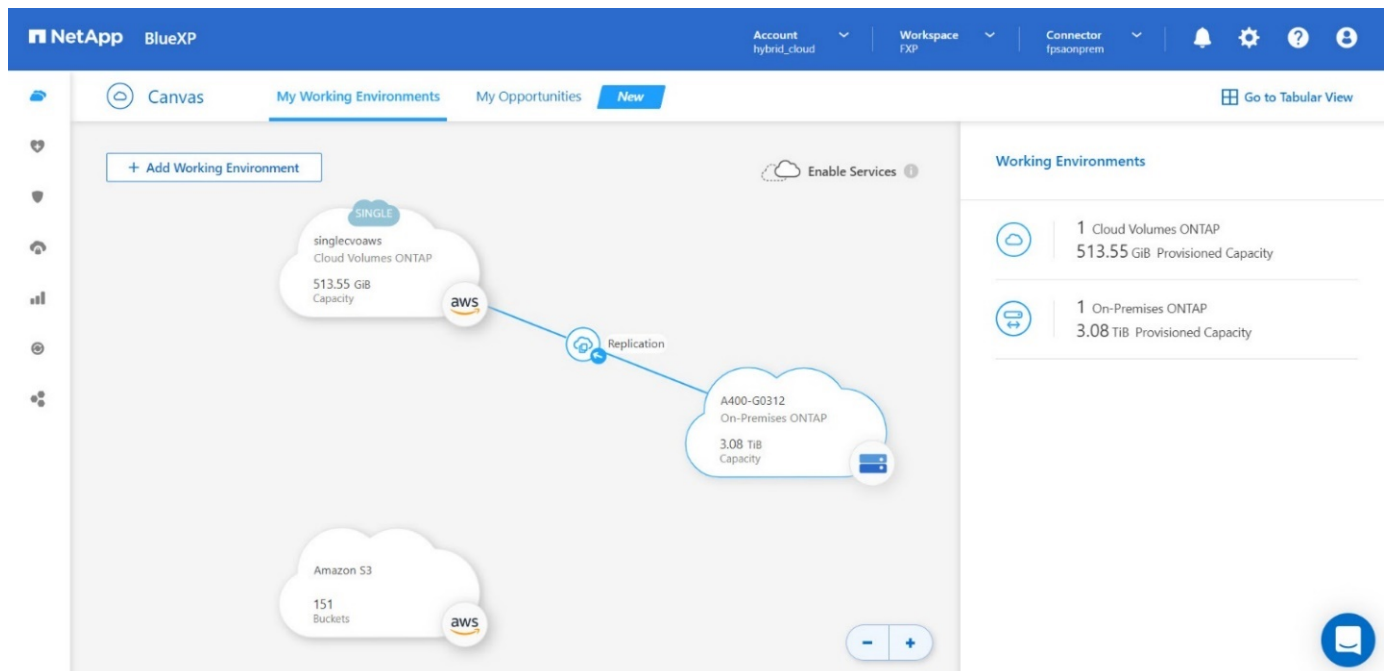


10. **Review.** Überprüfen Sie Ihre Auswahl und klicken Sie auf **Go**.



Ausführliche Informationen zu diesen Konfigurationsschritten finden Sie unter ["Hier"](#).

BlueXP startet den Datenreplizierungsprozess. Jetzt können Sie den Dienst **Replikation** sehen, der zwischen Ihrem lokalen ONTAP-System und Cloud Volumes ONTAP eingerichtet wurde.



Im Cloud Volumes ONTAP Cluster können Sie das neu erstellte Volume sehen.

NetApp BlueXP Account hybrid\_cloud Workspace FXP Connector fpsaonprem

singlecvoaws Switch to Advanced View AWS AWS Managed Encryption

Volumes Cost Replications

Volumes hc\_iscsi Add Volume

★ New version available Upgrade now

1 of 21 Volumes | 500 GB Allocated | 170.02 GB Total Used (511.70 GB in EBS, 0 KB in S3)

hc\_iscsi\_vol\_copy ONLINE

INFO

Disk Type	GP2
Tiering Policy	None
Backup	OFF

CAPACITY

500 GB Allocated

170.02 GB EBS Used

Sie können auch überprüfen, ob die SnapMirror Beziehung zwischen dem lokalen Volume und dem Cloud Volume aufgebaut ist.

NetApp BlueXP Account hybrid\_cloud Workspace FXP Connector fpsaonprem

singlecvoaws Switch to Advanced View AWS AWS Managed Encryption

Volumes Cost Replications

1 Volume Relationships 170.26 GB Replicated Capacity 0 Currently Transferring 1 Healthy 0 Failed

Search 1 relationship Refresh Add / Remove columns

Source	Target	Lag Duration	Relationship Health	Status	Mirror State	Last Successful Transfer	Policy	Schedule
hc_iscsi_vol A400-G0312	hc_iscsi_vol_copy singlecvoaws	An hour	Healthy	idle	snapmirrored	Dec 21, 2022 05:05:00 ... 0 Byte	Mirror	daily

Cloud Manager 3.9.24 Build: 3 Dec 14, 2022 11:42:27 am UTC

Weitere Informationen zur Replikationsaufgabe finden Sie auf der Registerkarte **Replikation**.

