Hybrid Cloud

FlexPod

NetApp
November 04, 2025

Inhalt

Hybrid Cloud

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.

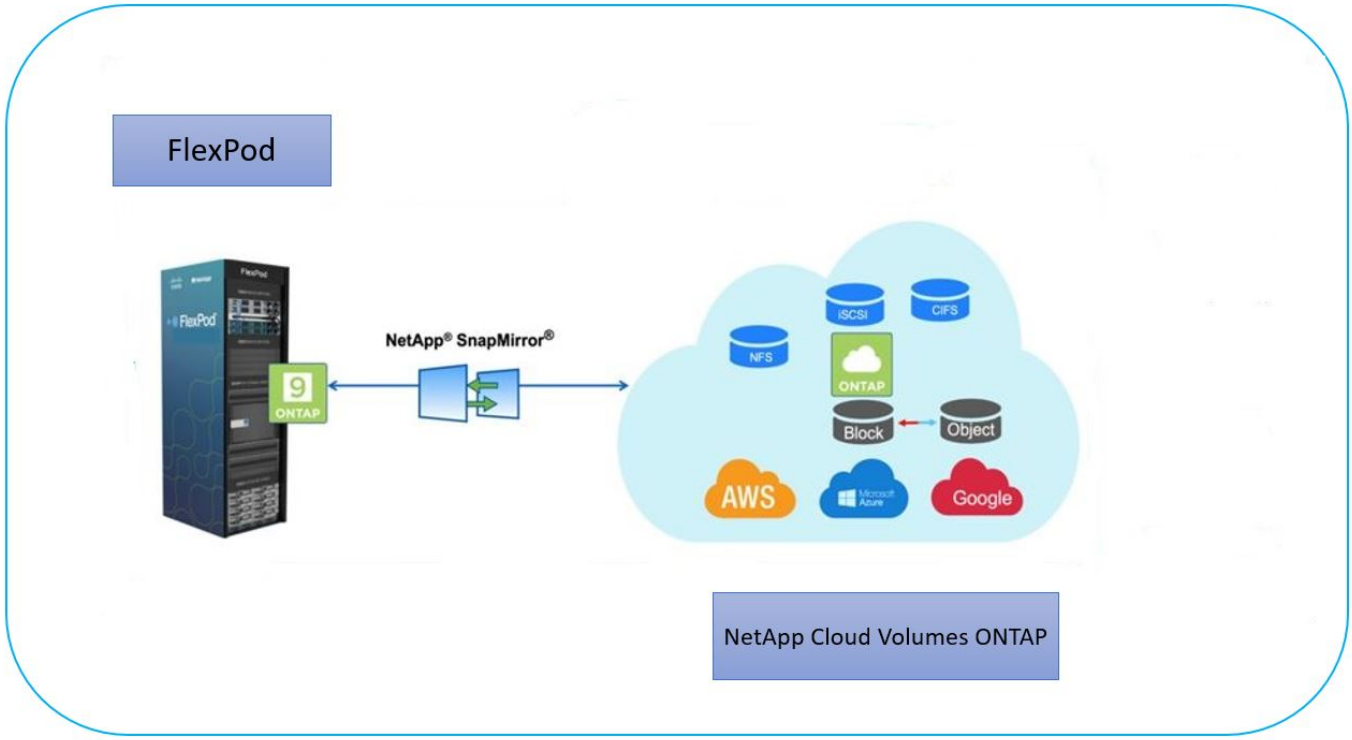
Durch die stetig wachsende Datenmenge im Gesundheitswesen und die wertvollen Einblicke, die diese Daten bieten, werden Datenservices und Datensicherung im Gesundheitswesen zu einer wichtigen und schwierigen Herausforderung. Erstens müssen Daten im Gesundheitswesen sowohl verfügbar als auch geschützt 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 Datenreplizierung, 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 Datenreplizierung 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

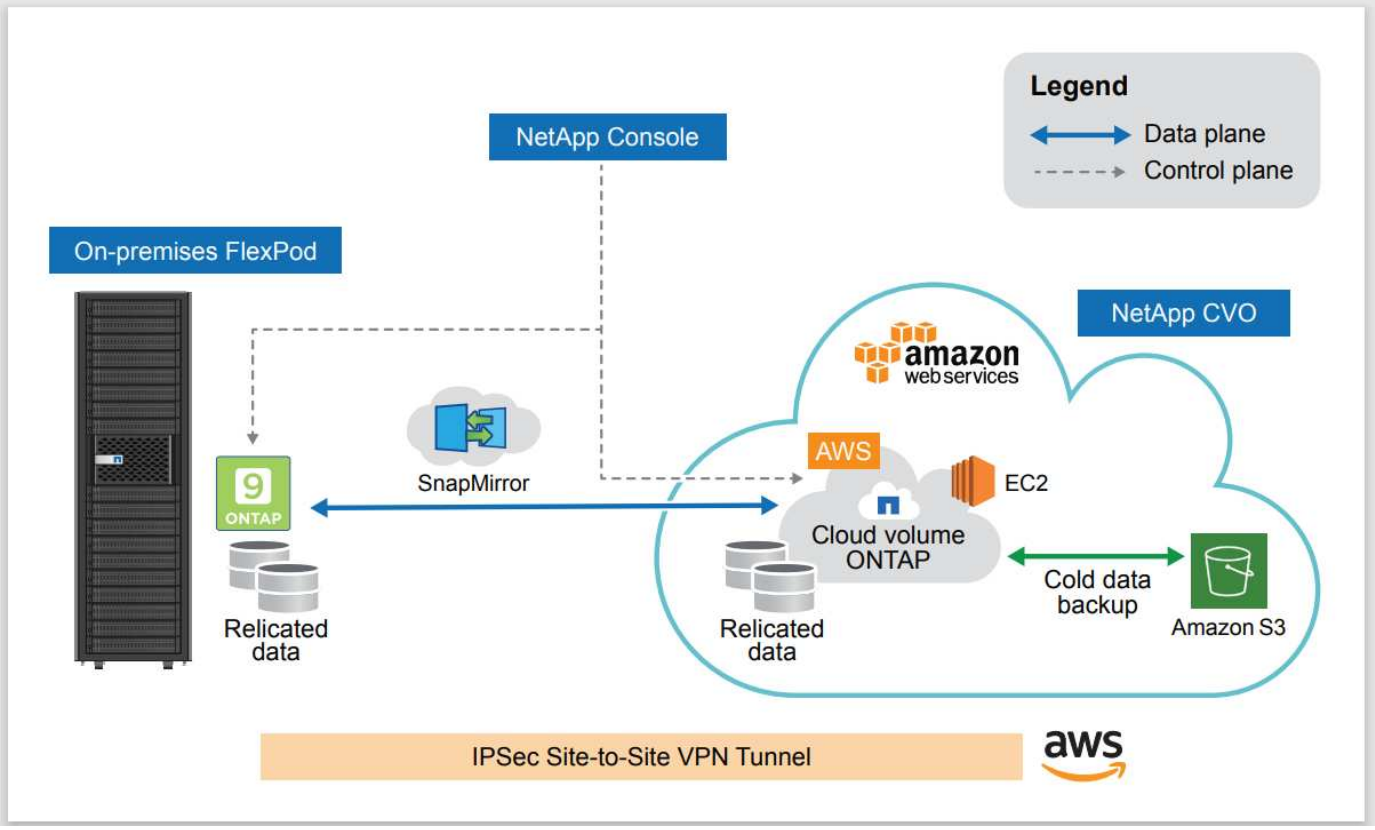
Eine Integration von FlexPod Datacenter mit NetApp Cloud Volumes ONTAP bietet folgende Vorteile für Workloads im Gesundheitswesen:

- **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 Datenreplizierung 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.

- **Schutz vor Ransomware.** Der Ransomware-Schutz der NetApp Console scannt Datenquellen in lokalen und Cloud-Umgebungen, erkennt Sicherheitslücken und gibt deren aktuellen Sicherheitsstatus und Risikobewertung an. Anschließend werden konkrete Handlungsempfehlungen gegeben, die Sie weiter untersuchen und befolgen können, um Abhilfe zu schaffen. Dies ermöglicht es Ihnen, Ihre kritischen Gesundheitsdaten vor Ransomware-Angriffen zu schützen.

Topologie der Lösung

Dieser Abschnitt beschreibt die logische Topologie der Lösung. Die folgende Abbildung stellt die Lösungstopologie dar, die aus der FlexPod -On-Premises-Umgebung, NetApp Cloud Volumes ONTAP (CVO), das auf Amazon Web Services (AWS) läuft, und der NetApp Console SaaS-Plattform besteht.



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 Continuance

FlexPod ist EHR-zertifiziert 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 hohen Komfortniveau von EHR für NetApp -Speicher mit ONTAP, ermöglicht es Ihnen, Ihre Anwendungen im Gesundheitswesen in einer vollständig verwalteten privaten Cloud über FlexPod auszuführen, die auch mit jedem beliebigen öffentlichen Cloud-Anbieter verbunden werden kann.

NetApp Console

NetApp Console ist eine SaaS-basierte Managementplattform der Enterprise-Klasse, die es IT-Experten und Cloud-Architekten ermöglicht, ihre hybride Multi-Cloud-Infrastruktur mithilfe von NetApp Cloud-Lösungen zentral zu verwalten. Es bietet ein zentralisiertes System zur Anzeige und Verwaltung Ihres lokalen und Cloud-Speichers und unterstützt Hybrid-Cloud-Umgebungen sowie mehrere Cloud-Anbieter und -Konten. Weitere Informationen finden Sie unter "Dokumentation zur NetApp Console".

Konsolenagent

Eine Console-Agent-Instanz ermöglicht es der Console, Ressourcen und Prozesse innerhalb einer öffentlichen Cloud-Umgebung zu verwalten. Für viele der von der Konsole bereitgestellten Funktionen wird ein Konsolenagent benötigt, der in der Cloud oder im lokalen Netzwerk bereitgestellt werden kann.

Ein Konsolenagent wird an folgenden Standorten unterstützt:

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

"Erfahren Sie mehr über Konsolenagenten".

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.

Für detailliertere Informationen siehe"Cloud Volumes ONTAP" Die

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.

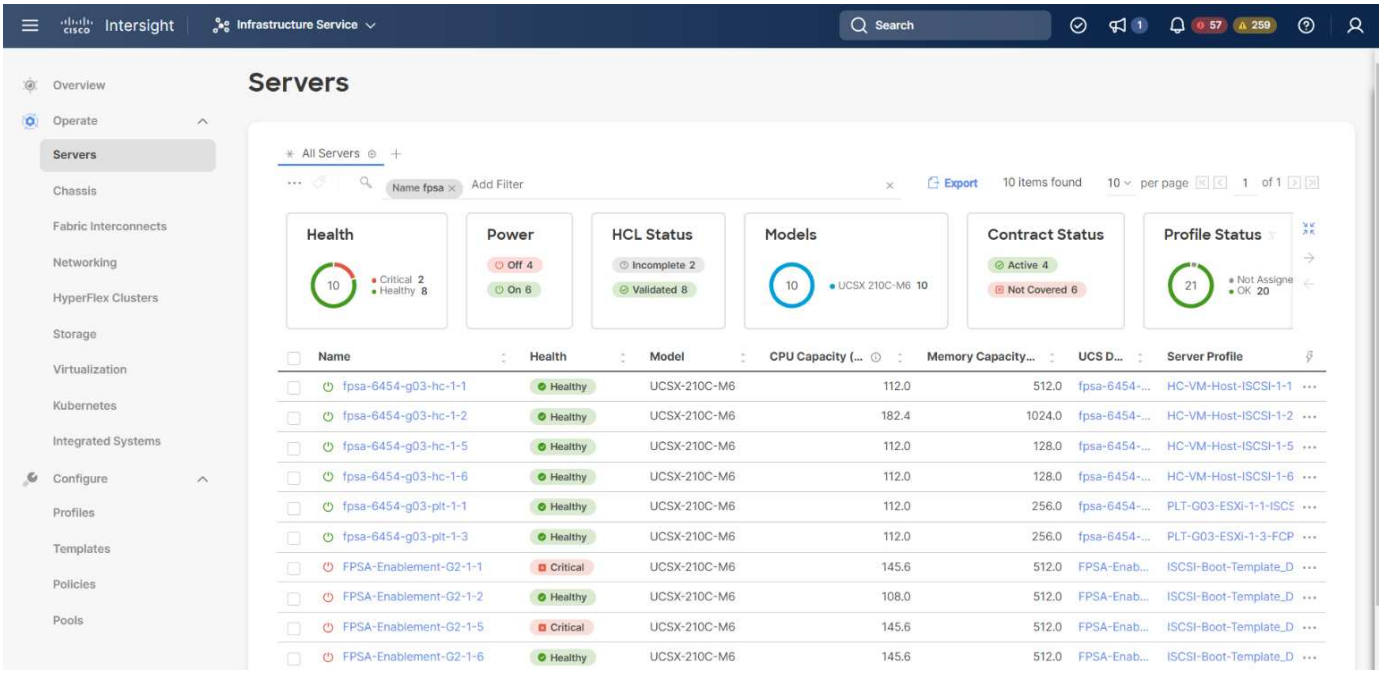
Weitere Informationen finden Sie unter "Active IQ Unified Manager".

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 zu VMware vSphere und seinen Komponenten finden Sie unter"VMware vSphere" Die

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.

Für detaillierte Informationen siehe"VMware vCenter" Die

Hardware- und Software-Versionen

Diese Hybrid-Cloud-Lösung kann auf jede FlexPod -Umgebung erweitert werden, die unterstützte Versionen von Software, Firmware und Hardware gemäß der Definition in der"NetApp Interoperabilitäts-Matrix-Tool" ,"UCS Hardware- und Softwarekompatibilität" , Und"VMware Compatibility Guide" Die

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

Komponente	Produkt	Version
Computing	Cisco UCS X210c M6	5.0(1b)

Komponente	Produkt	Version
	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

Die folgende Tabelle zeigt die Versionen von Console und Cloud Volumes ONTAP .

Anbieter	Produkt	Version
NetApp	Konsole	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 die NetApp Console zu.

Um auf die Konsole und andere Cloud-Dienste zuzugreifen, müssen Sie sich anmelden bei "NetApp Console" Die Informationen zum Einrichten von Arbeitsbereichen und Benutzern im Konsolenkonto finden Sie unter "Einrichtung und Verwaltung der NetApp Console" Die Sie benötigen ein Konto, das die Berechtigung besitzt, den Console-Agenten direkt von der Console aus bei Ihrem Cloud-Anbieter bereitzustellen. Um die benötigten Berechtigungen zu erhalten, lesen Sie bitte Folgendes: "Berechtigungsübersicht für die NetApp Console" Die

4. Konsolenagent bereitstellen.

   Bevor Sie ein Cloud Volume ONTAP -System hinzufügen, müssen Sie einen Konsolenagenten bereitstellen. Die Konsole fordert Sie auf, wenn Sie versuchen, Ihr erstes Cloud Volumes ONTAP System ohne installierten Konsolenagenten zu erstellen. Informationen zur Bereitstellung eines Console-Agenten in AWS über die Console finden Sie unter "Installationsoptionen für Konsolenagenten in AWS" Die

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".

   Bei dieser Lösung haben wir ein Cloud Volumes ONTAP System mit einem einzigen Knoten in AWS bereitgestellt.

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 Repositorys 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. vserver create -vserver Healthcare_SVM -rootvolume
Healthcare_SVM_root -aggregate aggr1_A400_G0312_01 -rootvolume-security
-style unix
2. vserver add-protocols -vserver Healthcare_SVM -protocols iscsi
3. vserver iscsi create -vserver Healthcare_SVM

   To verify:

   A400-G0312::> vserver iscsi show -vserver 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 -vserver 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 der NetApp Console lokalen FlexPod Speicher hinzu.

Führen Sie die folgenden Schritte aus, um Ihren FlexPod -Speicher mithilfe der Konsole zum System hinzuzufügen.

1. Wählen Sie im Navigationsmenü **Speicher** > **Systeme**.
2. Klicken Sie auf der Seite „Systeme“ auf **System hinzufügen** und wählen Sie **Lokale Installation** aus.
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**.
5. Geben Sie auf der Seite Details und Anmeldeinformationen einen Namen und eine Beschreibung für die Arbeitsumgebung ein, und klicken Sie dann auf **Go**.

   Die Konsole erkennt den ONTAP Cluster und fügt ihn als System auf der Seite „Systeme“ hinzu.

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 `pvcreate` 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 den I/O-Simulator von EHR
(GenerateIO).  Die Daten innerhalb der LUNs werden mit dem EHR generiert.
`Dgen.pl` Skript.  Das Skript ist so konzipiert, dass es Daten erzeugt,
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** > **Systeme**.
2. Wählen Sie unter „Systeme“ das System aus, das das Quellvolume enthält, ziehen Sie es auf das System, auf das 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. **Zieldatentyp und Tiering.** Wenn es sich bei dem Ziel um ein Cloud Volumes ONTAP-System handelt, wählen Sie den Zieldatentyp aus und wählen, ob Sie Daten-Tiering aktivieren möchten.
6. **Zieldatenträger Name:** Geben Sie den Namen des Zieldatenträger an und wählen Sie das Zielaggregat. Wenn das Ziel ein ONTAP-Cluster ist, müssen Sie auch die Ziel-Storage-VM angeben.
7. **Maximale Übertragungsrate.** Geben Sie die maximale Übertragungsrate (in Megabyte pro Sekunde) an.
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".

Die Konsole startet den Datenreplikationsprozess. In diesem Stadium können Sie den **Replikationsdienst** 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.

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

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

"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 NetApp Console GUI unter der Registerkarte **Replikation** 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.

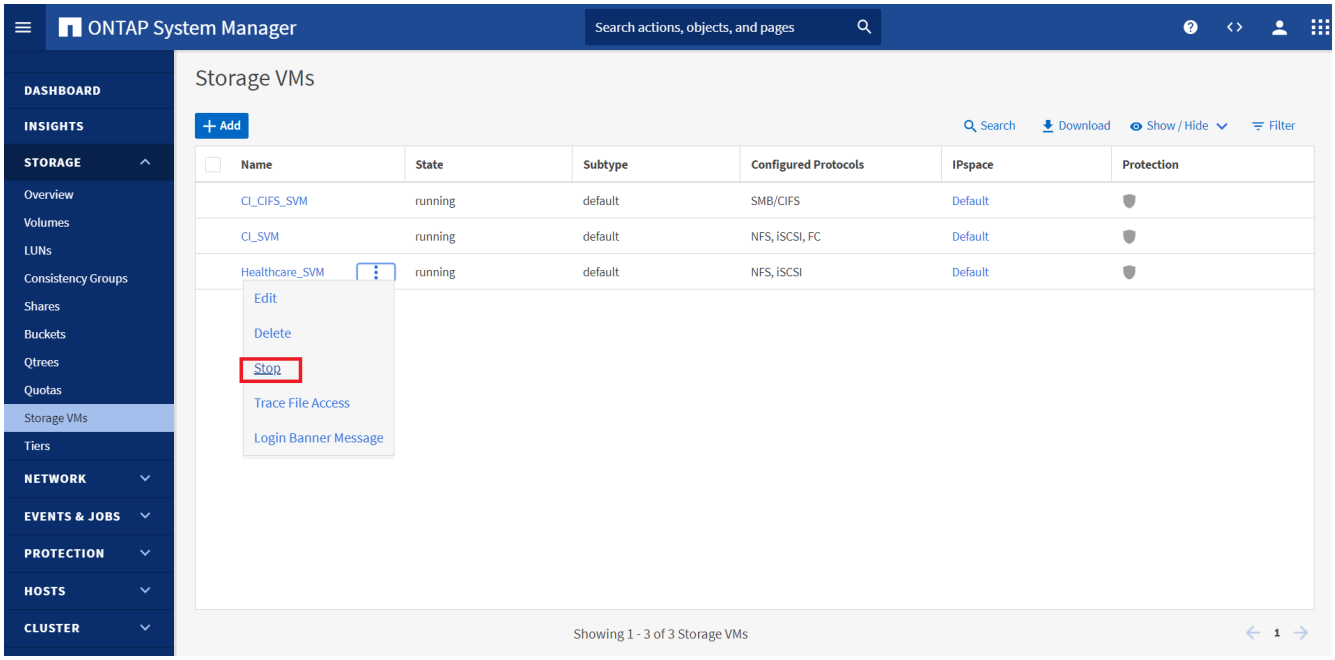
Disaster Recovery

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`).