The screenshot shows the NetApp BlueXP Replication interface. At the top, there's a navigation bar with 'NetApp BlueXP' and various account/workspace/connector dropdowns. The main content area is titled 'Replication' and displays three components: 'hc\_iscsi\_vol (A400-G0312)' as the Source Volume, 'hc\_iscsi\_vol\_copy (singlecvoaws)' as the Target Volume, and a 'Healthy' Replication Health status. Below this, there are three sections: 'Transfer Info', 'Last Transfer Info', and 'Volume Info'. The 'Transfer Info' section contains a table with details like Status, Type, Total Size, Lag Duration, Priority, Max Transfer Rate, Total Transfer Time, Mirror State, Used Size / Used on Cloud, and Network Compression Ratio. The 'Last Transfer Info' section shows the last successful transfer date, size, duration, and type. The 'Volume Info' section lists source and destination availability zones and SVM names.

Transfer Info				
idle	N/A	101.48 GiB	6 hours 19 minutes 24 secon...	N/A
Status	Type	Total Size	Lag Duration	Priority
100 MiB/s	34 minutes 9 seconds	snapirored	170.01 GiB / 0 B	1:1
Max Transfer Rate	Total Transfer Time	Mirror State	Used Size / Used on Cloud	Network Compression Ratio

Last Transfer Info			
Jan 19, 2023, 5:40:04 AM	25.63 KiB	2 seconds	update
Last Successful	Size	Duration	Type

Volume Info			
Source Availability Zone	Healthcare_SVM	us-east-1a	svm_singlecvoaws
	Source SVM Name	Destination Availability Zone	Destination SVM Name

"Weiter: Lösungsvalidierung."

## Lösungsvalidierung

"Zurück: SAN-Konfiguration."

In diesem Abschnitt werden einige Anwendungsfälle für Lösungen vorgestellt.

- Ein primärer Anwendungsfall für SnapMirror ist das Daten-Backup. SnapMirror kann als primäres Backup Tool genutzt werden, indem Daten innerhalb desselben Clusters oder zu Remote-Zielen repliziert werden.
- Verwendung der DR-Umgebung für Applikationsentwicklung (Entwicklung/Test)
- DR im Falle eines Disasters in der Produktion.
- Datenverteilung und Remote-Datenzugriff:

Bemerkenswert ist, dass die in dieser Lösung validierten relativ wenigen Anwendungsfälle nicht die gesamte Funktionalität der SnapMirror Replizierung darstellen.

## Applikationsentwicklung und -Tests (Entw./Test)

Zur Beschleunigung der Applikationsentwicklung können replizierte Daten am DR-Standort geklont und zum entwickeln und Testen von Applikationen genutzt werden. Durch das Zusammenführen von DR- und Entwicklungs-/Testumgebungen lässt sich die Auslastung von Backup- oder DR-Einrichtungen immens verbessern. Zudem stehen durch Klone für Test und Entwicklung so viele Datenkopien wie nötig zur Verfügung, um die Produktion zu beschleunigen.

Mit der NetApp FlexClone Technologie kann schnell eine Lese-/Schreibkopie eines SnapMirror Ziel-FlexVol-Volumes erstellt werden, falls Sie einen Lese-/Schreibzugriff auf die sekundäre Kopie haben möchten, um zu bestätigen, ob alle Produktionsdaten verfügbar sind.

Gehen Sie wie folgt vor, um die DR-Umgebung für die Entwicklung/den Test von Applikationen zu nutzen:

1. Erstellen einer Kopie der Produktionsdaten Führen Sie dazu einen Anwendungs-Snapshot eines On-

Premises-Volumes aus. Das Erstellen eines Applikations-Snapshots besteht aus drei Schritten: Lock, Snap, und Unlock.

- a. Legen Sie das Filesystem still, damit der I/O ausgesetzt wird und die Anwendungen konsistent bleiben. Alle Anwendungen, die auf das Dateisystem schreiben, bleiben in einem Wartezustand, bis der Befehl zum unstilllegen in Schritt c ausgegeben wird. Die Schritte a, b und c werden über einen transparenten Prozess oder einen transparenten Workflow ausgeführt, der die SLA für Applikationen nicht beeinträchtigt.

```
[root@hc-cloud-secure-1 ~]# fsfreeze -f /file1
```

Diese Option fordert das angegebene Dateisystem auf, von neuen Änderungen eingefroren zu werden. Jeder Prozess, der versucht, in das eingefrorene Dateisystem zu schreiben, wird blockiert, bis das Dateisystem nicht eingefroren ist.

- b. Erstellen Sie einen Snapshot des On-Premises-Volumes.

```
A400-G0312::> snapshot create -vserver Healthcare_SVM -volume  
hc_iscsi_vol -snapshot kamini
```

- c. Heben Sie die Stilllegung des Dateisystems auf, um I/O neu zu starten

```
[root@hc-cloud-secure-1 ~]# fsfreeze -u /file1
```

Diese Option wird verwendet, um das Dateisystem aufzufrieren und den Betrieb fortzusetzen. Alle Dateisystemänderungen, die durch das Einfrieren blockiert wurden, werden entsperrt und können abgeschlossen werden.

Applikationskonsistente Snapshots können darüber hinaus mithilfe von NetApp SnapCenter erstellt werden, mit der der oben beschriebene Workflow im Rahmen von SnapCenter vollständig orchestriert wird. Ausführliche Informationen finden Sie unter ["Hier"](#).

2. Führen Sie einen SnapMirror Update-Vorgang durch, um die Produktions- und DR-Systeme synchron zu halten.

```
singlecvoaws::> snapmirror update -destination-path  
svm_singlecvoaws:hc_iscsi_vol_copy -source-path  
Healthcare_SVM:hc_iscsi_vol  
  
Operation is queued: snapmirror update of destination  
"svm_singlecvoaws:hc_iscsi_vol_copy".
```

Ein SnapMirror Update kann auch über die BlueXP GUI unter der Registerkarte **Replication** durchgeführt werden.

3. Erstellen Sie auf Basis des bereits zuvor erstellten Applikations-Snapshots eine FlexClone Instanz.

```
singlecvoaws::> volume clone create -flexclone kamini_clone -type RW
-parent-vserver svm_singlecvoaws -parent-volume hc_iscsi_vol_copy
-junction-active true -foreground true -parent-snapshot kamini
```

```
[Job 996] Job succeeded: Successful
```

Für die vorherige Aufgabe kann auch ein neuer Snapshot erstellt werden, Sie müssen jedoch die gleichen Schritte wie oben ausführen, um die Anwendungskonsistenz zu gewährleisten.

4. Aktivieren Sie ein FlexClone Volume, um die EHR-Instanz in der Cloud zu erstellen.

```
singlecvoaws::> lun mapping create -vserver svm_singlecvoaws -path
/vol/kamini_clone/iscsi_lun1 -igroup ehr-igroup -lun-id 0
```

```
singlecvoaws::> lun mapping show
```

Vserver	Path	Igroup	LUN ID	Protocol
svm_singlecvoaws	/vol/kamini_clone/iscsi_lun1	ehr-igroup	0	iscsi

5. Führen Sie die folgenden Befehle für die EHR-Instanz in der Cloud aus, um auf die Daten oder das Dateisystem zuzugreifen.
  - a. ONTAP Storage entdecken. Überprüfen Sie den Multipathing-Status.

```

sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show

```

Output:

```

controller(7mode/E-Series)/          device      host          lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
-----
-----

```

```

svm_singlecvoaws                      /dev/sda  host2      iSCSI      200g
cDOT

```

```

/vol/kamini_clone/iscsi_lun1

```

```

sudo multipath -ll

```

Output:

```

3600a09806631755a452b543041313053 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running

```

b. Aktivieren Sie die Volume-Gruppe.

```

sudo vgchange -ay datavg

```

Output:

```

1 logical volume(s) in volume group "datavg" now active

```

c. Mounten Sie das Dateisystem und zeigen Sie die Zusammenfassung der Dateisysteminformationen an.

```

sudo mount -t xfs /dev/datavg/datalv /file1

```

```

cd /file1

```

```

df -k .

```

Output:

```

Filesystem              1K-blocks  Used    Available  Use%
Mounted on
/dev/mapper/datavg-datalv 209608708 183987096 25621612   88%
/file1

```

So wird überprüft, ob Sie die DR-Umgebung für Entwicklung und Tests von Applikationen verwenden können. Mithilfe der Entwicklungs- und Testverfahren für Applikationen auf Ihrem DR-Storage nutzen

Sie Ressourcen besser, die andernfalls möglicherweise die meiste Zeit ungenutzt bleiben.

## Disaster Recovery

SnapMirror Technologie wird auch als Teil von DR-Plänen eingesetzt. Wenn kritische Daten an einen anderen physischen Standort repliziert werden, muss ein schwerwiegender Ausfall nicht zu längeren Datenperioden für geschäftskritische Applikationen führen. Clients können bis zur Wiederherstellung des Produktionsstandorts vor Beschädigung, versehentlichem Löschen, Naturkatastrophen usw. über das Netzwerk auf replizierte Daten zugreifen.

Im Falle eines Failback zum primären Standort bietet SnapMirror eine effiziente Möglichkeit, den DR-Standort am primären Standort neu zu synchronisieren. Dabei werden nur geänderte oder neue Daten vom DR-Standort aus zurück zum primären Standort übertragen, indem die SnapMirror Beziehung einfach umgekehrt wird. Nachdem der primäre Produktionsstandort den normalen Applikationsbetrieb wiederaufgenommen hat, setzt SnapMirror die Übertragung zum DR-Standort fort, ohne dass ein weiterer Basistransfer erforderlich ist.

Gehen Sie wie folgt vor, um ein erfolgreiches DR-Szenario zu validieren:

1. Simulieren Sie einen Notfall auf der Quell- (Produktions-) Seite, indem Sie die SVM, die das lokale ONTAP Volume hostet, anhalten (`hc_iscsi_vol`).