   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 gestoppt wurde, `hc_iscsi_vol` Die Lautstärke wird in der Konsole nicht angezeigt.

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.

a. 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.

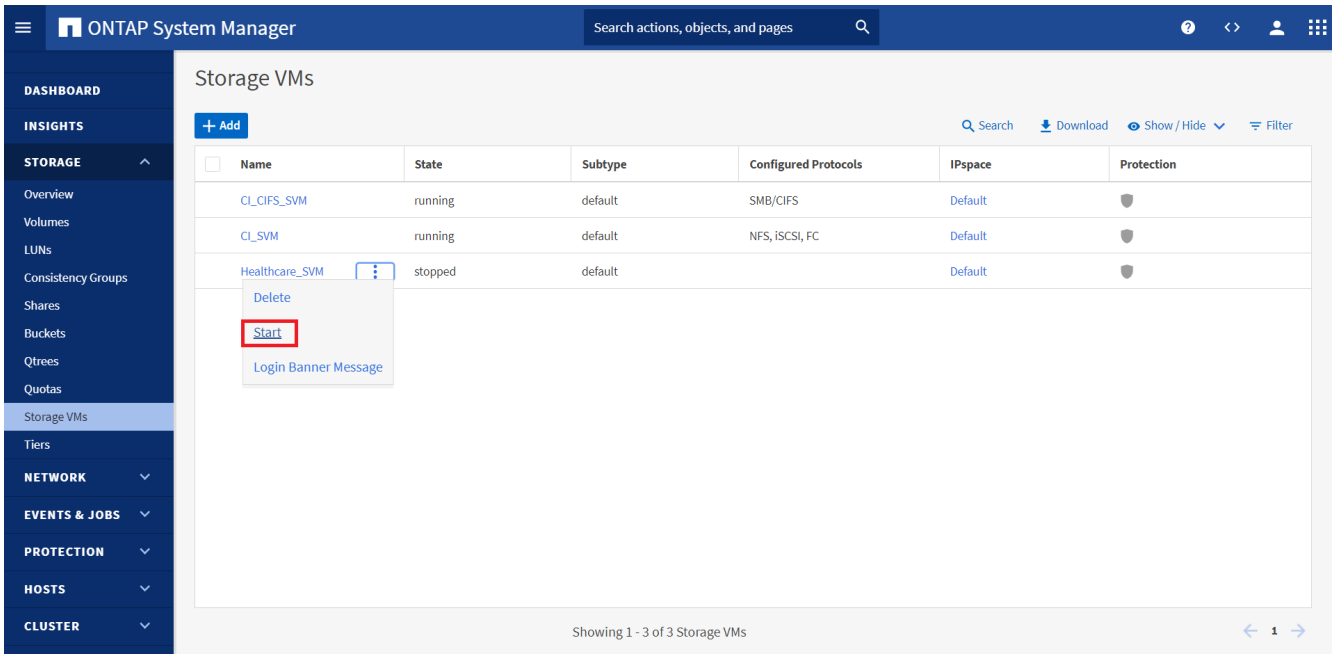
Verifizierung der Daten am Produktionsstandort

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:

1. Stellen Sie sicher, dass der Quellstandort jetzt verfügbar ist. Starten Sie dazu die SVM, die das lokale ONTAP Volume hostet (`hc_iscsi_vol`).



2. 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).

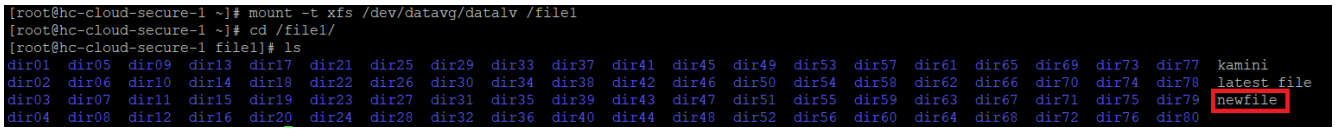
```
A400-G0312::> volume show -volume hc_iscsi_vol -fields type
vserver        volume       type
-------------- ------------ ----
Healthcare_SVM hc_iscsi_vol RW
```

3. 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.



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"

- 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"

- NetApp Console

  "https://console.netapp.com/"

- NetApp Cloud Volumes ONTAP

  "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"

- SnapMirror Replizierung

  "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"

- FlexPod für Epic

  "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/"

- Cisco UCS Hardware and Software Interoperability Tool

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- VMware Compatibility Guide

  "http://www.vmware.com/resources/compatibility/search.php"

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	März 2023	Ausgangsversion

FlexPod Hybrid Cloud für Google Cloud Platform mit NetApp Cloud Volumes ONTAP und Cisco Intersight

TR-4939: FlexPod Hybrid Cloud for Google Cloud Platform with NetApp Cloud Volumes ONTAP and Cisco Intersight

Ruchika Lahoti, NetApp

Einführung

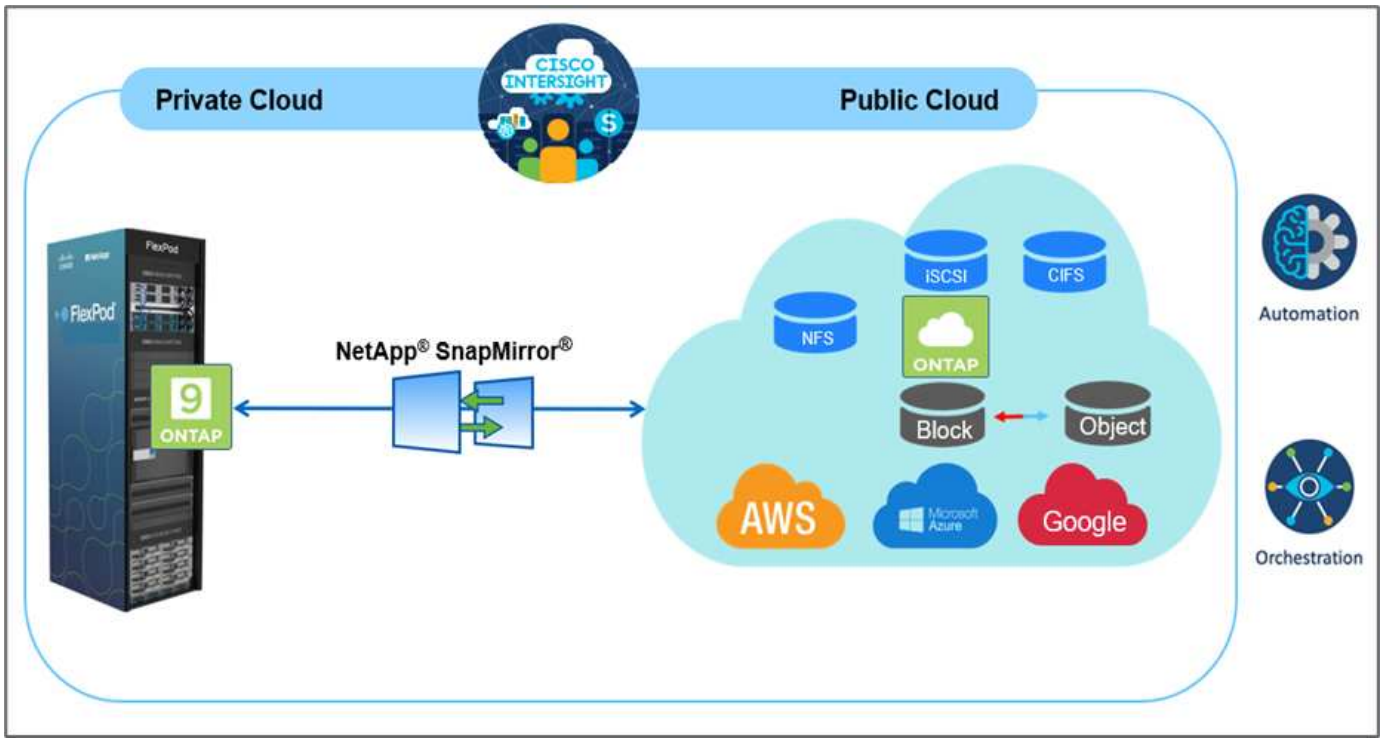
Der Schutz von Daten mit Disaster Recovery (DR) ist ein wichtiges Ziel für die Aufrechterhaltung von Unternehmenskontinuität. DR ermöglicht Unternehmen ein Failover ihrer Betriebsabläufe an einem sekundären Standort und Recovery und Failback effizient und zuverlässig zum primären Standort. Aufgrund diverser Bedenken wie Naturkatastrophen, Netzwerkausfälle, Softwareschwachstellen und menschlichem Versagen ist die Entwicklung einer DR-Strategie eine der obersten IT-Prioritäten.

Beim DR müssen alle Workloads, die am primären Standort ausgeführt werden, originalgetreu wiedergegeben werden. Ein Unternehmen muss außerdem über eine aktuelle Kopie aller Unternehmensdaten verfügen, einschließlich Datenbanken, File Services, NFS- und iSCSI-Storage usw. Da die Daten in der Produktionsumgebung kontinuierlich aktualisiert werden, müssen regelmäßig Änderungen an den DR-Standort übertragen werden.

Die Implementierung von DR-Umgebungen ist für die meisten Unternehmen eine Herausforderung, da die Infrastruktur und der Standort unabhängig sein müssen. Die Zahl der erforderlichen Ressourcen und die Kosten für das Einrichten, Testen und Warten eines sekundären Datacenters können sehr hoch sein. Damit sinken normalerweise die Kosten für die gesamte Produktionsumgebung. Es ist schwierig, einen minimalen Platzbedarf für Daten mit angemessener Sicherung zu gewährleisten, die Daten kontinuierlich zu synchronisieren und für nahtloses Failover und Failback zu sorgen. Nach dem Aufbau des DR-Standorts besteht die Herausforderung darin, die Daten aus der Produktionsumgebung zu replizieren und weiterhin synchronisiert zu halten.

In diesem technischen Bericht werden die konvergente Infrastrukturlösung FlexPod, NetApp Cloud Volumes ONTAP auf Google Cloud und Cisco Intersight zu einem Hybrid Cloud-Datacenter für DR kombiniert. Bei dieser Lösung wird über den Entwurf und die Ausführung eines ONTAP-Workflows vor Ort mithilfe von Cisco Intersight Cloud Orchestrator diskutiert. Wir sprechen auch über die Implementierung von NetApp Cloud Volumes ONTAP sowie die Orchestrierung und Automatisierung der Datenreplizierung und DR zwischen FlexPod und Cloud Volumes ONTAP mithilfe des Cisco Intersight Service für HashiCorp Terraform.

Die folgende Abbildung bietet einen Lösungsüberblick.



Diese Lösung bietet zahlreiche Vorteile, darunter:

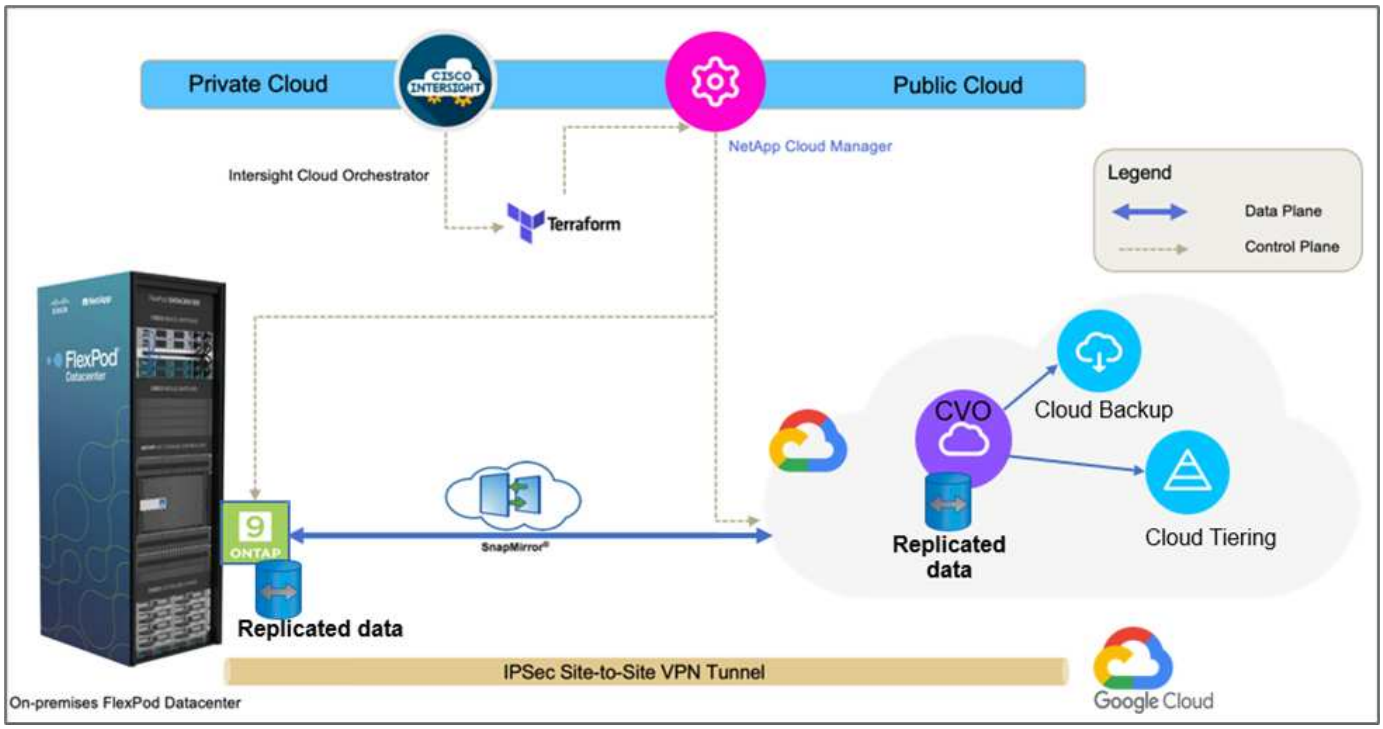
- **Orchestrierung und Automatisierung.** Cisco Intersight vereinfacht den täglichen Betrieb einer FlexPod Hybrid-Cloud-Infrastruktur durch Bereitstellung konsistenter Orchestrierungs-Frameworks, die über Automatisierung bereitgestellt werden.
- **Customized Protection.** Cloud Volumes ONTAP bietet Daten auf Block-Ebene von ONTAP in die Cloud, die das Ziel auf dem neuesten Stand durch inkrementelle Updates hält. Benutzer können einen Zeitplan alle 5 Minuten oder jede Stunde angeben, beispielsweise basierend auf von Änderungen an der Quelle, die übertragen werden.
- **Nahtloses Failover und Failback.** bei einem Ausfall können Storage-Administratoren schnell ein Failover auf Cloud Volumes durchführen. Wenn der primäre Standort wiederhergestellt ist, werden die in der DR-Umgebung erstellten neuen Daten zurück zu den Quell-Volumes synchronisiert und die sekundäre Datenreplizierung wiederhergestellt.
- **Effizienz:** der Speicherplatz und die Kosten für die sekundäre Cloud Kopie werden durch Datenkomprimierung, Thin Provisioning und Deduplizierung optimiert. Die Daten werden auf Blockebene komprimiert und dedupliziert und so die Übertragungsgeschwindigkeit verbessert. 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.
- **Höhere IT-Produktivität.** die Verwendung von Intersight als eine einzige sichere Plattform der Enterprise-Klasse für Infrastruktur- und Application Lifecycle Management vereinfacht das Konfigurationsmanagement und die Automatisierung manueller Aufgaben nach Maß für die Lösung.

Zielgruppe

Dieses Dokument richtet sich an Vertriebsmitarbeiter, Berater im Außendienst, Professional Services, IT-Manager, Engineers von Partnern, Techniker für Standortzuverlässigkeit, Cloud-Architekten, Cloud Engineers und Kunden, die eine Infrastruktur nutzen möchten, um IT-Effizienz und IT-Innovationen zu liefern.

Topologie der Lösung

In diesem Abschnitt wird die logische Topologie der Lösung beschrieben. Die folgende Abbildung zeigt die Lösungstopologie der lokalen FlexPod Umgebung, NetApp Cloud Volumes ONTAP auf Google Cloud, Cisco Intersight und NetApp Cloud Manager.



Die Kontrollebenen und Datenebenen werden zwischen den Endpunkten klar angezeigt. Die Datenebene stellt über eine sichere Site-to-Site-VPN-Verbindung eine Verbindung her, um die ONTAP Instanz, die auf FlexPod All Flash FAS ausgeführt wird, mit der NetApp Cloud Volumes ONTAP Instanz in Google Cloud zu verbinden.

Die Replizierung von Workload-Daten von FlexPod in NetApp Cloud Volumes ONTAP wird von NetApp SnapMirror übernommen. Insgesamt wird Cisco Intersight Cloud Orchestrator sowohl für On-Premises- als auch für Cloud-Umgebungen orchestriert. Cisco Intersight Cloud Orchestrator nutzt Terraform Resource Providers für NetApp Cloud Manager, um Operationen für die NetApp Cloud Volumes ONTAP-Implementierung durchzuführen und Datenreplizierungsbeziehungen einzurichten.

Diese Lösung unterstützt auch das optionale Backup und Tiering kalter Daten in der NetApp Cloud Volumes ONTAP Instanz zu Google Cloud Storage.

"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 Networking, Cisco MDS Storage Networking und Cisco Unified Computing System (Cisco UCS). Das Design ist flexibel genug, dass Netzwerk, Computing und Storage in ein Datacenter Rack passen oder nach dem Datacenter-Design des Kunden bereitgestellt werden können. Dank der Port-Dichte können die

Netzwerkkomponenten mehrere Konfigurationen aufnehmen.