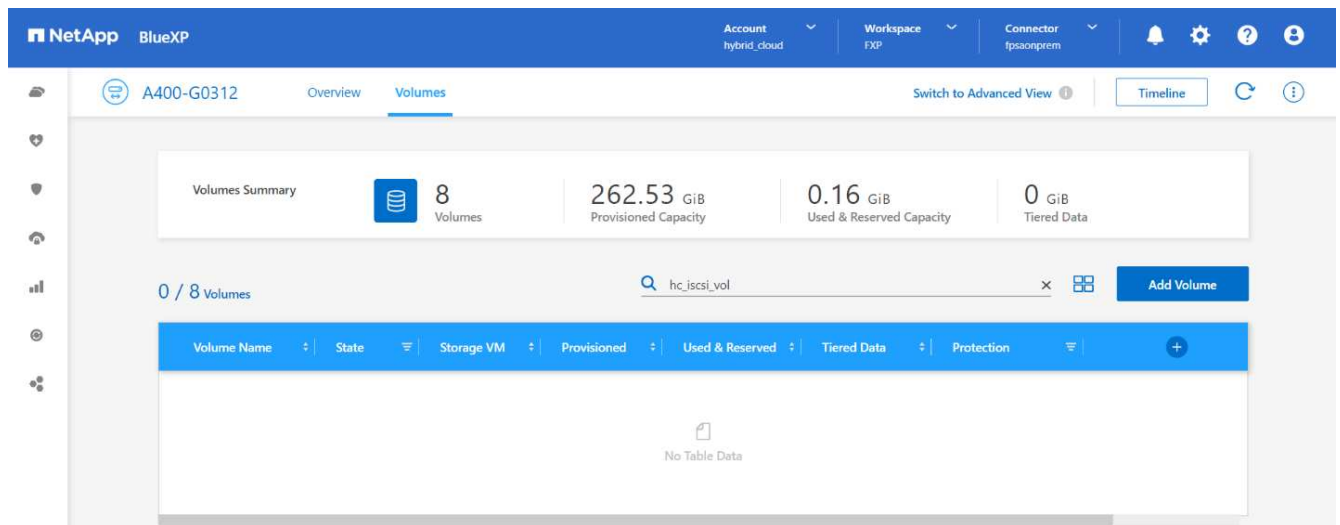
The screenshot shows the ONTAP System Manager interface. The left sidebar contains navigation links: DASHBOARD, INSIGHTS, STORAGE (expanded), Overview, Volumes, LUNs, Consistency Groups, Shares, Buckets, Qtrees, Quotas, Storage VMs (selected), Tiers, NETWORK, EVENTS & JOBS, PROTECTION, HOSTS, and CLUSTER. The main panel displays the 'Storage VMs' table with columns: Name, State, Subtype, Configured Protocols, IPspace, and Protection. Three rows are listed: CL\_CIFS\_SVM, CL\_SVM, and Healthcare\_SVM. The Healthcare\_SVM row is selected, and a context menu is open over it, showing options: Edit, Delete, Stop (highlighted with a red box), Trace File Access, and Login Banner Message. The bottom status bar indicates 'Showing 1 - 3 of 3 Storage VMs'.

Name	State	Subtype	Configured Protocols	IPspace	Protection
CL_CIFS_SVM	running	default	SMB/CIFS	Default	Shield icon
CL_SVM	running	default	NFS, iSCSI, FC	Default	Shield icon
Healthcare_SVM	running	default	NFS, iSCSI	Default	Shield icon

Vergewissern Sie sich, dass die SnapMirror Replizierung bereits zwischen der On-Premises-ONTAP in der FlexPod-Instanz und Cloud Volumes ONTAP in AWS eingerichtet ist, sodass Sie häufige Applikations-Snapshots erstellen können.

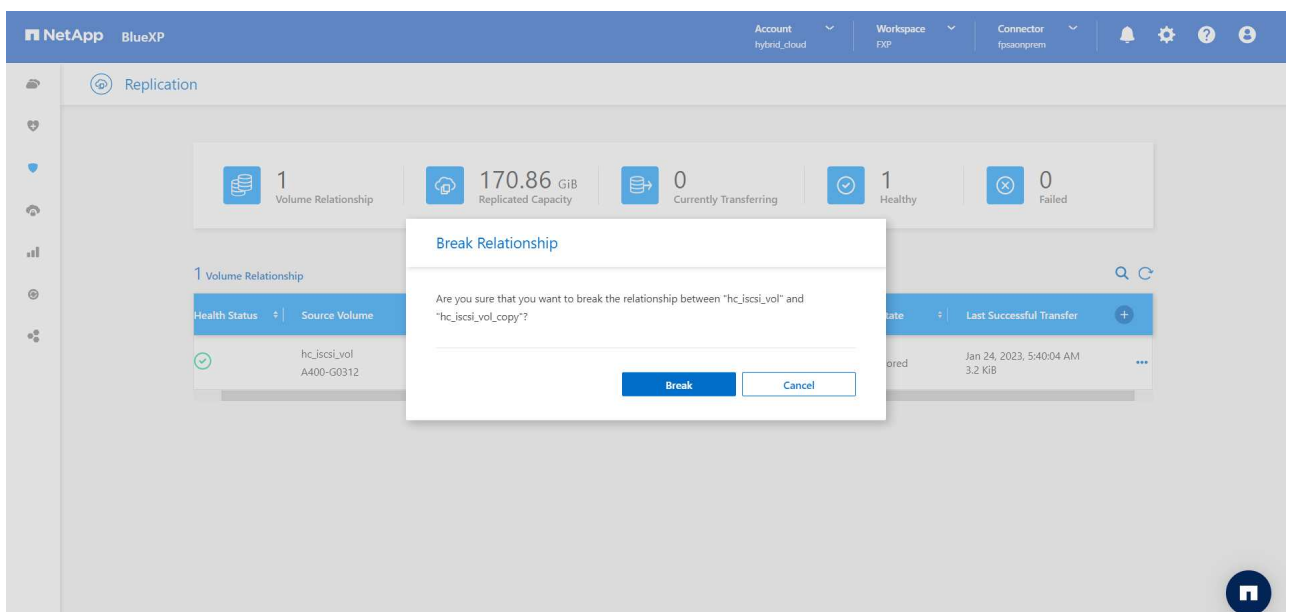
Nachdem die SVM angehalten wurde, führt der `hc_iscsi_vol` Volume ist in BlueXP nicht sichtbar.





## 2. DR in CVO aktivieren.

- a. Die SnapMirror Replizierungsbeziehung zwischen On-Premises-ONTAP und Cloud Volumes ONTAP wird unterbrochen, und das CVO-Zielvolume wird heraufgestuft (hc\_iscsi\_vol\_copy) Bis zur Produktion.



Nachdem die SnapMirror Beziehung beschädigt wurde, ändert sich der Typ des Ziel-Volume von Datensicherung (DP) in Lesen/Schreiben (RW).

```
singlecvoaws::> volume show -volume hc_iscsi_vol_copy -fields typev
server          volume          type
-----
svm_singlecvoaws hc_iscsi_vol_copy RW
```

- b. Aktivieren Sie das Ziel-Volume in Cloud Volumes ONTAP, um die EHR-Instanz auf einer EC2-Instanz in der Cloud zu öffnen.

```
singlecvoaws::> lun mapping create -vserver svm_singlecvoaws -path
/vol/hc_iscsi_vol_copy/iscsi_lun1 -igroup ehr-igroup -lun-id 0

singlecvoaws::> lun mapping show
Vserver      Path                                          Igroup    LUN ID
Protocol
-----
svm_singlecvoaws
          /vol/hc_iscsi_vol_copy/iscsi_lun1  ehr-igroup  0      iscsi
```

- c. Um auf die Daten und das Dateisystem auf der EHR-Instanz in der Cloud zuzugreifen, ermitteln Sie zuerst den ONTAP-Speicher und überprüfen Sie den Multipathing-Status.

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show
Output:
controller(7mode/E-Series)/          device    host          lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
-----
svm_singlecvoaws                      /dev/sda  host2        iSCSI        200g
cDOT
          /vol/hc_iscsi_vol_copy/iscsi_lun1
sudo multipath -ll
Output:
3600a09806631755a452b543041313051 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

- d. Aktivieren Sie dann die Volume-Gruppe.

```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

- e. Schließlich mounten Sie das Dateisystem und zeigen die Dateisysteminformationen an.

```

sudo mount -t xfs /dev/datavg/datalv /file1

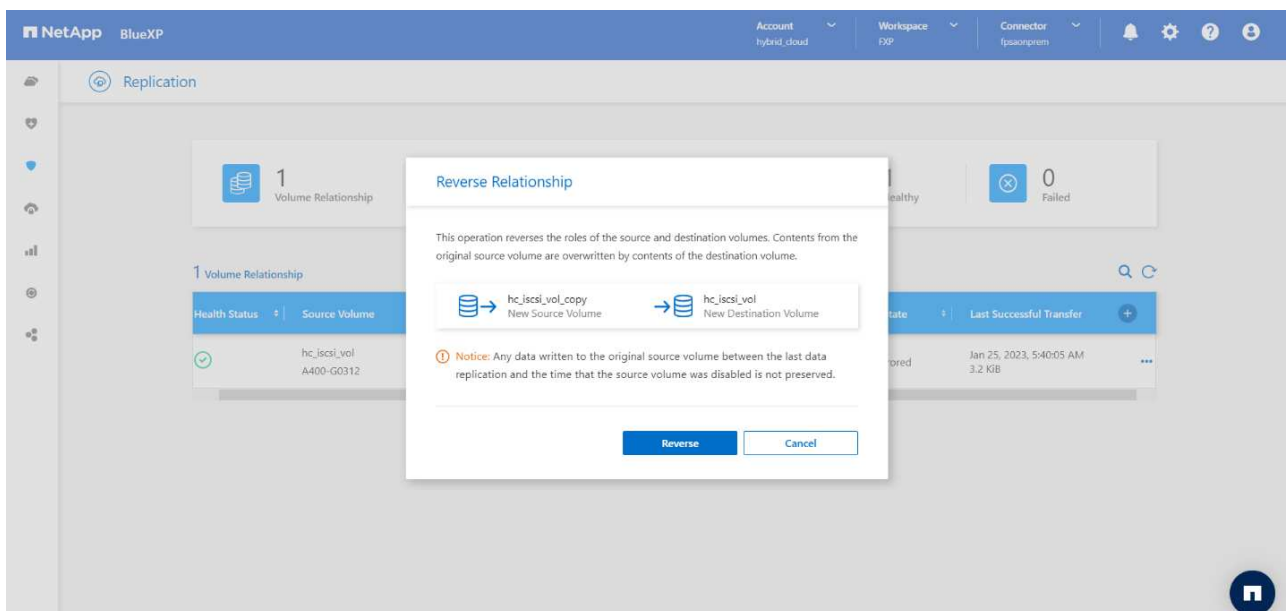
cd /file1
df -k .
Output:

```

Filesystem	1K-blocks	Used	Available	Use%
Mounted on				
/dev/mapper/datavg-datalv	209608708	183987096	25621612	88%
/file1				

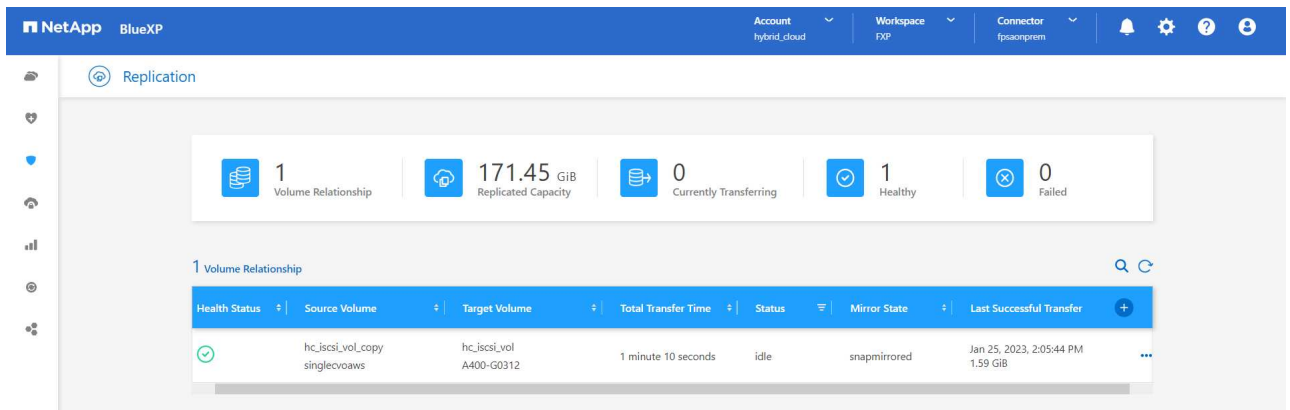
Diese Ausgabe zeigt, dass Benutzer auf replizierte Daten im gesamten Netzwerk zugreifen können, bis die Recovery des Produktionsstandorts nach einem Ausfall erfolgt.

- f. Rückgängig machen der SnapMirror Beziehung Dieser Vorgang kehrt die Rollen der Quell- und Ziel-Volumes um.



Bei diesem Vorgang werden die Inhalte des ursprünglichen Quell-Volume durch den Inhalt des Ziel-Volume überschrieben. Dies ist hilfreich, wenn Sie ein Quell-Volume, das offline gegangen ist, reaktivieren möchten.

Jetzt das CVO Volumen (`hc_iscsi_vol_copy`) Wird zum Quell-Volume und zum On-Premises-Volume (`hc_iscsi_vol`) Wird zum Zielvolume.



Alle Daten, die zwischen der letzten Datenreplizierung und dem Zeitpunkt, zu dem das Quell-Volume deaktiviert wurde, auf das ursprüngliche Quell-Volume geschrieben wurden, bleiben nicht erhalten.

- Erstellen Sie eine neue Datei auf der EHR-Instanz in der Cloud, um den Schreibzugriff auf das CVO-Volume zu überprüfen.