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.** als Service aus der Cloud oder im Rechenzentrum des Kunden mit häufigen Updates und fortgesetzten Innovationen durch ein agiles, auf Software basierendes Entwicklungsmodell geliefert. So kann sich der Kunde auf eine schnellere Bereitstellung von Geschäftsbereichen konzentrieren.
- * Vereinfachter Betrieb.* vereinfachter Betrieb durch den Einsatz eines einzigen sicheren SaaS-bereitgestellten Tools mit gemeinsamem Inventar, Authentifizierung und APIs für die Zusammenarbeit im gesamten Stack und an allen Standorten, sodass Silos in allen Teams vermieden werden. Vom Management physischer Server und Hypervisoren vor Ort, zu VMs, K8s, serverlos, Automatisierung, Die Optimierung und Kostenkontrolle über On-Premises- und Public Clouds hinweg.
- **Kontinuierliche Optimierung.** Optimieren Sie Ihre Umgebung mithilfe von Informationen, die von Cisco Intersight in allen Schichten bereitgestellt werden, sowie von Cisco TAC. Diese Informationen werden in empfohlene und automatisierbare Aktionen umgewandelt, mit denen Sie Echtzeit an jede Änderung anpassen können: Von dem Verschieben von Workloads und der Überwachung des Zustands von physischen Servern bis hin zu Kostenreduzierungsempfehlungen für die Public Clouds, mit denen Sie arbeiten.

Cisco Intersight ermöglicht zwei verschiedene Managementmodi: UCSM Managed Mode (UMM) und Intersight Managed Mode (IMM). Bei der erstmaligen Einrichtung von Fabric Interconnects können Sie natives UMM oder IMM für Fabric-Attached Cisco UCS-Systeme auswählen. In dieser Lösung wird natives IMM verwendet.

Cisco Intersight-Lizenzierung

Cisco Intersight verwendet eine abonnementbasierte Lizenz mit mehreren Ebenen.

Cisco Intersight Lizenz-Tiers sind wie folgt:

- **Cisco Intersight Essentials.** enthält alle Basisfunktionen sowie die folgenden Funktionen:
  - Cisco UCS Central
  - Cisco IMC Supervisor-Berechtigung
  - Richtlinienbasierte Konfiguration mit Server-Profilen
  - Firmware-Management
  - Bewertung der Kompatibilität mit der Hardware Compatibility List (HCL)
- **Cisco Intersight Advantage.** umfasst die Merkmale und Funktionen des Essentials-Tier sowie die folgenden Funktionen:
  - Widgets, Inventar, Kapazität, Auslastungsfunktionen und domänenübergreifende Korrelation zwischen physischem Computing, Netzwerk, Storage, VMware Virtualisierung und AWS Public Cloud
  - Der Cisco Security Advisory Service, bei dem Kunden wichtige Sicherheitswarnungen und Hinweise zu betroffenen Endgeräten erhalten können.
- **Cisco Intersight Premier.** Zusätzlich zu den in der Advantage-Stufe angebotenen Funktionen bietet Cisco Intersight Premier Folgendes:
  - Intersight Cloud Orchestrator (ICO) für Computing, Netzwerk, Storage, integrierte Systeme,

Virtualisierung, Container und Public-Cloud-Plattformen

- Uneingeschränkte Abonnementberechtigung für Cisco UCS Director ohne zusätzliche Kosten.

Weitere Informationen zu Intersight Licensing und den in jeder Lizenz unterstützten Funktionen finden Sie hier "Hier".

> In dieser Lösung verwenden wir Intersight Cloud Orchestrator und Intersight Service für HashiCorp Terraform. Diese Funktionen stehen Benutzern mit der Intersight Premier-Lizenz zur Verfügung, sodass diese Lizenzstufe aktiviert werden muss.

Terraform Cloud-Integration mit ICO

Mithilfe von Cisco Intersight Cloud Orchestrator (ICO) können Workflows erstellt und ausgeführt werden, die Terraform Cloud (TFC)-APIs genannt werden. Die Aufgabe Web-API-Anfrage aufrufen unterstützt Terraform Cloud als Ziel und kann mithilfe von HTTP-Methoden mit Terraform Cloud-APIs konfiguriert werden. Der Workflow kann somit über eine Kombination von Aufgaben verfügen, die unter Verwendung generischer API-Aufgaben und anderer Operationen mehrere Terraform Cloud-APIs aufrufen. Für die Nutzung der ICO-Funktion benötigen Sie eine Premier-Lizenz.

Cisco Intersight Assist

Cisco Intersight Assist unterstützt Sie beim Hinzufügen von Endpunktgeräten zu Cisco Intersight. Ein Rechenzentrum kann mehrere Geräte haben, die nicht direkt mit Cisco Intersight verbunden sind. Jedes von Cisco Intersight unterstützte Gerät, das jedoch keine direkte Verbindung zu diesem Gerät herstellt, erfordert einen Verbindungsmechanismus. Der Cisco Intersight Assist bietet diesen Verbindungsmechanismus und hilft Ihnen beim Hinzufügen von Geräten zu Cisco Intersight.

Der Cisco Intersight Assist ist innerhalb der Cisco Intersight Virtual Appliance erhältlich, die als zur Verfügung stehende Virtual Machine verteilt wird, die sich in einem OVA-Dateiformat (Open Virtual Appliance) befindet. Sie können das Gerät auf einem ESXi-Server installieren. Weitere Informationen finden Sie im "Cisco Intersight Virtual Appliance – Erste Schritte".

Nach der Inanspruchnahme des Intersight Assist bei Intersight können Sie Endgeräte mithilfe der Option Claim through Intersight Assist anfordern. Weitere Informationen finden Sie unter "Erste Schritte".

NetApp Cloud Volumes ONTAP

- Nutzen Sie integrierte Datendeduplizierung, Datenkomprimierung, Thin Provisioning und Klonen und minimieren Sie so die Storage-Kosten.
- Zuverlässigkeit der Enterprise-Klasse und unterbrechungsfreien Betrieb bei Ausfällen in der Cloud-Umgebung.
- Cloud Volumes ONTAP nutzt die branchenführende Replizierungstechnologie NetApp SnapMirror bei der Replizierung von Daten vor Ort in der Cloud, sodass sekundäre Kopien für unterschiedliche Anwendungsfälle verfügbar sind.
- Cloud Volumes ONTAP ist auch in Cloud Backup Service integriert und bietet Backup- und Restore-Funktionen zur Sicherung und Langzeitarchivierung Ihrer Cloud-Daten.
- Wechsel zwischen hochperformanten Storage-Pools nach Bedarf, ohne Applikationen offline zu schalten
- Konsistenz von Snapshot Kopien mit NetApp SnapCenter.
- Cloud Volumes ONTAP unterstützt die Datenverschlüsselung und bietet Schutz vor Viren und Ransomware.

- Integration in Cloud Data Sense unterstützt Sie dabei, den Datenkontext zu verstehen und sensible Daten zu identifizieren.

Cloud Central

Cloud Central bietet einen zentralen Standort zum Zugriff auf NetApp Cloud-Datenservices und -Management. Mit diesen Services können Sie kritische Applikationen in der Cloud ausführen, automatisierte DR-Standorte erstellen, Ihre SaaS-Daten sichern und Daten effektiv über mehrere Clouds hinweg migrieren und steuern. Weitere Informationen finden Sie unter "Cloud Central".

Cloud Manager

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. Das zentralisierte System zur Anzeige und zum Management von lokalem und Cloud-Storage ermöglicht die Unterstützung diverser Hybrid-Cloud-Provider und -Konten. Weitere Informationen finden Sie unter "Cloud Manager".

Stecker

Mithilfe von Connector kann Cloud Manager Ressourcen und Prozesse in einer Public-Cloud-Umgebung managen. Um viele Funktionen von Cloud Manager nutzen zu können, muss eine Connector-Instanz eingesetzt werden, die in der Cloud oder im On-Premises-Netzwerk eingesetzt werden kann. Der Anschluss wird an folgenden Orten unterstützt:

- AWS
- Microsoft Azure
- Google Cloud
- On-Premises

NetApp Active IQ Unified Manager

Mit NetApp Active IQ Unified Manager überwachen Sie Ihre ONTAP Storage-Cluster über eine einzelne, neu gestaltete, intuitive Oberfläche, die wertvolle Informationen aus dem Wissen der Community und aus KI-Analysen liefert. Er bietet umfassenden Einblick 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 Korrekturmaßnahmen, die Sie zur Behebung des Problems ergreifen 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 lassen sich die Storage-Anforderungen Ihrer Benutzer planen, indem Kapazität und Nutzungstrends proaktiv vor Problemen vorhergesagt werden. Reaktive, kurzfristige Entscheidungen, die langfristig zu weiteren Problemen führen können, werden vermieden.

VMware vSphere

VMware vSphere ist eine Virtualisierungsplattform, mit der sich umfangreiche Sammlung von Infrastrukturen (Ressourcen wie CPUs, Storage und Netzwerk) vollständig als nahtlose, vielseitige und dynamische Betriebsumgebung managen lassen. Im Gegensatz zu herkömmlichen Betriebssystemen, die eine einzelne Machine managen, sammelt VMware vSphere die Infrastruktur eines gesamten Datacenters und erstellt so ein

einzelnes Kraftpaket, mit Ressourcen, die den jeweiligen Applikationen schnell und dynamisch zugewiesen werden können.

Weitere Informationen zu VMware vSphere finden Sie im folgenden "Dieser Link".

VMware vSphere vCenter

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.

Hardware- und Softwareversionen

Diese Hybrid Cloud-Lösung kann auf alle FlexPod Umgebungen erweitert werden, auf denen unterstützte Versionen von Software, Firmware und Hardware ausgeführt werden. Diese Versionen sind im NetApp Interoperabilitäts-Matrix-Tool und der Cisco UCS Hardware Compatibility List definiert.

Die FlexPod Lösung, die als Basisplattform in unserer On-Premises-Umgebung verwendet wird, wurde entsprechend den beschriebenen Richtlinien und Spezifikationen implementiert "Hier".

Das Netzwerk in dieser Umgebung ist auf ACI basiert. Weitere Informationen finden Sie unter "Hier".

- Weitere Informationen finden Sie unter den folgenden Links:
- "NetApp Interoperabilitäts-Matrix-Tool"
- "VMware Compatibility Guide"
- "Cisco UCS Hardware and Software Interoperability Tool"

In der folgenden Tabelle werden die Versionen von FlexPod Hardware und Software aufgeführt.

Komponente	Produkt	Version
Computing	CISCO UCS X210C-M6	5.0(1b)
	Cisco UCS Fabric Interconnects 6454	4.2(2a)
Netzwerk	Cisco Nexus 9332C (Spine)	14.2(7 s)
	Cisco Nexus 9336C-FX2 (Blatt)	14.2(7 s)
	Cisco ACI	4.2(7 s)
Storage	NetApp AFF A220	9.11.1
	NetApp ONTAP Tools für VMware vSphere	9.10
	NetApp NFS Plug-in für VMware VAAI	2.0-15
	Active IQ Unified Manager	9.11
Software	VSphere ESXi	7.0 (U3)

Komponente	Produkt	Version
	VMware vCenter Appliance	7.0.3
	Cisco Intersight Assist Virtual Appliance	1.0.11-306

Die Ausführung von Terraform-Konfigurationen findet auf dem Terraform Cloud for Business Account statt. Die Terraform-Konfiguration verwendet den Terraform-Provider für NetApp Cloud Manager.

In der folgenden Tabelle sind die Anbieter, Produkte und Versionen aufgeführt.

Komponente	Produkt	Version
HashiCorp	Terraform	1.2.7

Folgende Tabelle zeigt die Versionen des Cloud Manager und Cloud Volumes ONTAP.

Komponente	Produkt	Version
NetApp	Cloud Volumes ONTAP	9.11
	Cloud Manager	3.9.21

"Als Nächstes: Installation und Konfiguration – Deploy FlexPod."

Installation und Konfiguration

Implementieren Sie FlexPod

"Früher: Lösungskomponenten."

Um die Details zu FlexPod Design und Implementierung, einschließlich der Konfiguration verschiedener Design-Elemente und der zugehörigen Best Practices, zu verstehen, finden Sie unter "Cisco Validated Designs für FlexPod".

FlexPod kann sowohl im UCS Managed Mode als auch im Cisco Intersight Managed Mode implementiert werden. Wenn Sie FlexPod im UCS Managed Mode implementieren, finden Sie das neueste Cisco Validated Design "Hier".

Cisco Unified Compute System (Cisco UCS) X-Series ist ein brandneues modulares Computing-System, das über die Cloud konfiguriert und gemanagt wird. Sie wurde entwickelt, um die Anforderungen moderner Applikationen zu erfüllen sowie durch ein anpassbares, zukunftbares, modulares Design die betriebliche Effizienz, Flexibilität und Skalierbarkeit zu verbessern. Es ist eine Anleitung zum Design bezüglich der Integration der von Cisco Intersight gemanagten UCS X-Series Plattform in die FlexPod Infrastruktur vorhanden "Hier".

Eine Implementierung von FlexPod mit Cisco ACI findet sich "Hier".

"Als Nächstes: Konfiguration von Cisco Intersight."

Konfiguration von Cisco Intersight

"Früher waren sie FlexPod implementiert."

Zur Konfiguration des Cisco Intersight- und Intersight-Assistenten finden Sie in den Cisco Validated Designs for FlexPod Found "Hier".

"Weiter: Terraform Cloud Integration mit ICO-Voraussetzung."

Terraform Cloud Integration mit ICO-Voraussetzung

"Früher: Konfiguration von Cisco Intersight."

Prozedur 1: Cisco Intersight und Terraform Cloud verbinden

1. Mit den relevanten Terraform Cloud-Kontodetails können Sie ein Terraform-Cloud-Ziel anfordern oder erstellen.
2. Erstellen eines Terraform Cloud-Agent-Ziels für Private Clouds, damit Kunden den Agent im Datacenter installieren und die Kommunikation mit Terraform Cloud ermöglichen können

   Weitere Informationen finden Sie unter "Dieser Link".

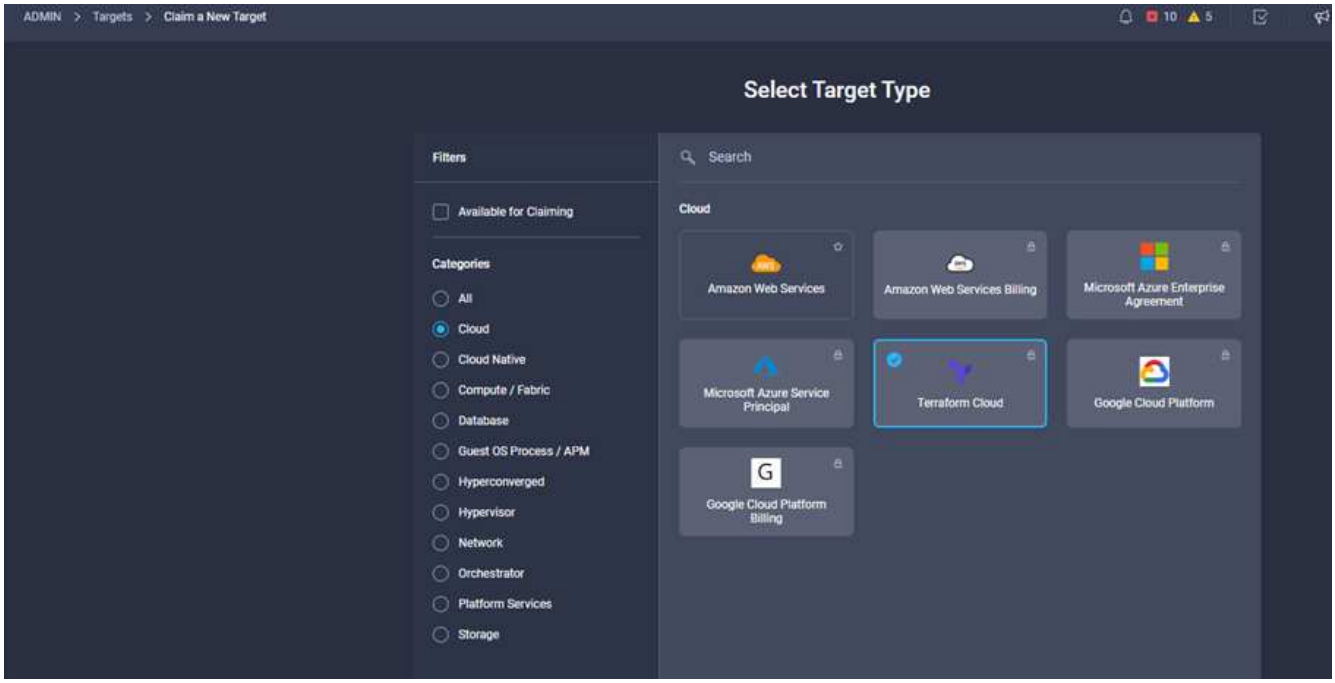
Verfahren 2: Benutzer-Token generieren

Beim Hinzufügen eines Ziels für Terraform Cloud müssen Sie auf der Terraform Cloud-Einstellungsseite den Benutzernamen und das API-Token bereitstellen.

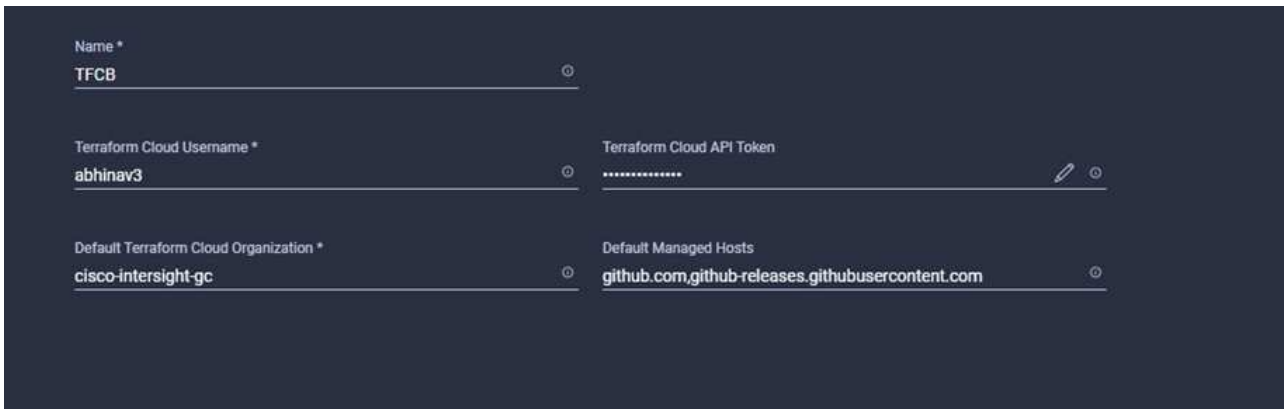
1. Melden Sie sich bei Terraform Cloud an und gehen Sie zu **Benutzer-Token**: "https://app.terraform.io/app/settings/tokens".
2. Klicken Sie auf **Erstellen Sie ein neues API-Token**.
3. Weisen Sie einen Namen zu merken und speichern Sie das Token an einem sicheren Ort.

Verfahren 3: Terraform Cloud-Ziel Beanspruchen

1. Melden Sie sich bei Intersight mit den Berechtigungen für Account Administrator, Geräteadministrator oder Gerätetechniker an.
2. Navigieren Sie zu **ADMIN > Ziele > ein neues Ziel anfordern**.
3. Klicken Sie in **Categories** auf **Cloud**.
4. Klicken Sie auf **Terraform Cloud** und klicken Sie auf **Start**.