```
cd /file1/
sudo touch newfile
```

Wenn der Produktionsstandort ausfällt, können Clients weiterhin auf die Daten zugreifen und auch Schreibvorgänge auf das Cloud Volumes ONTAP Volume ausführen, das jetzt das Quell-Volume ist.

Im Falle eines Failback zum primären Standort bietet SnapMirror eine effiziente Möglichkeit, den DR-Standort am primären Standort neu zu synchronisieren. Dabei werden nur geänderte oder neue Daten vom DR-Standort aus zurück zum primären Standort übertragen, indem die SnapMirror Beziehung einfach umgekehrt wird. Nachdem der primäre Produktionsstandort den normalen Applikationsbetrieb wiederaufgenommen hat, setzt SnapMirror die Übertragung zum DR-Standort fort, ohne dass ein weiterer Basistransfer erforderlich ist.

Dieser Abschnitt veranschaulicht die erfolgreiche Lösung eines DR-Szenarios, wenn der Produktionsstandort durch einen Notfall betroffen ist. Daten können jetzt sicher von Applikationen genutzt werden, die jetzt die Clients bedienen können, während der Quellstandort die Wiederherstellung durchläuft.

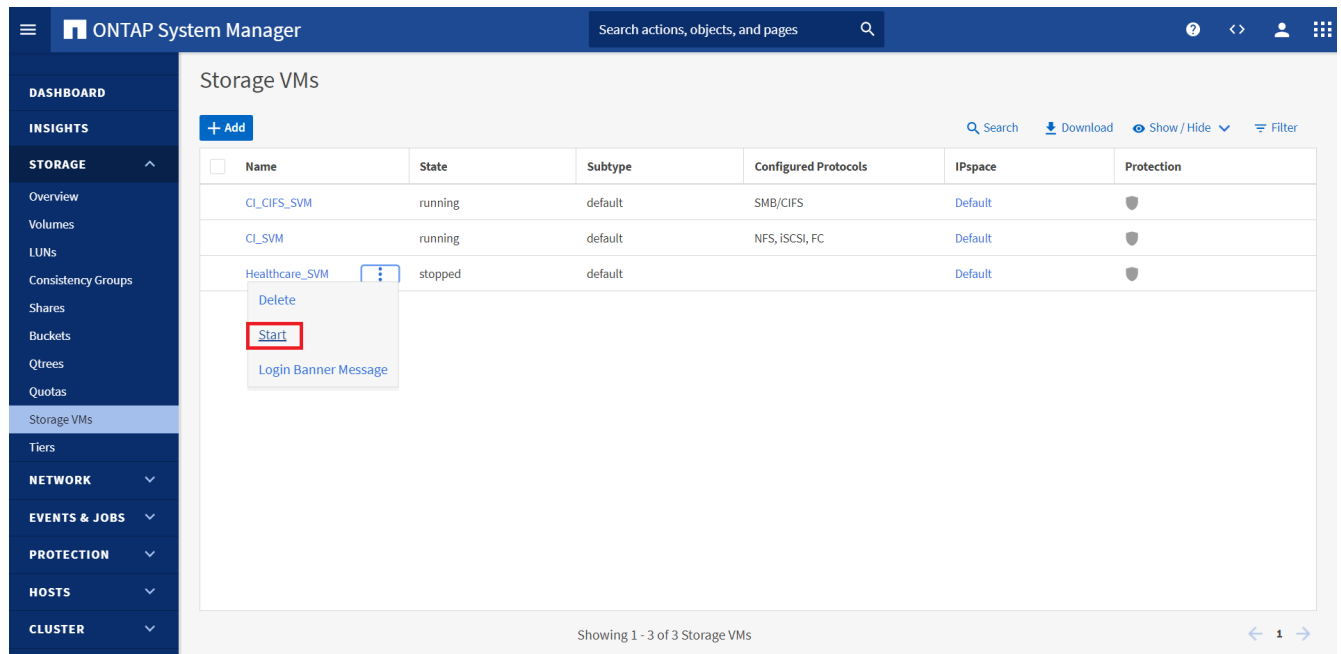
## Verifizierung der Daten am Produktionsstandort

Nach der Wiederherstellung des Produktionsstandorts müssen Sie sicherstellen, dass die ursprüngliche Konfiguration wiederhergestellt ist und Clients vom Quellstandort aus auf die Daten zugreifen können.

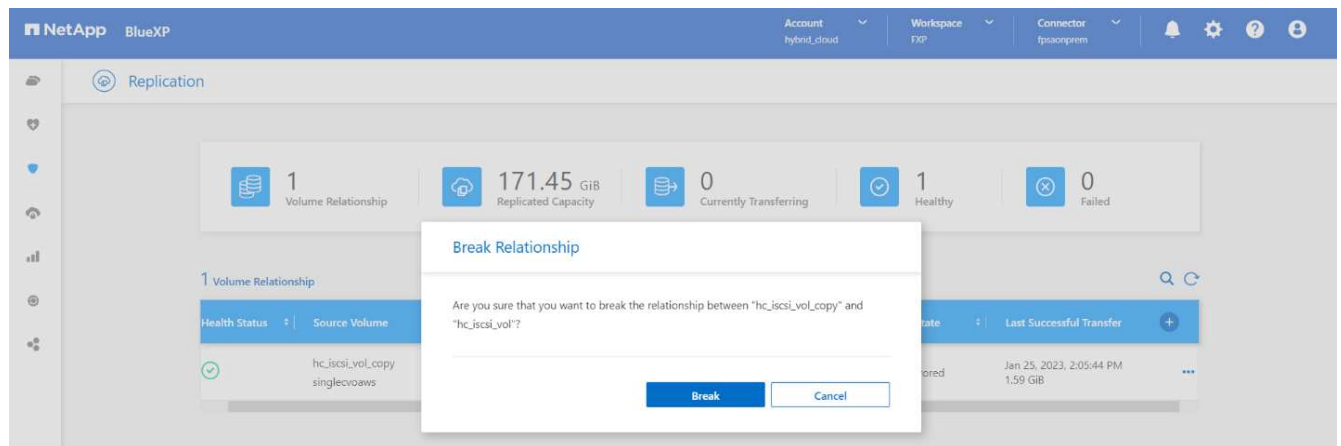
In diesem Abschnitt sprechen wir über die Einrichtung der Quellsite, die Wiederherstellung der SnapMirror-Beziehung zwischen On-Premises ONTAP und Cloud Volumes ONTAP und haben schließlich am Quellende eine Datenintegritätsprüfung durchgeführt

Für die Verifizierung der Daten am Produktionsstandort kann folgendes Verfahren verwendet werden:

- Stellen Sie sicher, dass der Quellstandort jetzt verfügbar ist. Starten Sie dazu die SVM, die das lokale ONTAP Volume hostet (hc\_iscsi\_vol).



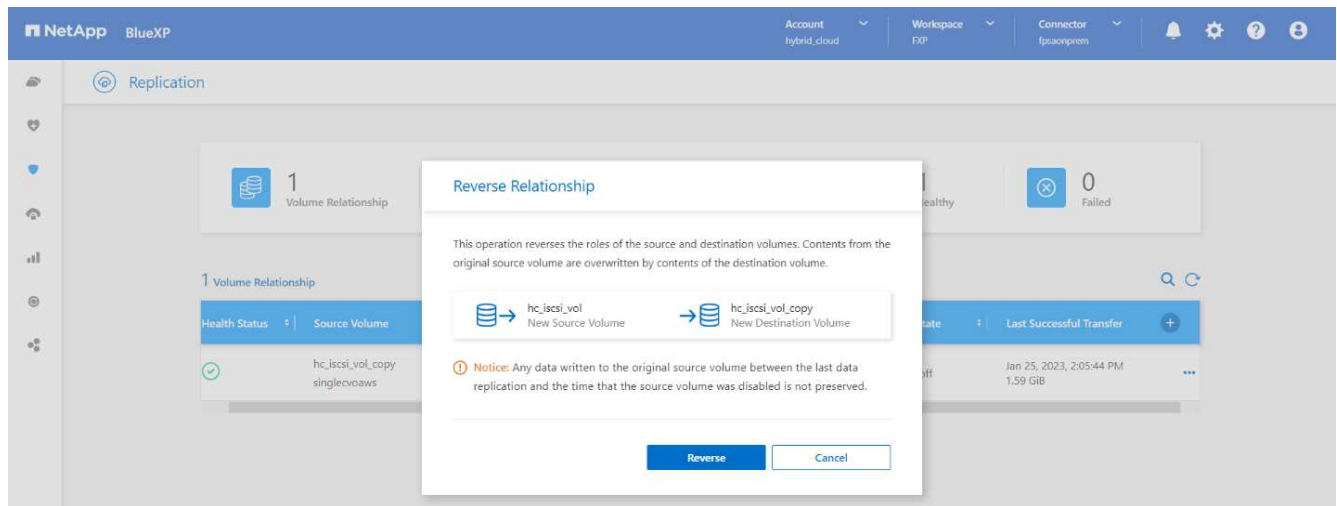
- Die SnapMirror Replizierungsbeziehung zwischen Cloud Volumes ONTAP und On-Premises-ONTAP wird unterbrochen und das On-Premises-Volume hochgestuft (hc\_iscsi\_vol) Zurück zur Produktion.



Nachdem die SnapMirror Beziehung beschädigt wurde, ändert sich der Typ des lokalen Volumes von Datensicherung (DP) in Lesen/Schreiben (RW).