5. Geben Sie einen Namen für das Ziel, Ihren Benutzernamen für die Terraform Cloud, das API-Token und eine Standardorganisation in Terraform Cloud ein, wie im folgenden Bild angezeigt.
6. Stellen Sie sicher, dass Sie im Feld **Default Managed Hosts** folgende Links zusammen mit anderen verwalteten Hosts hinzufügen:
   - github.com
   - github-releases.githubusercontent.com



Wenn alles korrekt eingegeben wurde, wird Ihr Terraform Cloud-Ziel im Abschnitt **Intersight Targets** angezeigt.

Verfahren 4: Terraform Cloud-Agenten hinzufügen

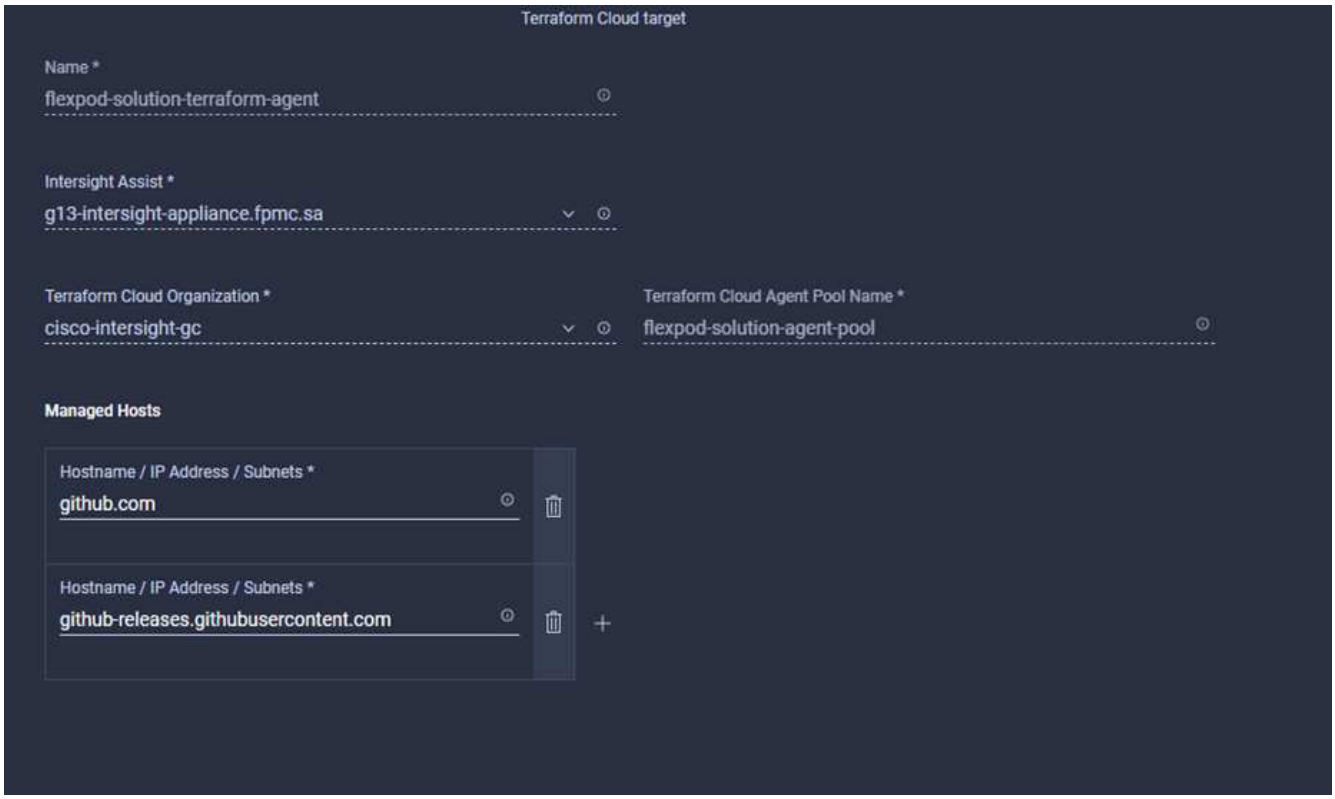
Voraussetzungen:

- Terraform Cloud-Ziel:
- Beanspruchte die Intersight-Unterstützung beim Intersight, bevor der Terraform Cloud Agent bereitgestellt wurde.

Sie können nur fünf Agenten für jeden Assist beanspruchen.

Nachdem Sie die Verbindung zu Terraform erstellt haben, müssen Sie einen Terraform Agent hochdrehen, um den Terraform-Code auszuführen.

1. Klicken Sie in der Dropdown-Liste Ihres Terraform Cloud-Ziels auf **Claim Terraform Cloud Agent**.
2. Geben Sie die Details für den Terraform Cloud-Agent ein. Im folgenden Screenshot sind die Konfigurationsdetails für Terraform Agent aufgeführt.



Sie können alle Terraform Agent-Eigenschaften aktualisieren. Wenn sich das Ziel im Status **nicht verbunden** befindet und sich noch nie im Status **verbunden** befindet, wurde für den Terraform-Agent kein Token generiert.

Nachdem die Agentenvalidierung erfolgreich war und ein Agententoken generiert wurde, können Sie die Organisation und/oder den Agentenpool nicht neu konfigurieren. Die erfolgreiche Bereitstellung eines Terraform-Agenten wird durch den Status **Connected** gekennzeichnet.

Nachdem Sie die Terraform Cloud-Integration aktiviert und beansprucht haben, können Sie einen oder mehrere Terraform Cloud-Agenten im Cisco Intersight Assist implementieren. Der Terraform Cloud-Agent wird als untergeordnetes Ziel des Terraform Cloud-Ziels modelliert. Wenn Sie das Agentenziel anfordern, wird eine Meldung angezeigt, die angibt, dass der Zielanspruch im Gange ist.

Nach einigen Sekunden wird das Ziel in den **Connected**-Status verschoben, und die Intersight-Plattform leitet HTTPS-Pakete vom Agenten zum Terraform Cloud-Gateway weiter.

Ihr Terraform Agent sollte ordnungsgemäß beantragt werden und unter Zielwerten als **verbunden** angezeigt werden.

"Als Nächstes konfigurieren Sie den Public Cloud-Service-Provider."

Konfigurieren Sie den Public Cloud-Service-Provider

"Früher: Terraform Cloud Integration mit ICO-Voraussetzung."

Verfahren 1: Zugriff auf NetApp Cloud Manager

Um Zugriff auf NetApp Cloud Manager und andere Cloud-Services zu erhalten, müssen Sie sich anmelden "NetApp Cloud Central".

Klicken Sie zum Einrichten von Workspaces und Benutzern im Cloud Central Konto auf "Hier".

Verfahren 2: Anschluss Einsetzen

Informationen zum Bereitstellen von Connector in Google Cloud finden Sie hier "Verlinken".

"Der nächste Schritt: Automatisierte Implementierung von Hybrid Cloud NetApp Storage."

Automatisierte Implementierung von NetApp Hybrid Cloud Storage

"Früher: Public Cloud-Service-Provider konfigurieren."

Google Cloud

Sie müssen zunächst APIs aktivieren und ein Service-Konto erstellen, über das Cloud Manager Berechtigungen für die Implementierung und das Management von Cloud Volumes ONTAP-Systemen erhält, die sich im selben Projekt wie der Connector oder verschiedene Projekte befinden.

Bevor Sie einen Konnektor in einem Google Cloud-Projekt bereitstellen, stellen Sie sicher, dass der Connector nicht auf Ihrem Gelände oder in einem anderen Cloud-Anbieter läuft.

Vor der Bereitstellung eines Connectors direkt aus Cloud Manager müssen zwei Berechtigungssätze vorhanden sein:

- Sie müssen Connector mit einem Google-Konto bereitstellen, das über Berechtigungen zum Starten der Connector-VM-Instanz von Cloud Manager verfügt.
- Bei der Bereitstellung von Connector werden Sie aufgefordert, die VM-Instanz auszuwählen. Cloud Manager erhält Berechtigungen vom Service-Konto, um Cloud Volumes ONTAP Systeme in Ihrem Auftrag zu erstellen und zu managen. Berechtigungen werden durch Hinzufügen einer benutzerdefinierten Rolle an das Dienstkonto bereitgestellt.Sie müssen zwei YAML-Dateien einrichten, die die erforderlichen Berechtigungen für den Benutzer und das Dienstkonto enthalten. Verwendung erfahren "Die YAML-Dateien zum Einrichten von Berechtigungen" Hier.

Siehe "Dieses detaillierte Video" Für alle erforderlichen Voraussetzungen.

Cloud Volumes ONTAP Bereitstellungsmodi und Architektur

Cloud Volumes ONTAP ist in Google Cloud als Single-Node-System und als HA-Paar von Nodes erhältlich. Je nach Anforderungen können wir den Cloud Volumes ONTAP-Implementierungsmodus auswählen. Ein Upgrade eines Single Node-Systems auf ein HA-Paar wird nicht unterstützt. Wenn Sie zwischen einem Single-Node-System und einem HA-Paar wechseln möchten, müssen Sie ein neues System implementieren und Daten vom bestehenden System auf das neue System replizieren.

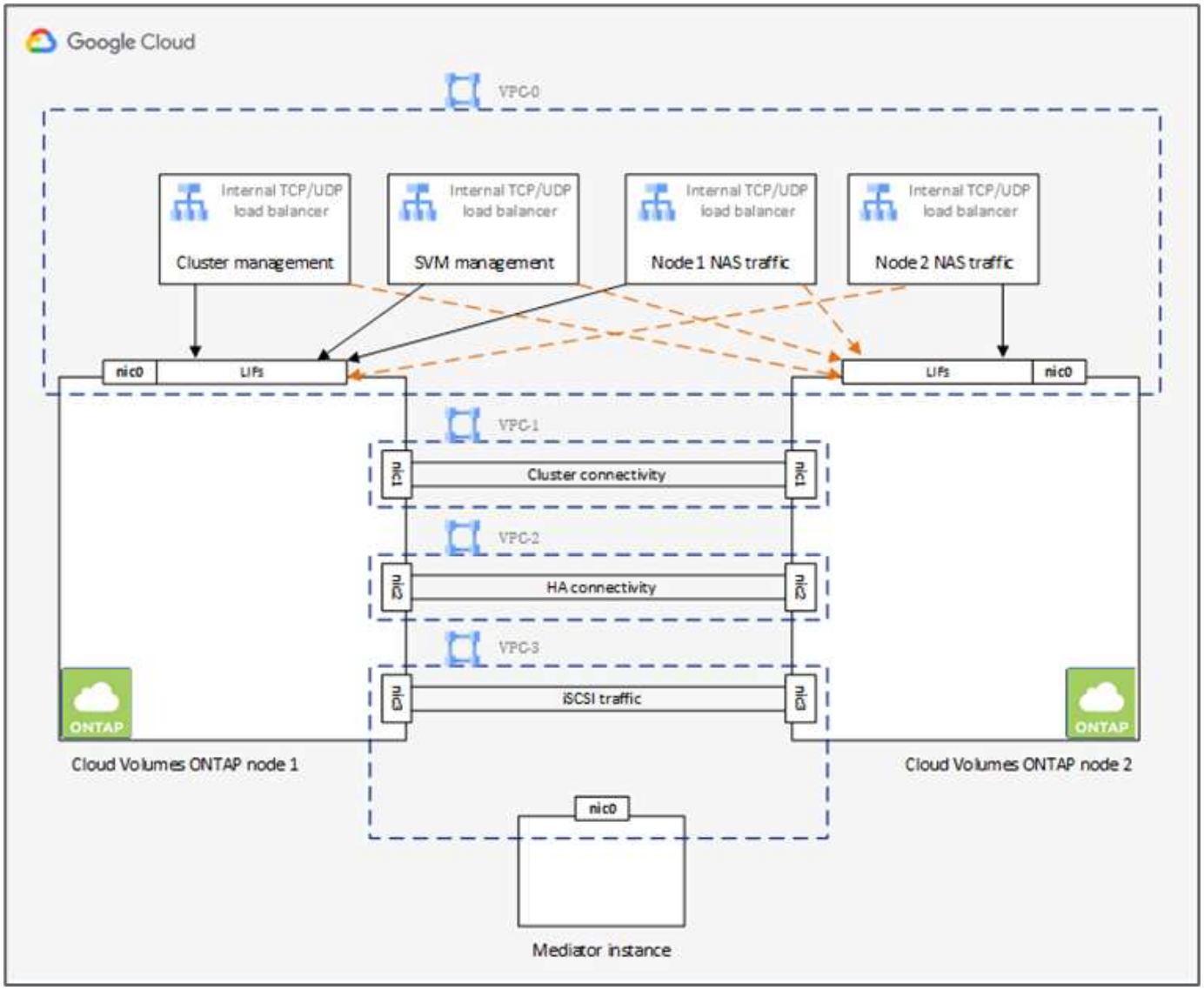
Hochverfügbare Cloud Volumes ONTAP in Google Cloud

Google Cloud unterstützt die Implementierung von Ressourcen über mehrere geografische Regionen und Zonen innerhalb einer Region hinweg. Die HA-Bereitstellung besteht aus zwei ONTAP-Knoten, die leistungsfähige Maschinentypen nach dem n1-Standard oder n2-Standard verwenden, die in Google Cloud verfügbar sind. Die Daten werden synchron zwischen den beiden Cloud Volumes ONTAP Nodes repliziert, um bei einem Ausfall Verfügbarkeit sicherzustellen. FÜR DIE HA-Implementierung von Cloud Volumes ONTAP sind vier VPCs und ein privates Subnetz in jeder VPC erforderlich. Die Subnetze in den vier VPCs sollten mit nicht überlappenden CIDR-Bereichen bereitgestellt werden.

Die vier VPCs werden für die folgenden Zwecke verwendet:

- VPC 0 ermöglicht die eingehende Kommunikation zu Daten und Cloud Volumes ONTAP-Nodes.
- Die VPC 1 ermöglicht die Cluster-Konnektivität zwischen Cloud Volumes ONTAP-Nodes.
- VPC 2 ermöglicht die nicht-flüchtige RAM (NVRAM)-Replizierung zwischen Nodes.
- VPC 3 wird für die Konnektivität zur HA-Mediator-Instanz und für Festplatten-Replizierungsdatenverkehr bei Node-Rebuilds verwendet.

Die folgende Abbildung zeigt eine hochverfügbare Cloud Volumes ONTAP in Goggle Cloud.



Weitere Informationen finden Sie unter "Dieser Link".

Informationen zu den Netzwerkanforderungen für Cloud Volumes ONTAP in Google Cloud finden Sie unter "Dieser Link".

Weitere Informationen zum Daten-Tiering finden Sie unter "Dieser Link".

Voraussetzungen für die Umgebung einrichten

Die automatisierte Erstellung von Cloud Volumes ONTAP-Clustern, die SnapMirror Konfiguration zwischen einem On-Premises-Volume und einem Cloud-Volume, die Erstellung eines Cloud-Volumes usw. werden mit der Terraform-Konfiguration durchgeführt. Diese Terraform-Konfigurationen werden auf einem Terraform Cloud for Business-Konto gehostet. Mithilfe von Intersight Cloud Orchestrator koordinieren Sie Aufgaben wie das Erstellen eines Arbeitsbereichs in einem Terraform Cloud for Business-Konto, fügen alle erforderlichen Variablen zum Workspace hinzu, führen einen Terraform Plan aus usw.

Für diese Automatisierungs- und Orchestrierungsaufgaben sind einige Anforderungen und Daten erforderlich, wie in den folgenden Abschnitten beschrieben.

GitHub Repository

Sie benötigen ein GitHub-Konto, um Ihren Terraform-Code zu hosten. Intersight Orchestrator erstellt im Terraform Cloud for Business-Konto einen neuen Arbeitsbereich. Dieser Arbeitsbereich ist mit einem Workflow zur Versionskontrolle konfiguriert. Dazu müssen Sie die Terraform-Konfiguration in einem GitHub-Repository belassen und bei der Erstellung des Arbeitsbereichs als Input bereitstellen.

"Dieser GitHub-Link" Stellt die Terraform-Konfiguration mit verschiedenen Ressourcen zur Verfügung Sie können dieses Repository anstellen und eine Kopie in Ihrem GitHub-Konto erstellen.

In diesem Repository `provider.tf` Hat die Definition für den erforderlichen Terraform-Provider definiert. Terraform-Provider für NetApp Cloud Manager wird verwendet.

`variables.tf` Enthält alle variablen Erklärungen. Der Wert für diese Variablen wird als Workflow-Eingabe des Intersight Cloud Orchestrator eingegeben. So können Werte bequem an einen Arbeitsbereich übergeben und die Terraform-Konfiguration ausgeführt werden.

`resources.tf` Definition der verschiedenen Ressourcen, die erforderlich sind, um eine lokale ONTAP der Arbeitsumgebung hinzuzufügen, ein Cloud Volumes ONTAP Cluster mit einzelnen Nodes in Google Cloud zu erstellen, eine SnapMirror Beziehung zwischen On-Premises und Cloud Volumes ONTAP herzustellen, ein Cloud Volume in Cloud Volumes ONTAP zu erstellen usw.

In diesem Repository:

- `provider.tf` Hat NetApp Cloud Manager als Definition für den erforderlichen Terraform-Provider eingesetzt.
- `variables.tf` Enthält die variablen Deklarationen, die als Input für den Intersight Cloud Orchestrator Workflow verwendet werden. So können Werte bequem an den Arbeitsbereich übergeben und die Terraform-Konfiguration ausgeführt werden.
- `resources.tf` Definition verschiedener Ressourcen zum Hinzufügen einer lokalen ONTAP zur Arbeitsumgebung, Erstellung eines Cloud Volumes ONTAP Clusters mit nur einem Node in Google Cloud, Festlegung einer SnapMirror Beziehung zwischen On-Premises und Cloud Volumes ONTAP, Erstellung eines Cloud Volumes in Cloud Volumes ONTAP usw.

Sie können einen zusätzlichen Ressourcen-Block hinzufügen, um mehrere Volumes auf Cloud Volumes

ONTAP zu erstellen, oder die Anzahl der Nutzung oder `for_each` Terraform-Konstrukte.

Damit Terraform-Arbeitsbereiche, -Module und -Richtlinien mit Terraform-Konfigurationen an Git-Repositorys mit Terraform-Konfigurationen angeschlossen werden können, benötigt Terraform Cloud Zugriff auf Ihren GitHub Repo.

Fügen Sie einen Client hinzu, und die OAuth Token-ID des Clients wird als eine der Workflow-Eingaben des Intersight Cloud Orchestrator verwendet.

1. Melden Sie sich bei Ihrem Terraform Cloud for Business-Konto an. Navigieren Sie zu **Einstellungen > Provider**.
2. Klicken Sie auf **VCS-Anbieter hinzufügen**.
3. Wählen Sie Ihre Version aus.
4. Befolgen Sie die Schritte unter **Anbieter einrichten**.
5. Sie sehen den hinzugefügten Client in **VCS Providers**. Notieren Sie sich die OAuth Token-ID.

Token für den NetApp Cloud Manager-API-Betrieb aktualisieren

Zusätzlich zur Webbrowser-Schnittstelle verfügt Cloud Manager über eine REST-API, die Softwareentwicklern über die SaaS-Schnittstelle direkten Zugriff auf die Funktionen von Cloud Manager bietet. Der Cloud Manager Service besteht aus mehreren Kernkomponenten, die gemeinsam eine erweiterbare Entwicklungsplattform bilden. Mit dem Token zum Aktualisieren können Sie für jeden API-Aufruf Access Token generieren, die Sie der Autorisierungs-Kopfzeile hinzufügen.

Ohne direkten Aufruf einer API verwendet der netapp-Cloud-Manager-Provider ein Aktualisierungs-Token und übersetzt die Terraform-Ressourcen in die entsprechenden API-Aufrufe. Sie müssen ein Aktualisierungs-Token für den NetApp Cloud Manager-API-Betrieb von generieren "NetApp Cloud Central".

Sie benötigen die Client-ID des Cloud Manager Connectors, um Ressourcen auf Cloud Manager zu erstellen, z. B. das Erstellen eines Cloud Volumes ONTAP Clusters, die Konfiguration von SnapMirror usw.

1. Melden Sie sich bei Cloud Manager an: "https://cloudmanager.netapp.com/".
2. Klicken Sie Auf **Connector**.
3. Klicken Sie Auf **Connectors Verwalten**.
4. Klicken Sie auf die Ellipsen und kopieren Sie die Konnektor-ID.

Cisco Intersight Cloud Orchestrator Workflow entwickeln

Cisco Intersight Cloud Orchestrator ist in Cisco Intersight verfügbar, wenn:

- Sie haben die Intersight Premier-Lizenz installiert.
- Sie sind Account-Administrator, Storage-Administrator, Virtualisierungsadministrator oder Server-Administrator und haben Ihnen mindestens einen Server zugewiesen.

Workflow Designer

Mit Workflow Designer können Sie neue Workflows (sowie Aufgaben und Datentypen) erstellen und vorhandene Workflows bearbeiten, um Ziele in Cisco Intersight zu verwalten.

Um den Workflow Designer zu starten, gehen Sie zu **Orchestrierung > Workflows**. In einem Dashboard werden unter den Registerkarten **Meine Workflows**, **Beispiel-Workflows** und **Alle Workflows** folgende

Details angezeigt:

- Validierungsstatus
- Letzter Ausführungsstatus
- Top Workflows nach Anzahl der Ausführung
- Oberste Workflow-Kategorien
- Anzahl systemdefinierter Workflows
- Top Workflows nach Zielen

Über das Dashboard können Sie eine Registerkarte erstellen, bearbeiten, klonen oder löschen. Um eine eigene benutzerdefinierte Ansichtsregisterkarte zu erstellen, klicken Sie auf **+**, geben Sie einen Namen an und wählen Sie dann die gewünschten Parameter aus, die in den Spalten, Tag-Spalten und Widgets angezeigt werden sollen. Sie können einen Tab umbenennen, wenn er nicht über ein **Lock**-Symbol verfügt.

Unter dem Dashboard befindet sich eine tabellarische Liste von Workflows mit den folgenden Informationen:

- Anzeigename
- Beschreibung
- Systemdefiniert
- Standardversion
- Ausführungen
- Letzter Ausführungsstatus
- Validierungsstatus
- Letztes Update
- Organisation

In der Spalte Aktionen können Sie die folgenden Aktionen ausführen:

- **Ausführen.** führt den Workflow aus.
- **Verlauf.** zeigt Workflow-Ausführungsverlauf an.
- **Versionen verwalten.** Erstellen und Verwalten von Versionen für Workflows.
- **Löschen.** Löschen Sie einen Workflow.
- **Wiederholen.** Versuchen Sie einen fehlgeschlagenen Workflow erneut.

Workflow

Erstellen Sie einen Workflow, der aus den folgenden Schritten besteht:

- **Definieren eines Workflows.** Geben Sie den Anzeigenamen, die Beschreibung und andere wichtige Attribute an.
- **Definieren von Workflow-Eingängen und Workflow-Ausgaben.** Geben Sie an, welche Eingabeparameter für die Workflow-Ausführung obligatorisch sind, und welche Outputs bei erfolgreicher Ausführung generiert wurden
- **Workflow-Aufgaben hinzufügen.** Fügen Sie im Workflow Designer eine oder mehrere Workflow-Aufgaben hinzu, die für die Ausführung der Funktion des Workflows erforderlich sind.

- *Validieren Sie den Workflow. *Überprüfen Sie einen Workflow, um sicherzustellen, dass keine Fehler bei der Verbindung von ein- und Ausgängen der Aufgabe auftreten.

Erstellen von Workflows für lokalen FlexPod Storage

Informationen zur Konfiguration eines Workflows für lokalen FlexPod Storage finden Sie unter "Dieser Link".

"Weiter: DR-Workflow."

DR-Workflow

"Früher: Automatisierte Implementierung von Hybrid Cloud NetApp Storage."

Die Reihenfolge der Schritte ist wie folgt:

1. Definieren Sie den Workflow.
    - Erstellen Sie einen kurzen, benutzerfreundlichen Namen für den Workflow, z. B. Disaster Recovery Workflow.
2. Definieren Sie die Workflow-Eingabe. Die Eingaben, die wir für diesen Workflow machen, umfassen Folgendes:
    - Volume-Optionen (Volume-Name, Mount-Pfad)
    - Volume-Kapazität
    - Dem neuen Datenspeicher zugeordneten Datacenter
    - Cluster, auf dem der Datastore gehostet wird
    - Name für den neuen Datastore, der in vCenter erstellt werden soll
    - Geben Sie den Typ und die Version des neuen Datenspeichers ein
    - Name der Terraform-Organisation
    - Terraform-Workspace
    - Beschreibung des Terraform-Arbeitsbereichs
    - Variablen (Sensitiv und nicht-empfindlich) erforderlich, um die Terraform-Konfiguration auszuführen
    - Grund für den Start des Plans
3. Fügen Sie die Workflow-Aufgaben hinzu.

    Zu den Aufgaben im Zusammenhang mit den Vorgängen in FlexPod gehören:

    - Volume-Erstellung in FlexPod:
    - Fügen Sie eine Storage-Exportrichtlinie zum erstellten Volume hinzu.
    - Das neu erstellte Volume einem Datenspeicher in VMware vCenter zuordnen

      Die Aufgaben zum Erstellen des Cloud Volumes ONTAP-Clusters:

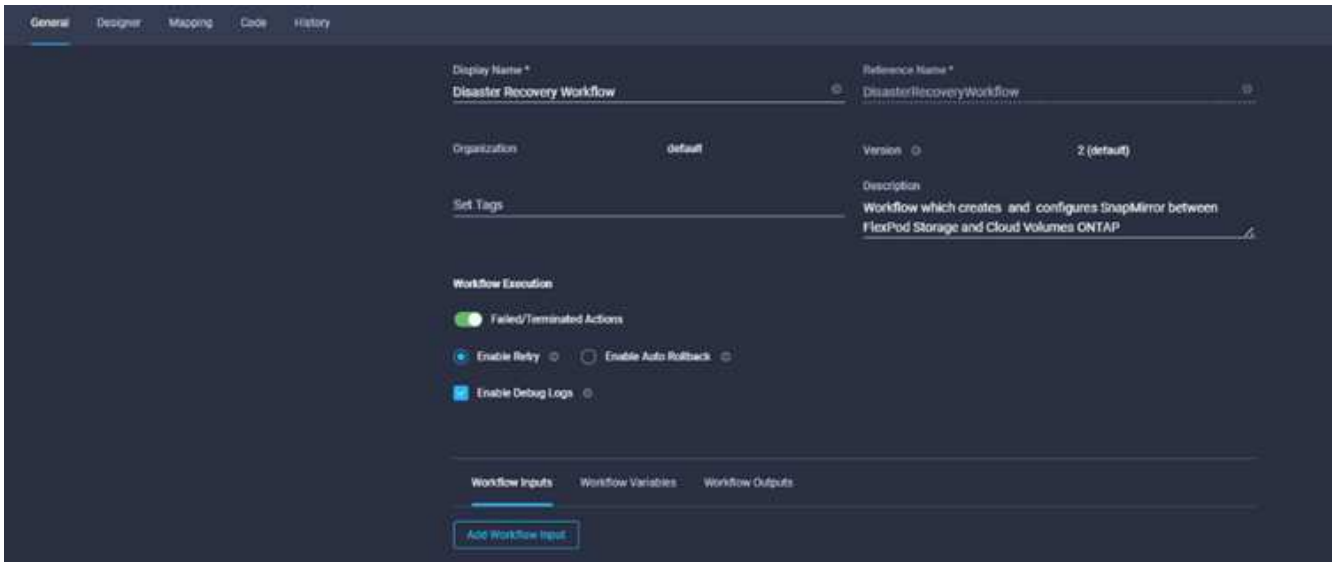
    - Terraform-Workspace hinzufügen
    - Terraform-Variablen hinzufügen
    - Terraform-sensible Variablen hinzufügen
    - Starten Sie den neuen Terraform-Plan

- Terraform-Lauf bestätigen

4. Validieren Sie den Workflow.

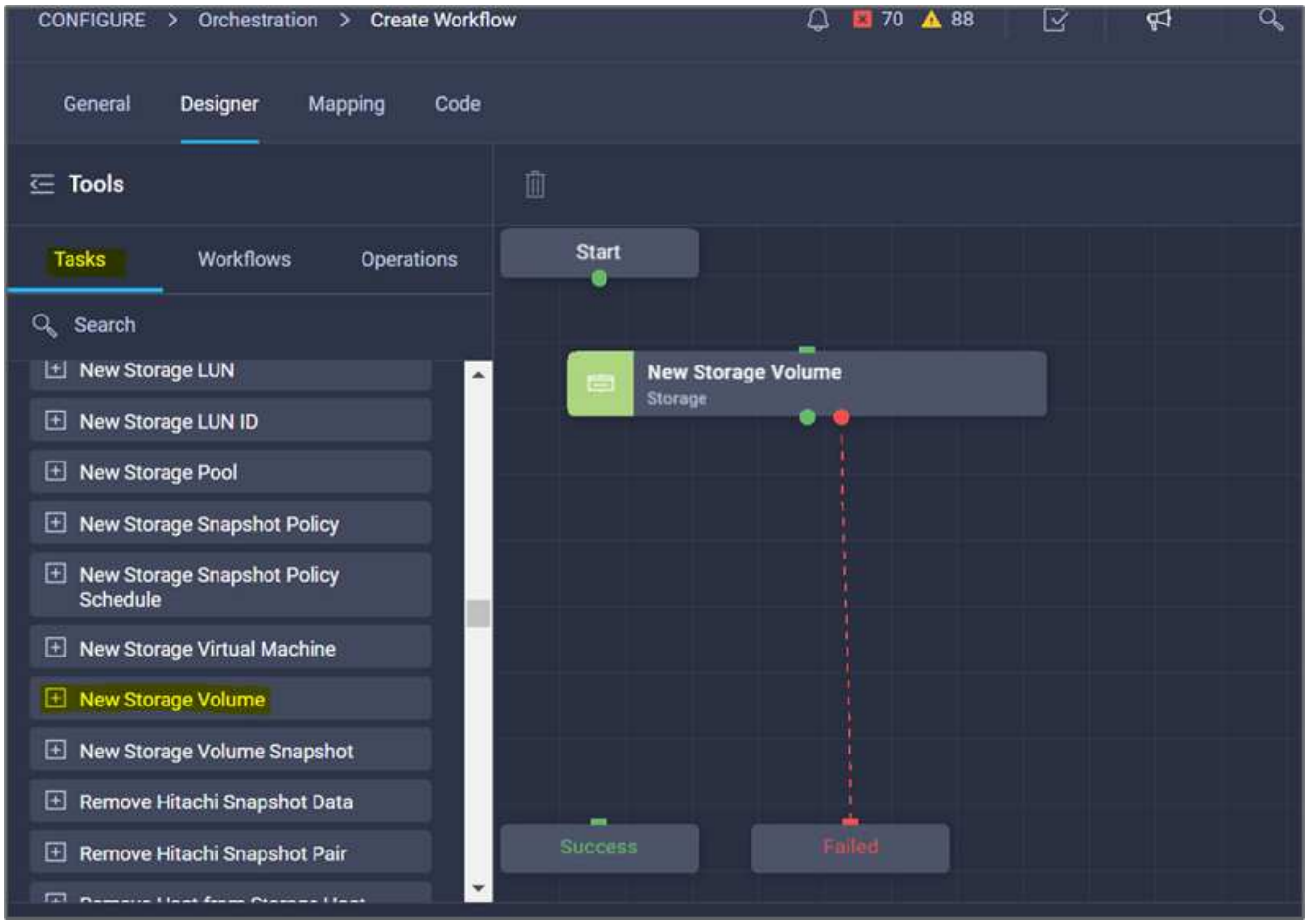
Verfahren 1: Erstellen Sie den Workflow

1. Klicken Sie im linken Navigationsbereich auf **Orchestration** und klicken Sie auf **Workflow erstellen**.
2. Auf der Registerkarte **Allgemein**:
   a. Geben Sie den Anzeigenamen an (Disaster Recovery Workflow).
   b. Wählen Sie die Organisation aus, legen Sie Tags fest und geben Sie eine Beschreibung ein.
3. Klicken Sie auf Speichern .

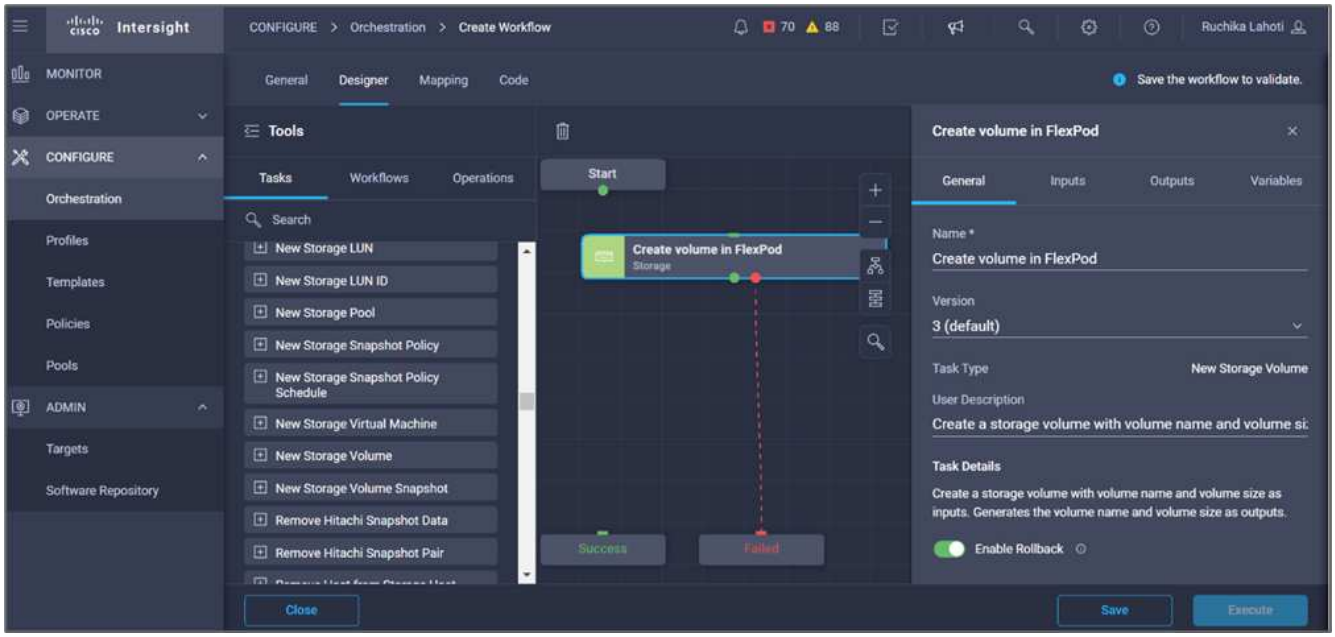


Verfahren 2. Erstellen Sie in FlexPod ein neues Volume

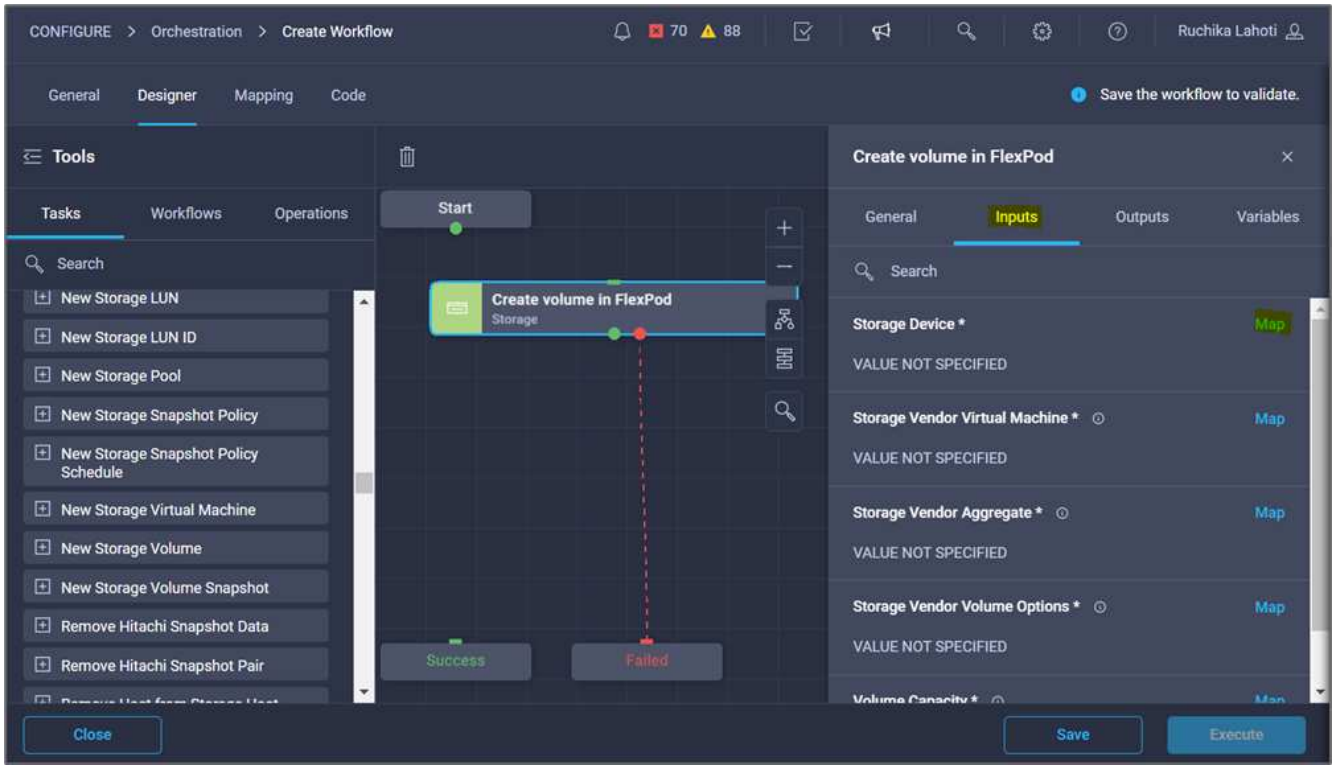
1. Gehen Sie zur Registerkarte **Designer** und klicken Sie im Abschnitt **Tools** auf **Tasks**.
2. Ziehen Sie die Aufgabe **Storage > New Storage Volume** aus dem Abschnitt **Tools** in den Bereich **Design**.
3. Klicken Sie Auf **Neues Speichervolume**.