```
A400-G0312::> volume show -volume hc_iscsi_vol -fields type
vserver          volume          type
-----
Healthcare_SVM hc_iscsi_vol RW
```

- Rückgängig machen der SnapMirror Beziehung Jetzt das lokale ONTAP Volume (hc\_iscsi\_vol) Wird das Quell-Volume, wie es früher war, und das Cloud Volumes ONTAP-Volume (hc\_iscsi\_vol\_copy) Wird zum Zielvolume.



Durch Befolgen dieser Schritte haben wir die ursprüngliche Konfiguration erfolgreich wiederhergestellt.

4. Starten Sie die lokale EHR-Instanz neu. Mounten Sie das Dateisystem und überprüfen Sie, ob das `newfile` Die Sie bei einem Produktionsstart auf der EHR-Instanz in der Cloud erstellt haben, existiert jetzt auch hier.

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1
[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01 dir05 dir09 dir13 dir17 dir21 dir25 dir29 dir33 dir37 dir41 dir45 dir49 dir53 dir57 dir61 dir65 dir69 dir73 dir77 kamini
dir02 dir06 dir10 dir14 dir18 dir22 dir26 dir30 dir34 dir38 dir42 dir46 dir50 dir54 dir58 dir62 dir66 dir70 dir74 dir78 latest file
dir03 dir07 dir11 dir15 dir19 dir23 dir27 dir31 dir35 dir39 dir43 dir47 dir51 dir55 dir59 dir63 dir67 dir71 dir75 dir79 newfile
dir04 dir08 dir12 dir16 dir20 dir24 dir28 dir32 dir36 dir40 dir44 dir48 dir52 dir56 dir60 dir64 dir68 dir72 dir76 dir80
```