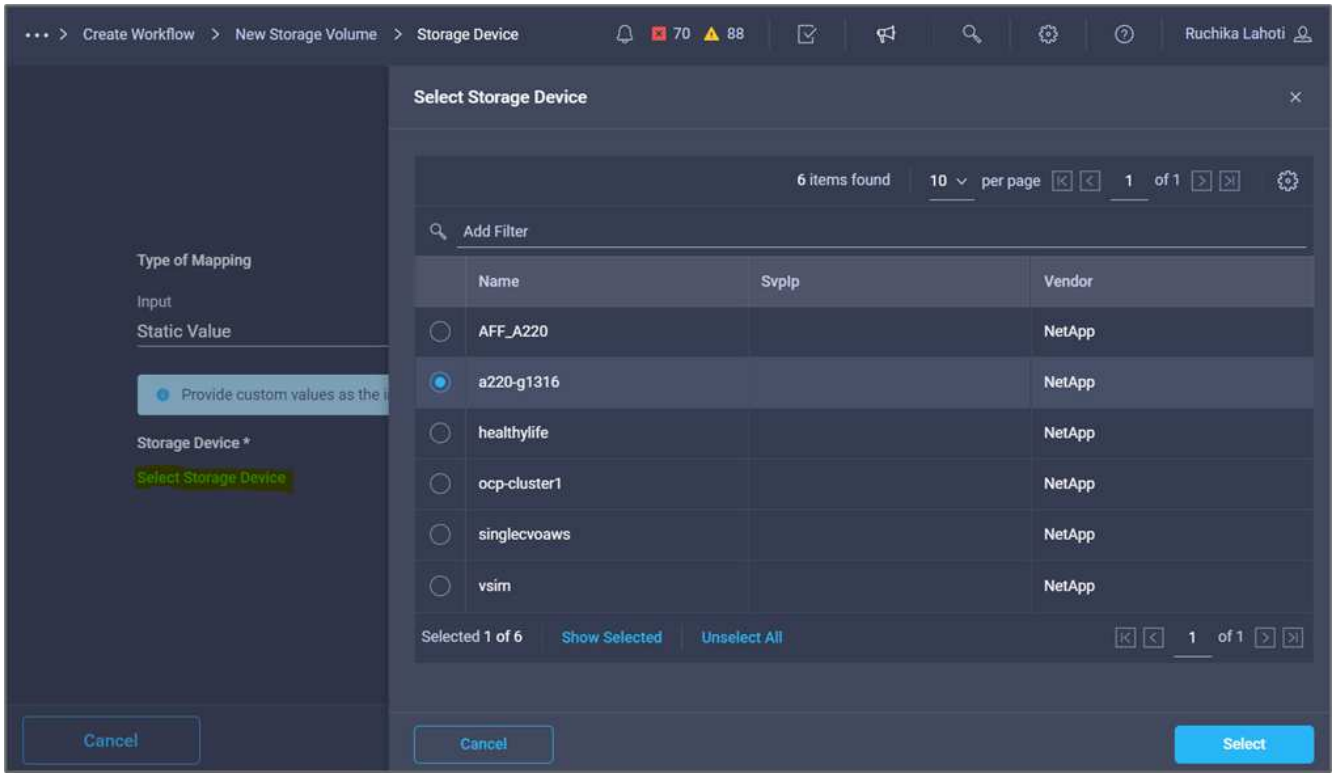
4. Klicken Sie im Bereich **Aufgabeneigenschaften** auf die Registerkarte **Allgemein**. Optional können Sie den Namen und die Beschreibung für diese Aufgabe ändern. In diesem Beispiel lautet der Name der Aufgabe **Volumen in FlexPod erstellen**.



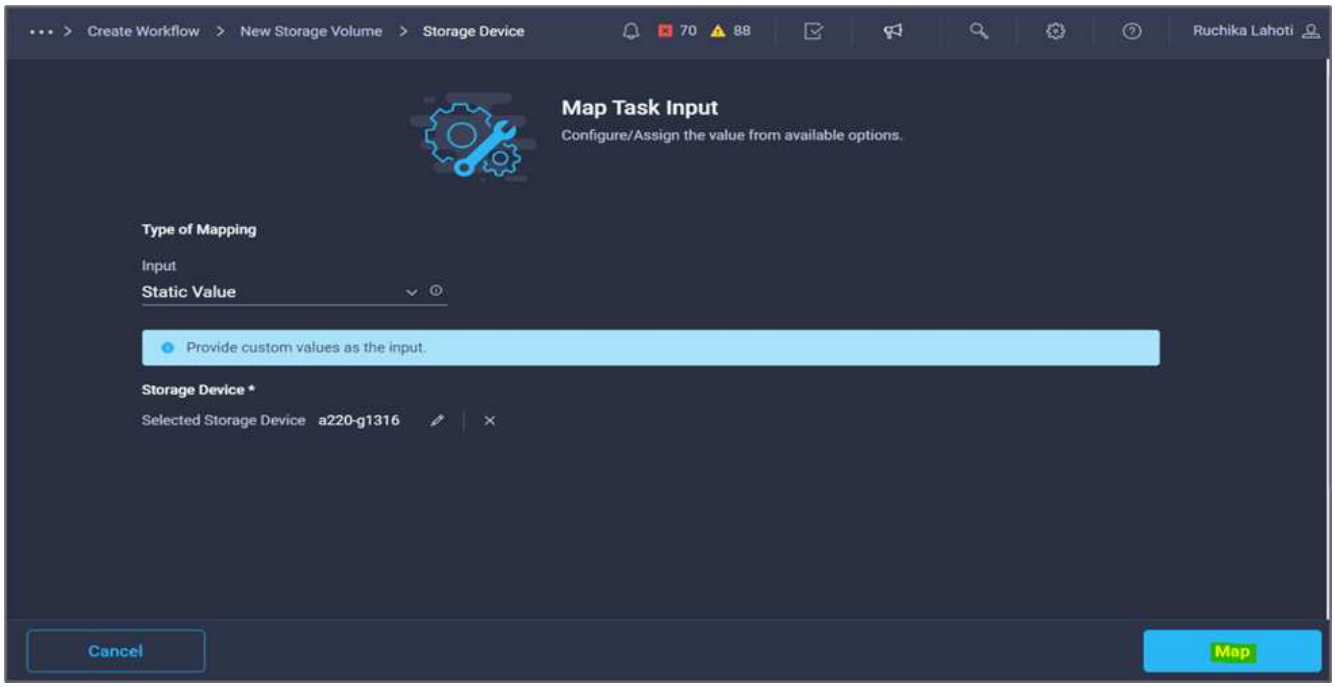
5. Klicken Sie im Bereich **Aufgabeneigenschaften** auf **Eingaben**.
6. Klicken Sie im Feld **Speichergerät** auf **Karte**.



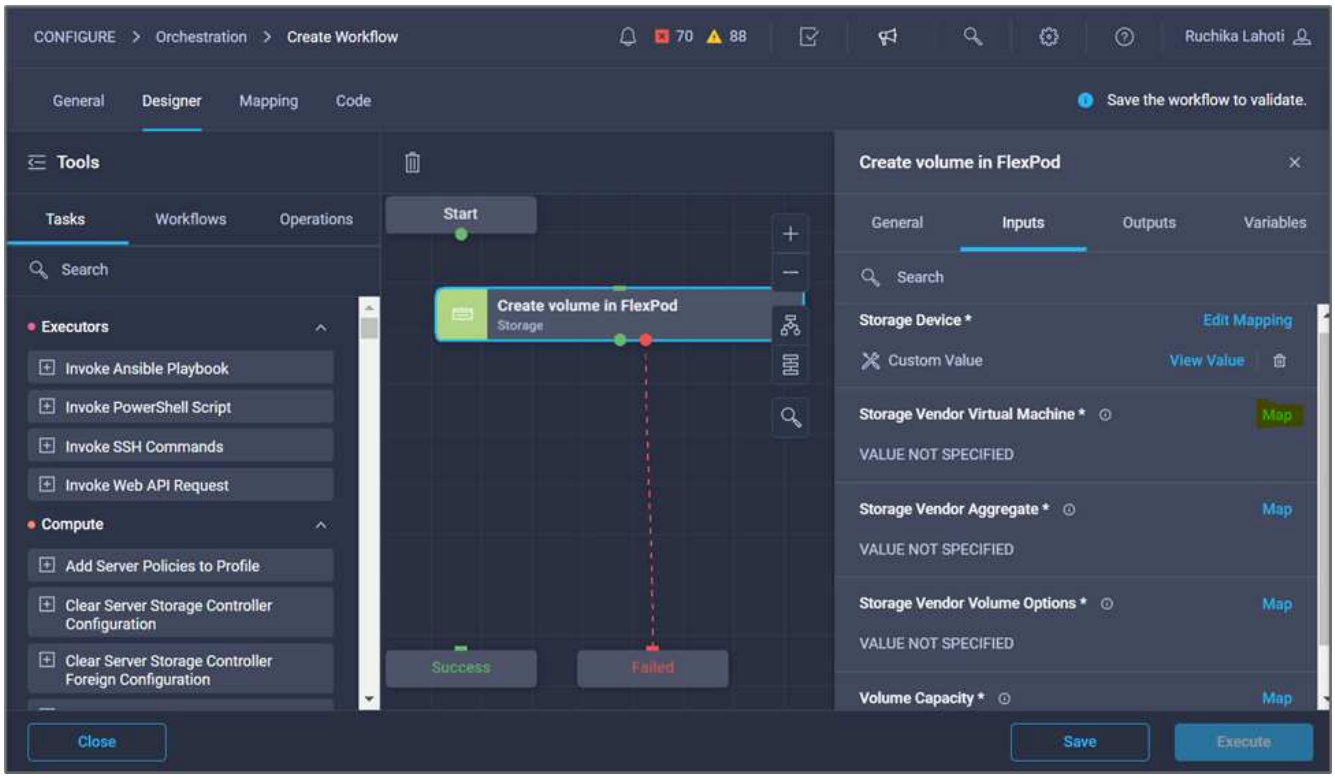
7. Wählen Sie **statischer Wert** und klicken Sie auf **Speichergerät auswählen**.
8. Klicken Sie auf das hinzugefügte Speicherziel und klicken Sie auf **Auswählen**.



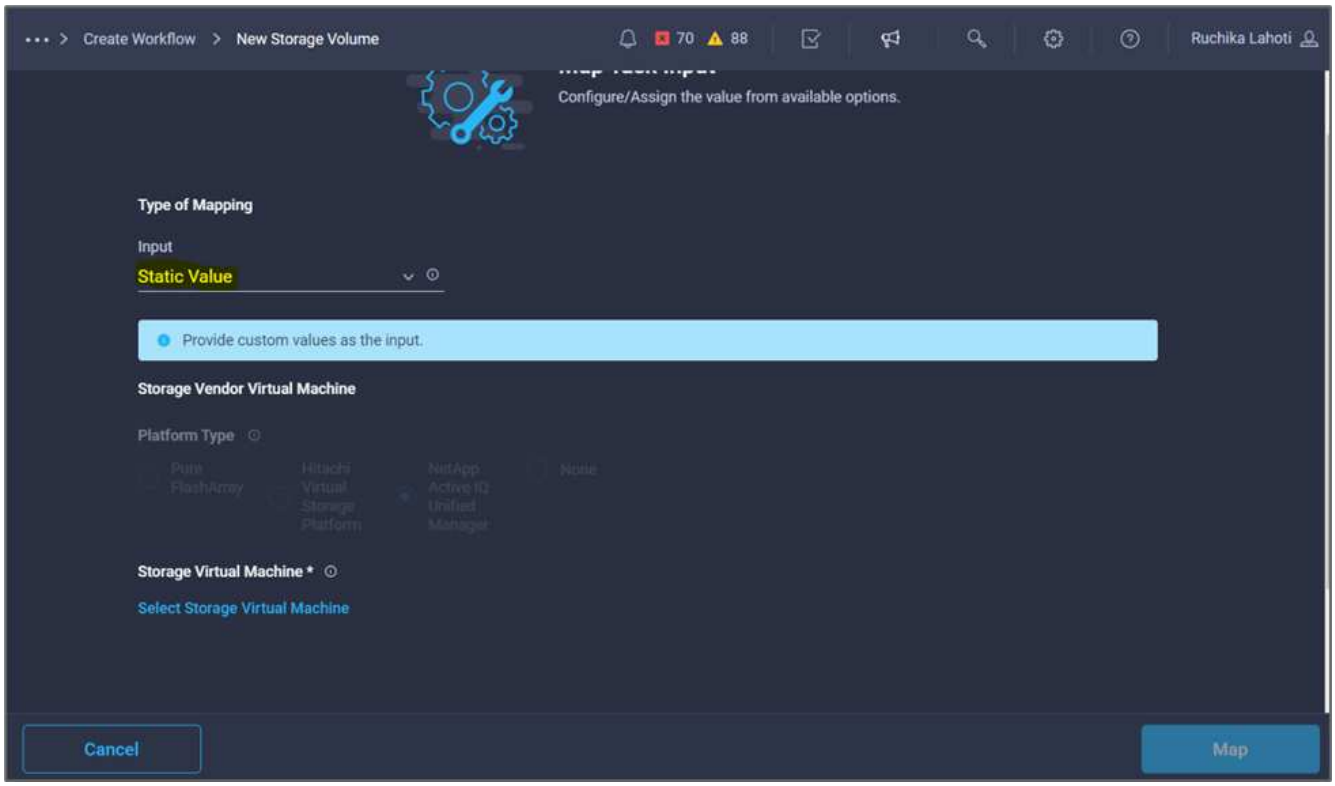
9. Klicken Sie Auf **Karte**.



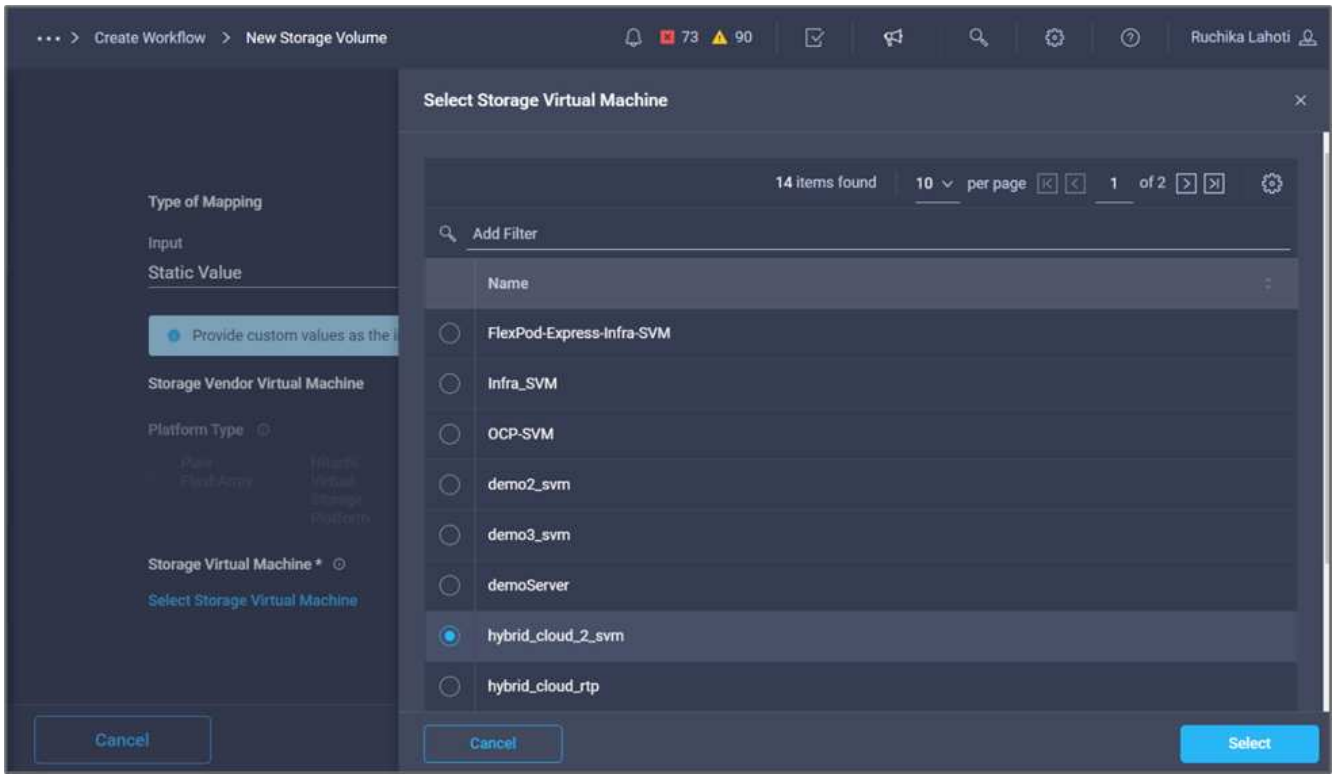
10. Klicken Sie im Feld **Storage Vendor Virtual Machine** auf **Map**.



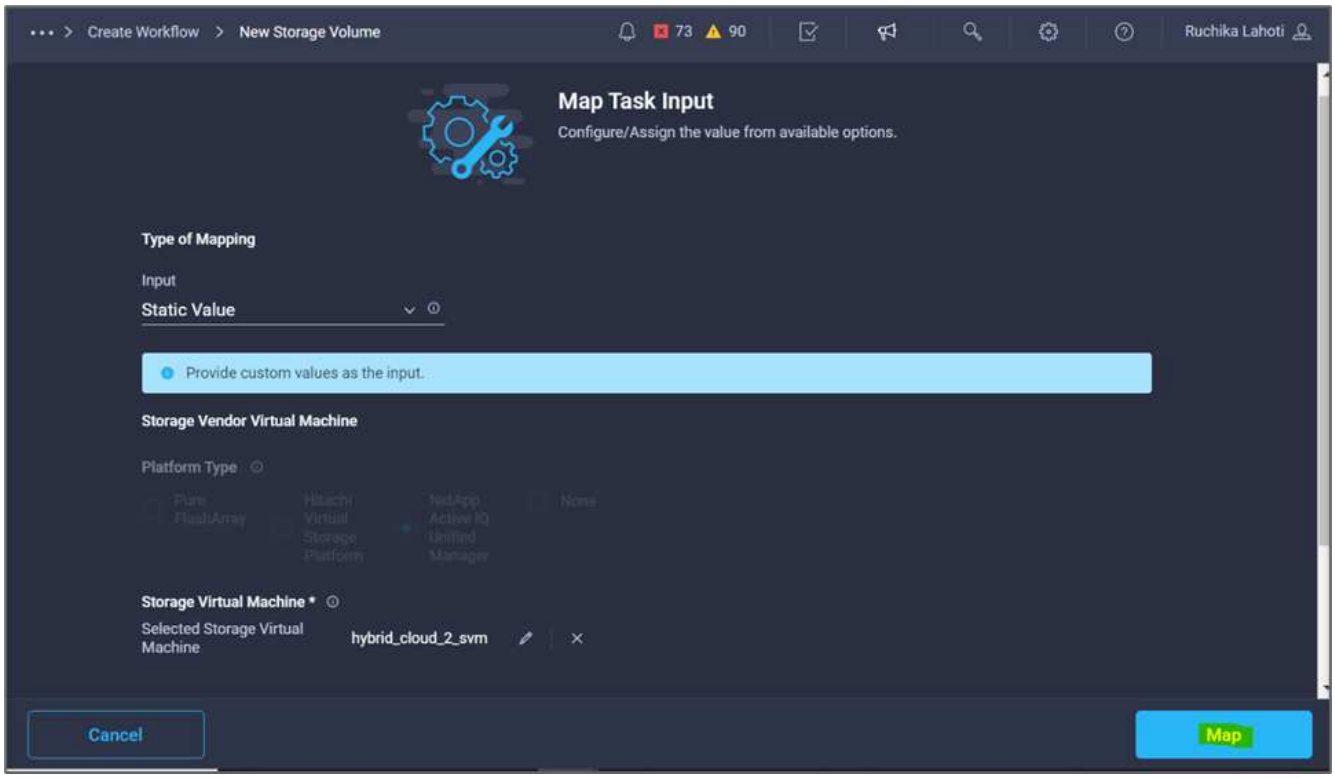
11. Wählen Sie **statischer Wert** und klicken Sie auf **Storage Virtual Machine auswählen**.



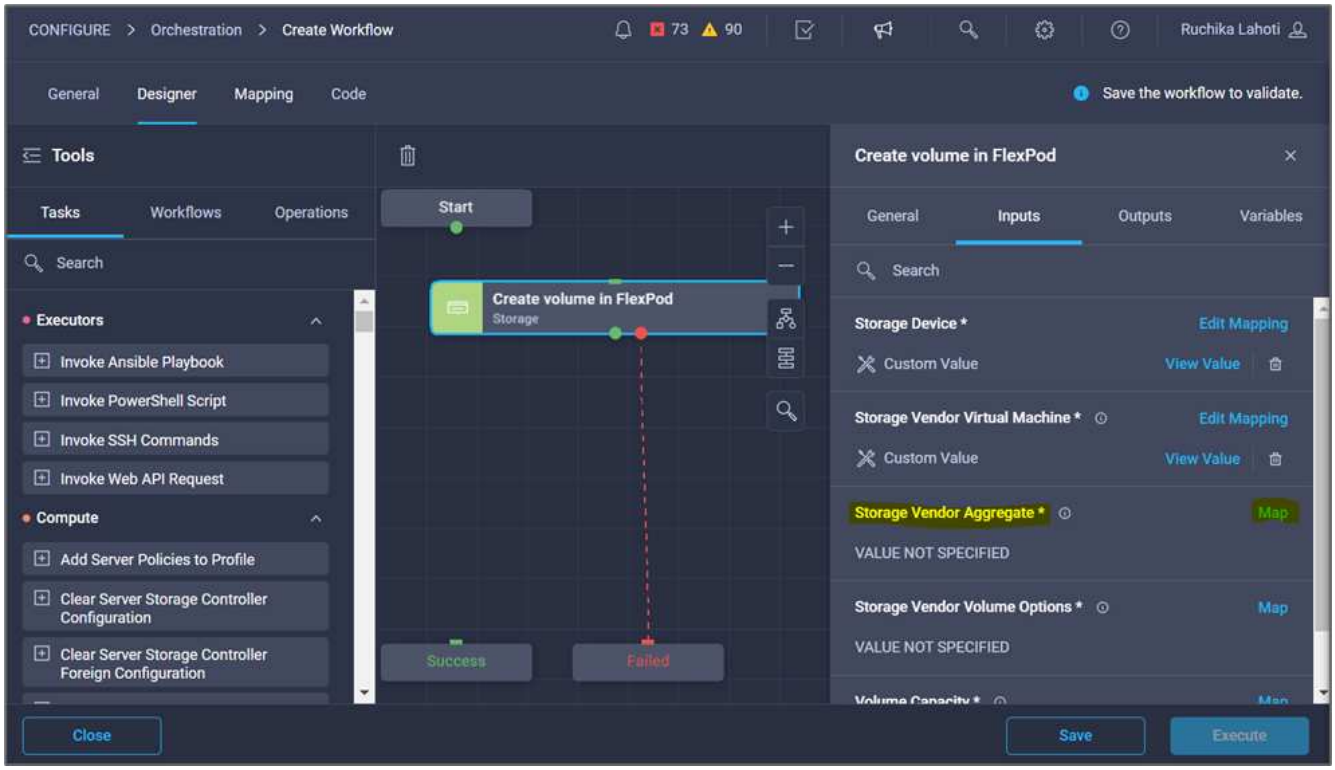
12. Wählen Sie die virtuelle Speichermaschine aus, auf der das Volume erstellt werden soll, und klicken Sie auf **Auswählen**.



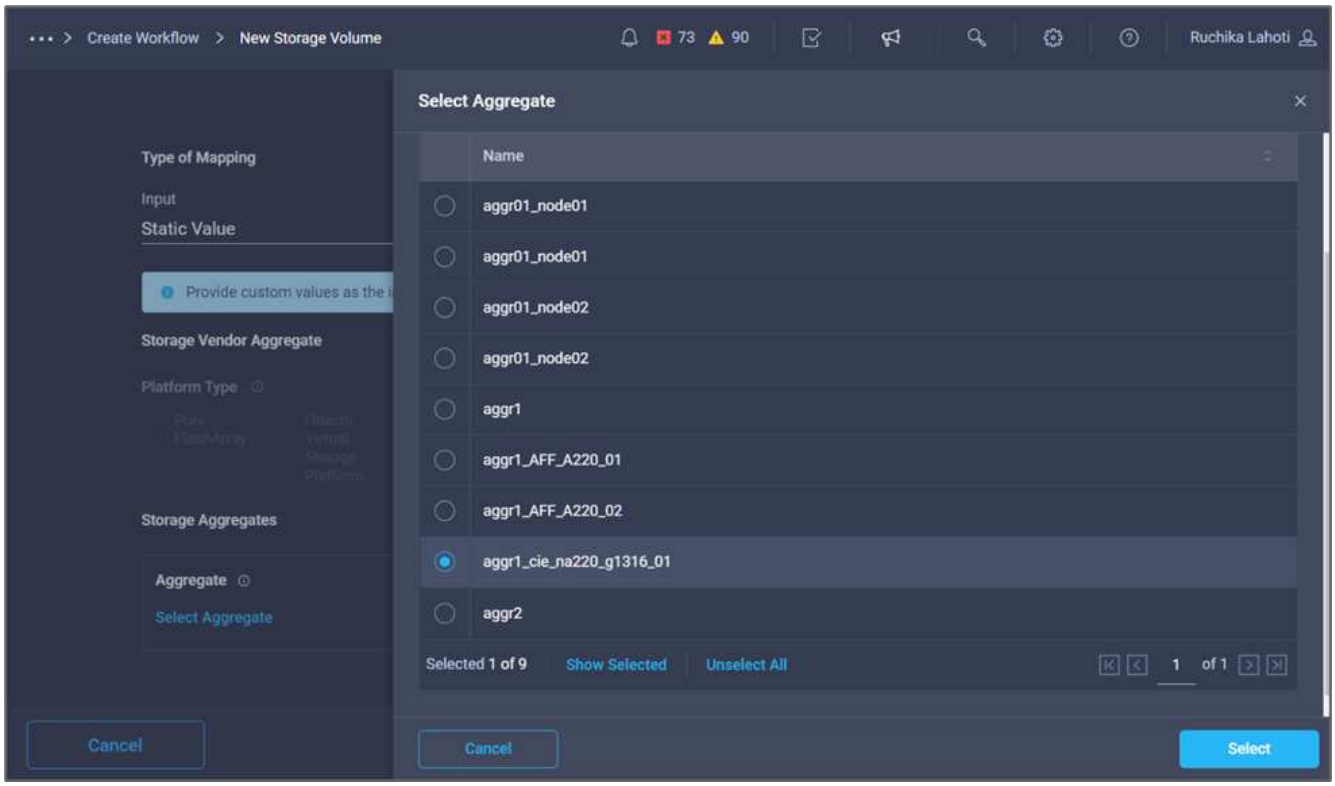
13. Klicken Sie Auf **Karte**.



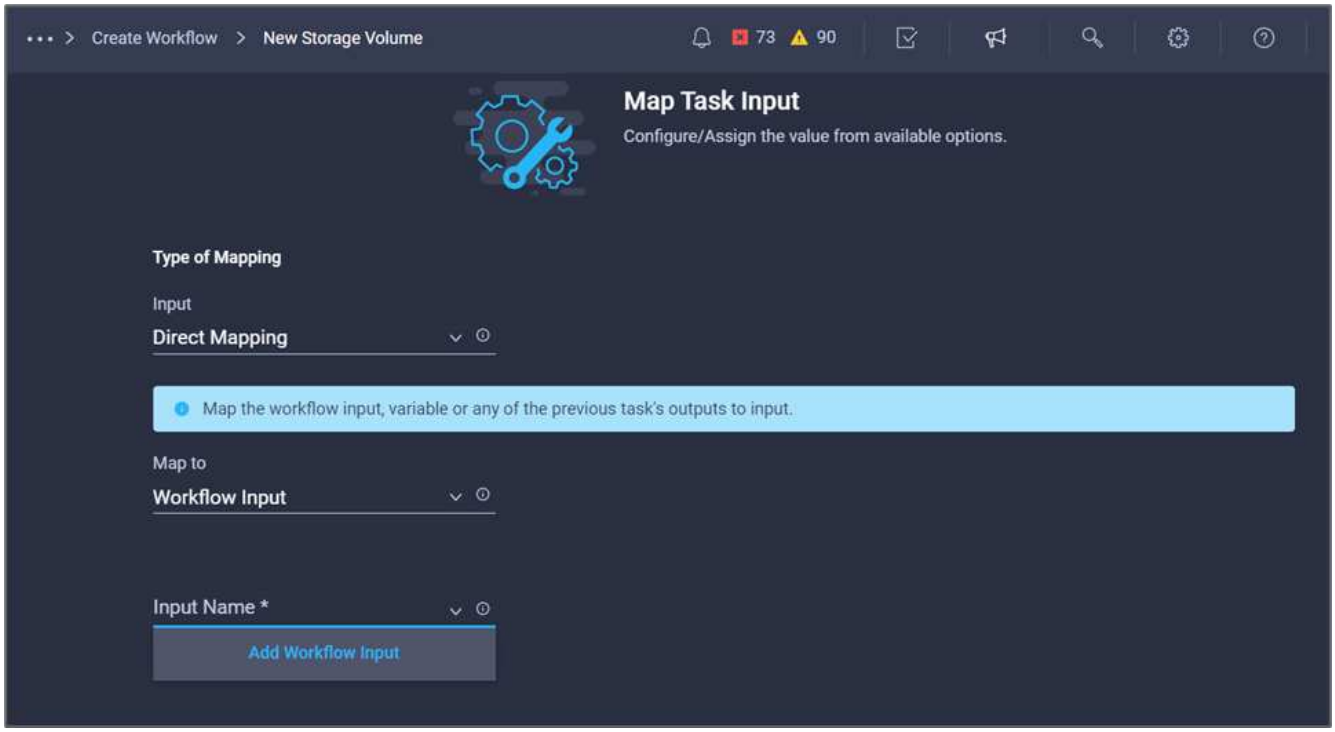
14. Klicken Sie im Feld **Storage Vendor Aggregate** auf **Map**.



15. Wählen Sie **statischer Wert** und klicken Sie auf **Storage-Aggregat auswählen**. Wählen Sie das Aggregat und klicken Sie auf **Auswählen**.



16. Klicken Sie Auf **Karte**.
17. Klicken Sie im Feld **Storage Vendor Volume Options** auf **Map**.
18. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Workflow-Eingabe**.



19. Führen Sie im Add Input Wizard die folgenden Schritte aus:
    a. Geben Sie einen Anzeigenamen und einen Referenznamen an (optional).
    b. Vergewissern Sie sich, dass **Storage Vendor Volume Options** für den **Typ** ausgewählt ist.

c. Klicken Sie auf **Standardwert festlegen und überschreiben**.

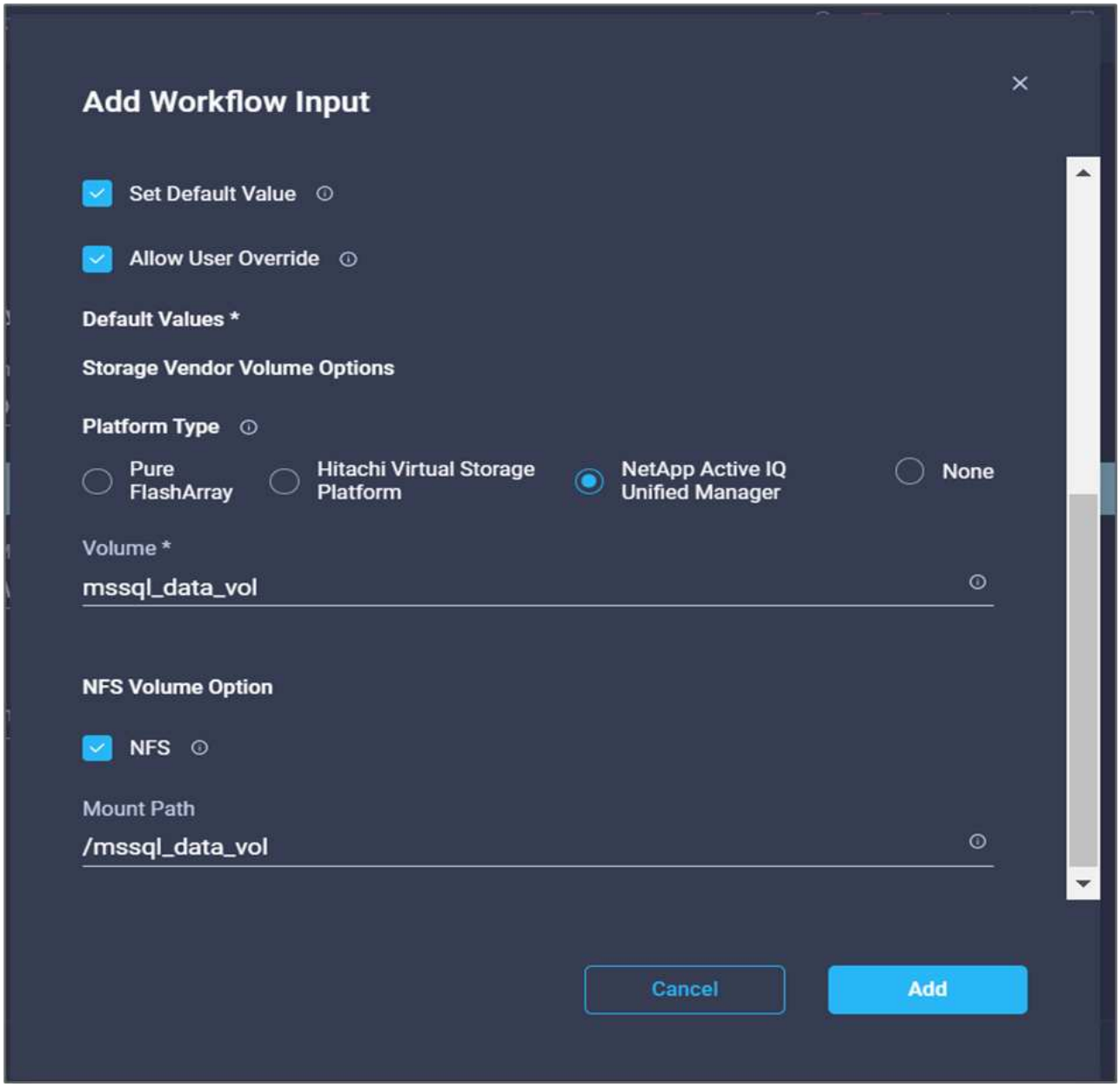
d. Klicken Sie Auf * Erforderlich*.

e. Stellen Sie den **Plattformtyp** auf **NetApp Active IQ Unified Manager** ein.

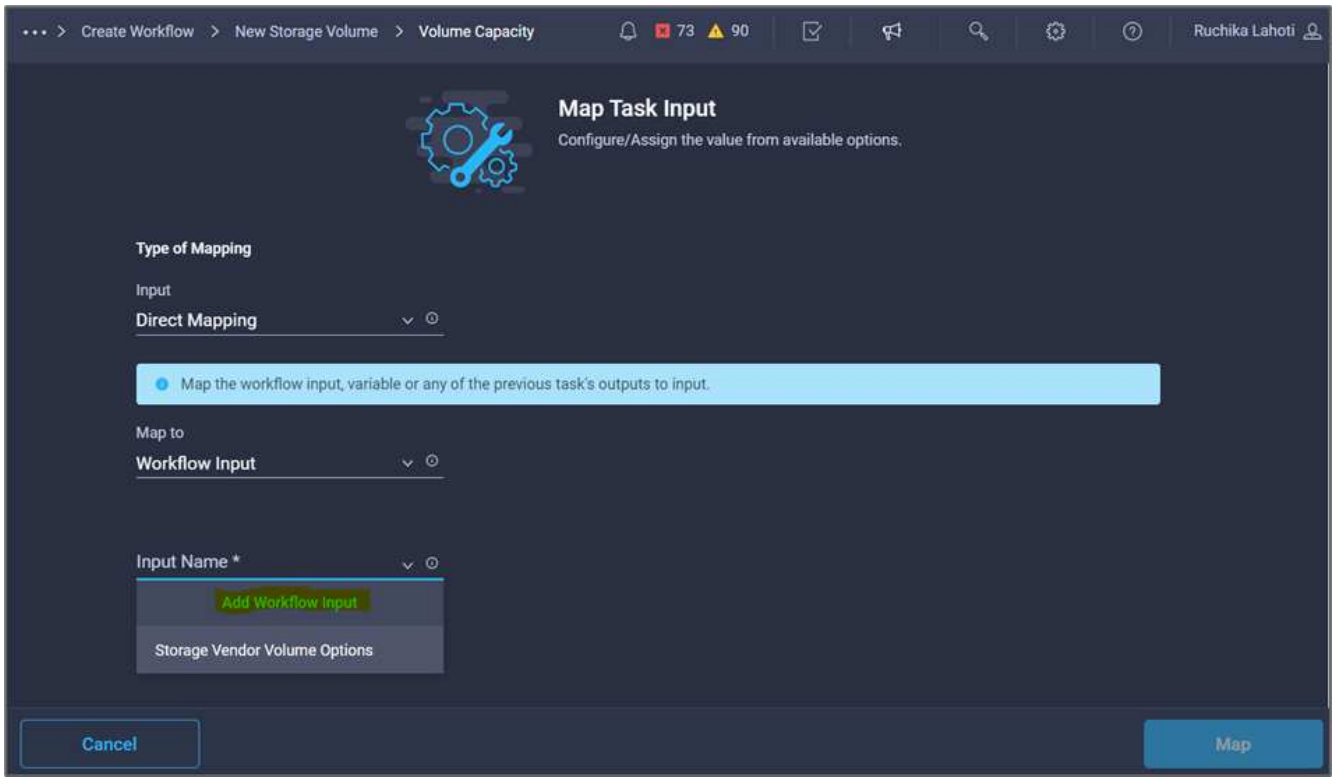
f. Geben Sie einen Standardwert für das erstellte Volume unter **Volume** an.

g. Klicken Sie auf **NFS**. Wenn NFS festgelegt ist, wird ein NFS Volume erstellt. Wenn dieser Wert auf false gesetzt ist, wird ein SAN-Volume erstellt.