Wir können daraus schließen, dass die Datenreplikation von der Quelle zum Ziel erfolgreich abgeschlossen wurde und dass die Datenintegrität gewahrt bleibt. Damit ist die Überprüfung der Daten am Produktionsstandort abgeschlossen.

"Weiter: Fazit."

## Schlussfolgerung

"Zurück: Lösungsvalidierung."

Der Aufbau einer Hybrid Cloud hat für die meisten Organisationen im Gesundheitswesen das Ziel, jederzeit für Verfügbarkeit der Daten zu sorgen. In dieser Lösung haben wir mit Cloud Volumes ONTAP eine FlexPod Hybrid-Cloud-Lösung implementiert und mithilfe der NetApp SnapMirror Replizierungstechnologie einige Anwendungsfälle für das Backup und Recovery von Applikationen und Workloads des Gesundheitswesens validiert.

FlexPod ist eine umfassend getestete und validierte konvergente Infrastruktur aus der strategischen Partnerschaft von Cisco und NetApp. Das Ziel ist es, vorhersehbare System-Performance mit niedriger Latenz und hohe Verfügbarkeit zu bieten. Dieser Ansatz führt zu einem hohen EHR-Komfort und letztendlich zu der besten Reaktionszeit für Benutzer des EHR-Systems.

Mit NetApp können Sie EHR-Produktion, Disaster Recovery, Backup oder Tiering in der Cloud genauso ausführen wie NetApp Storage-Funktionen in einem lokalen Datacenter. Mit NetApp Cloud Volumes ONTAP bietet NetApp die Funktionen der Enterprise-Klasse und die Performance, die für eine effiziente Ausführung von EHR in der Cloud erforderlich sind. Cloud-Optionen von NetApp bieten Block-über-iSCSI und File-über-NFS oder SMB.

Diese Lösung ist auf die Anforderungen von medizinischen Einrichtungen zugeschnitten und ermöglicht ihnen einen Schritt auf dem Weg hin zur digitalen Transformation. Außerdem kann sie ihre Applikationen und Workloads auf effiziente Weise managen.

"Weiter: Wo finden Sie zusätzliche Informationen."

## Wo Sie weitere Informationen finden

"Zurück: Schlussfolgerung."

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- FlexPod Startseite

["https://www.flexpod.com"](https://www.flexpod.com)

- Cisco Validated Design und Implementierungsleitfäden für FlexPod

["https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"](https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html)

- NetApp BlueXP

["https://bluexp.netapp.com/"](https://bluexp.netapp.com/)

- NetApp Cloud Volumes ONTAP

["https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html"](https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html)

- Schnellstart für Cloud Volumes ONTAP in AWS

["https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html"](https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html)

- SnapMirror Replizierung

["https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html"](https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html)

- TR-3928: NetApp Best Practices für Epic

<https://www.netapp.com/pdf.html?item=/media/17137-tr3928pdf.pdf>

- TR-4693 – Implementierungsleitfaden für FlexPod-Datacenter für Epic EHR

["https://www.netapp.com/media/10658-tr-4693.pdf"](https://www.netapp.com/media/10658-tr-4693.pdf)

- FlexPod für Epic

["https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/UCS\\_CVDs/flexpod\\_xseries\\_vmw\\_epic.html"](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmw_epic.html)

- NetApp Interoperabilitäts-Matrix-Tool

["http://support.netapp.com/matrix/"](http://support.netapp.com/matrix/)

- Cisco UCS Hardware and Software Interoperability Tool

["http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"](http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html)

- VMware Compatibility Guide

["http://www.vmware.com/resources/compatibility/search.php"](http://www.vmware.com/resources/compatibility/search.php)

#### **Versionsverlauf**

<b>Version</b>	<b>Datum</b>	<b>Versionsverlauf des Dokuments</b>
Version 1.0	März 2023	Ausgangsversion



## 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.