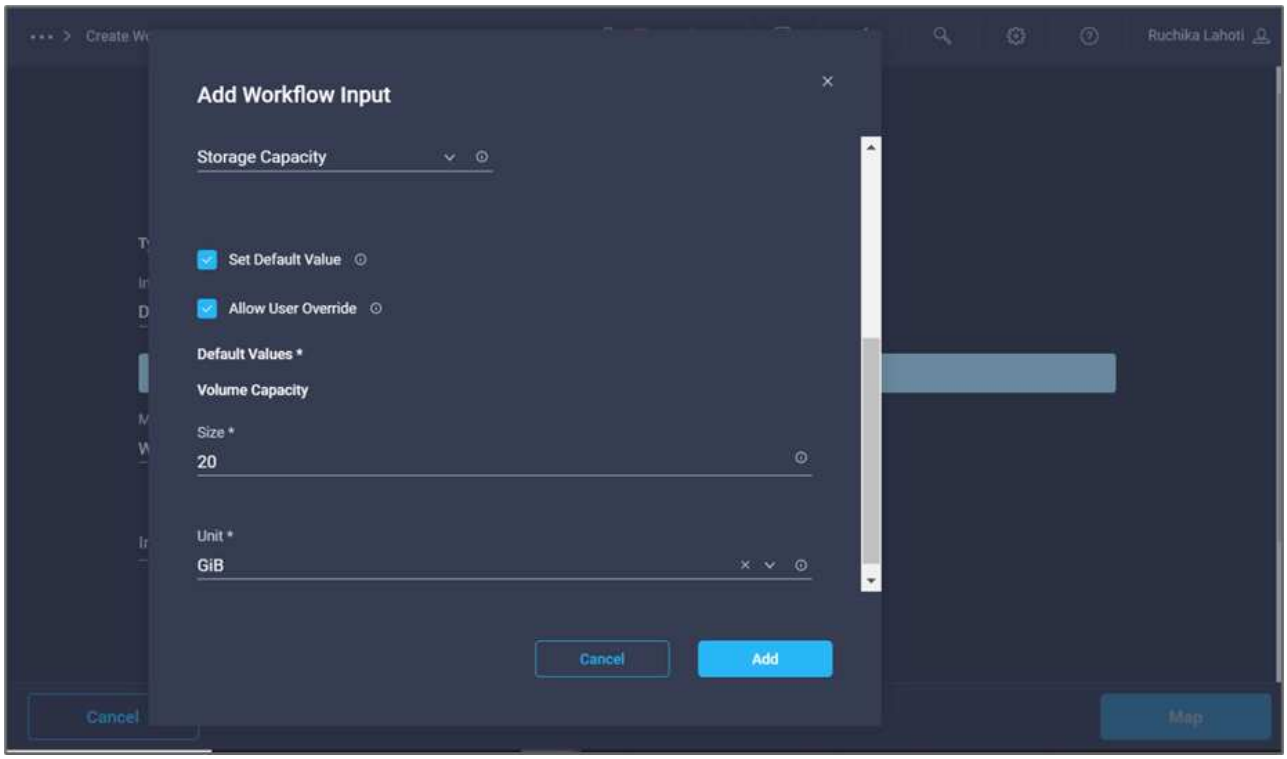
h. Geben Sie einen Mount-Pfad an und klicken Sie auf **Hinzufügen**.



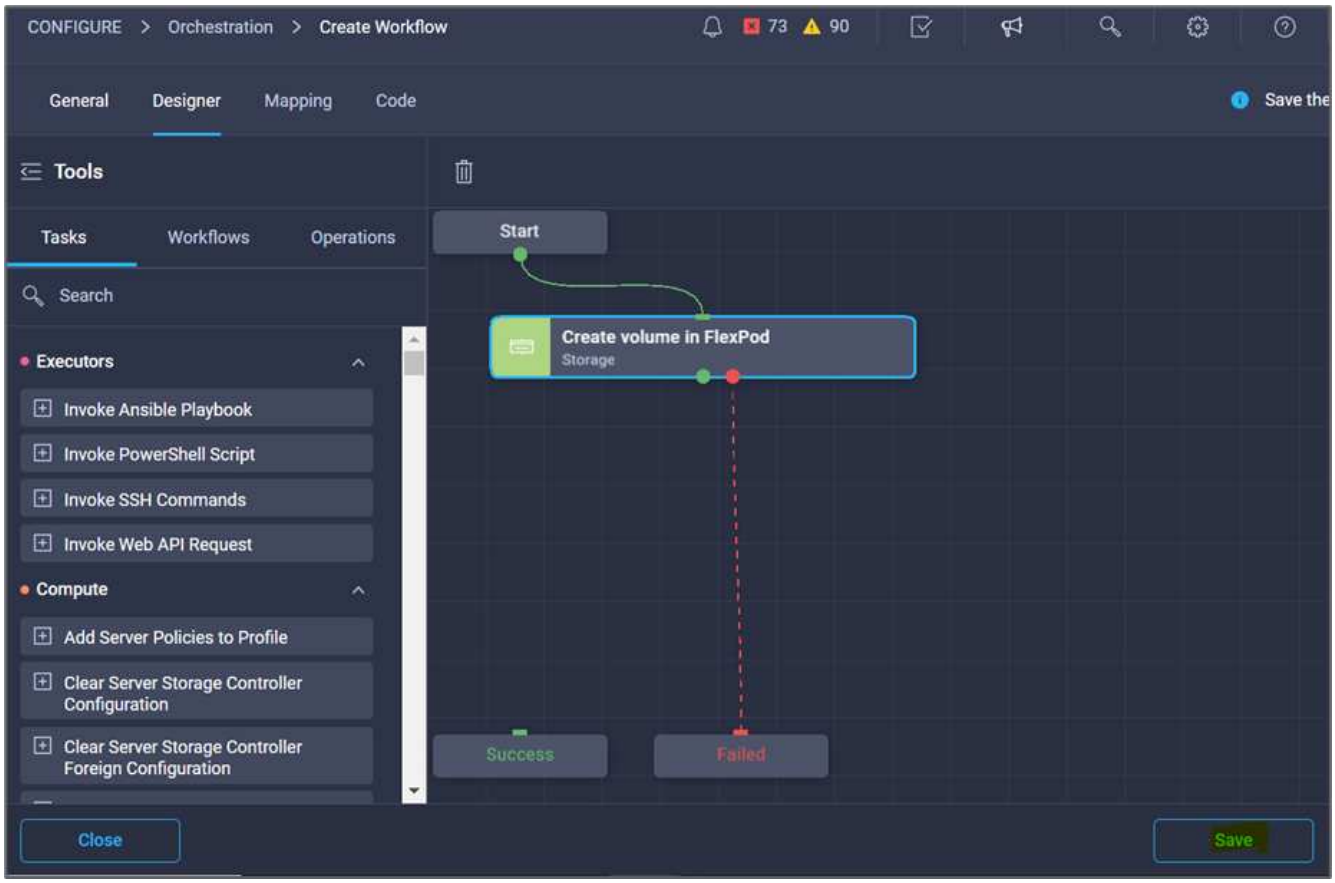
20. Klicken Sie Auf **Karte**.
21. Klicken Sie im Feld **Volume Capacity** auf **Map**.
22. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Workflow-Eingabe**.
23. Klicken Sie auf **Eingabename** und **Workflow-Eingabe erstellen**.



24. Im Add Input Wizard:
    a. Geben Sie einen Anzeigenamen und einen Referenznamen an (optional).
    b. Klicken Sie Auf * Erforderlich*.
    c. Wählen Sie für **Typ Speicherkapazität**.
    d. Klicken Sie auf **Standardwert festlegen und überschreiben**.
    e. Geben Sie einen Standardwert für Volume-Größe und -Einheit an.
    f. Klicken Sie Auf **Hinzufügen**.



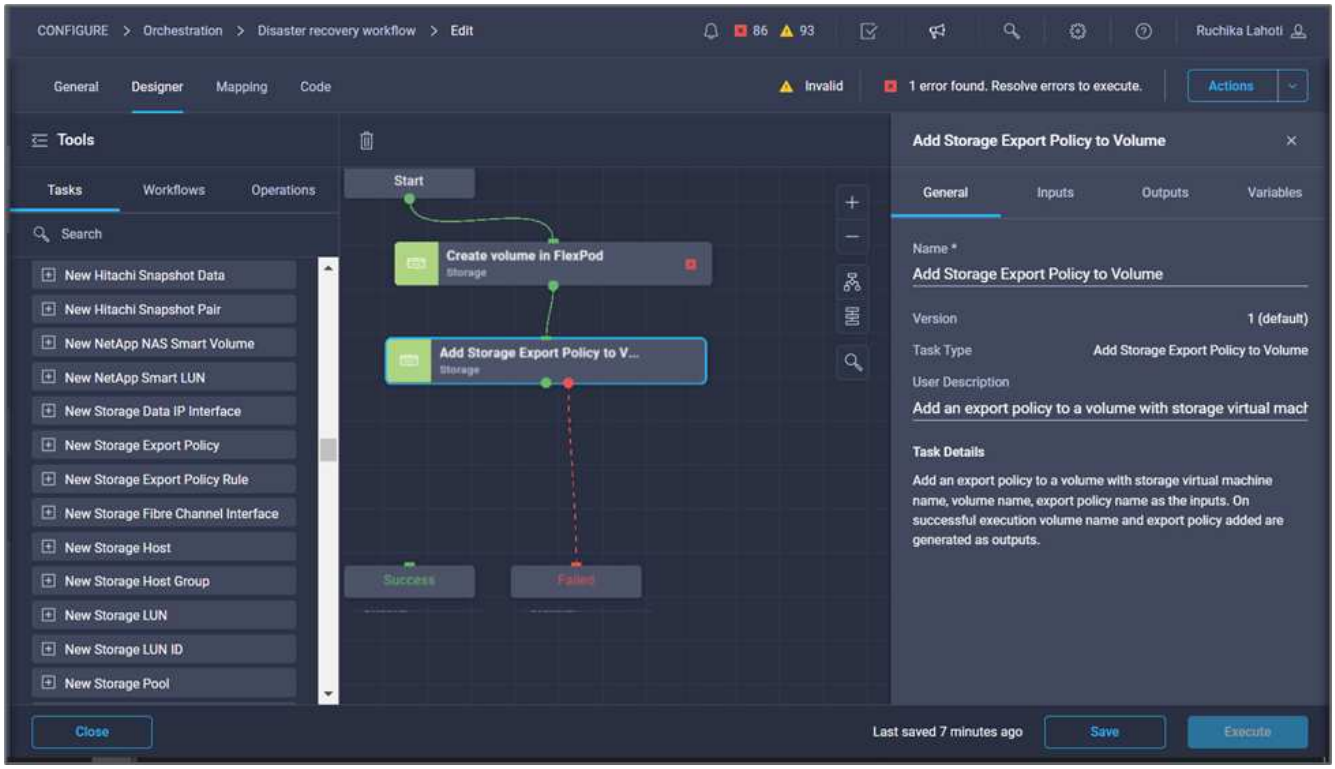
25. Klicken Sie Auf **Karte**.
26. Erstellen Sie mit Connector eine Verbindung zwischen den Aufgaben **Start** und **Lautstärke in FlexPod** erstellen, und klicken Sie auf **Speichern**.



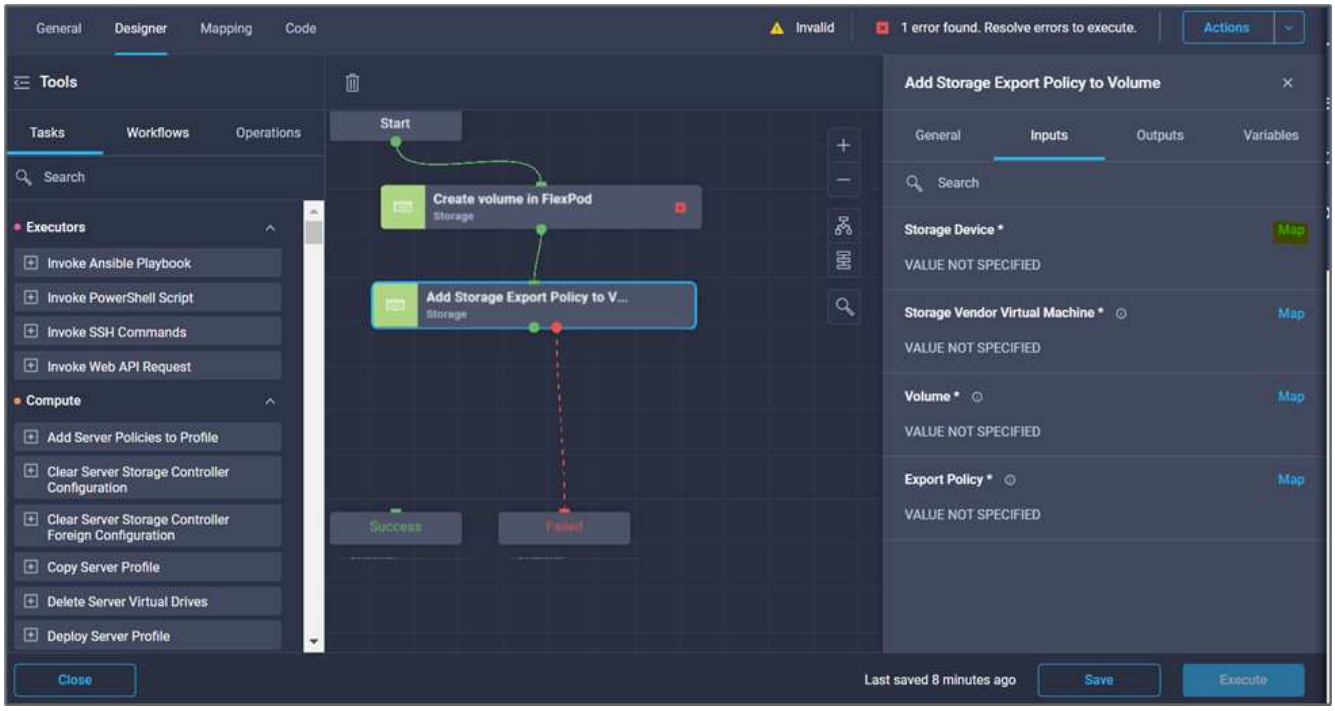
Ignorieren Sie den Fehler jetzt. Dieser Fehler wird angezeigt, weil es keine Verbindung zwischen den Tasks **Create Volume in FlexPod** und **success** gibt, die erforderlich ist, um den erfolgreichen Übergang festzulegen.

Verfahren 3: Add Storage Export Policy

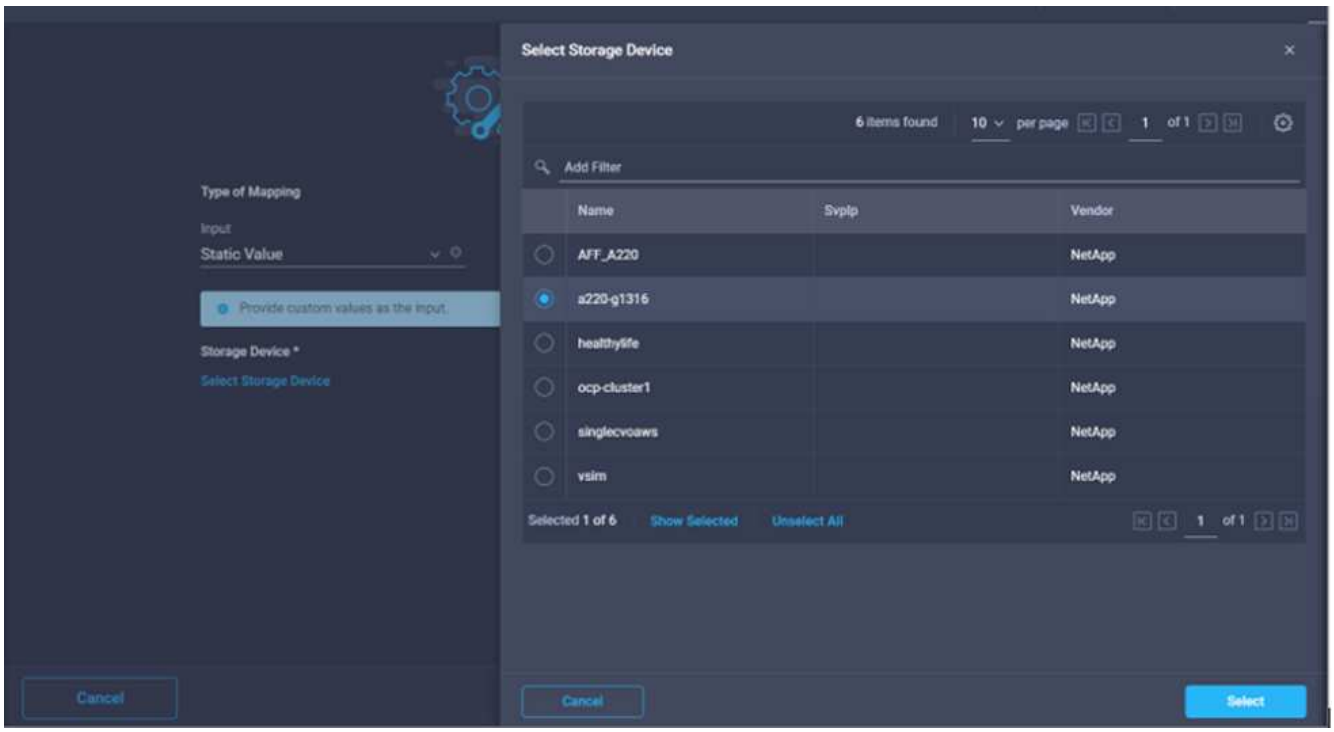
1. Gehen Sie zur Registerkarte **Designer** und klicken Sie im Abschnitt **Tools** auf **Tasks**.
2. Ziehen Sie die Aufgabe **Speicherung > Speicherexport Policy in Volume** hinzufügen aus dem Abschnitt **Tools** im Bereich **Design**.
3. Klicken Sie auf **Storage Export Policy zum Volume hinzufügen**. Klicken Sie im Bereich **Aufgabeneigenschaften** auf die Registerkarte **Allgemein**. Optional können Sie den Namen und die Beschreibung für diese Aufgabe ändern. In diesem Beispiel lautet der Name der Aufgabe „Add Storage Export Policy“.
4. Verwenden Sie den Konnektor, um eine Verbindung zwischen den Aufgaben herzustellen **Erstellen Sie Volumes in FlexPod** und **Speicherexportrichtlinie hinzufügen**. Klicken Sie Auf **Speichern**.



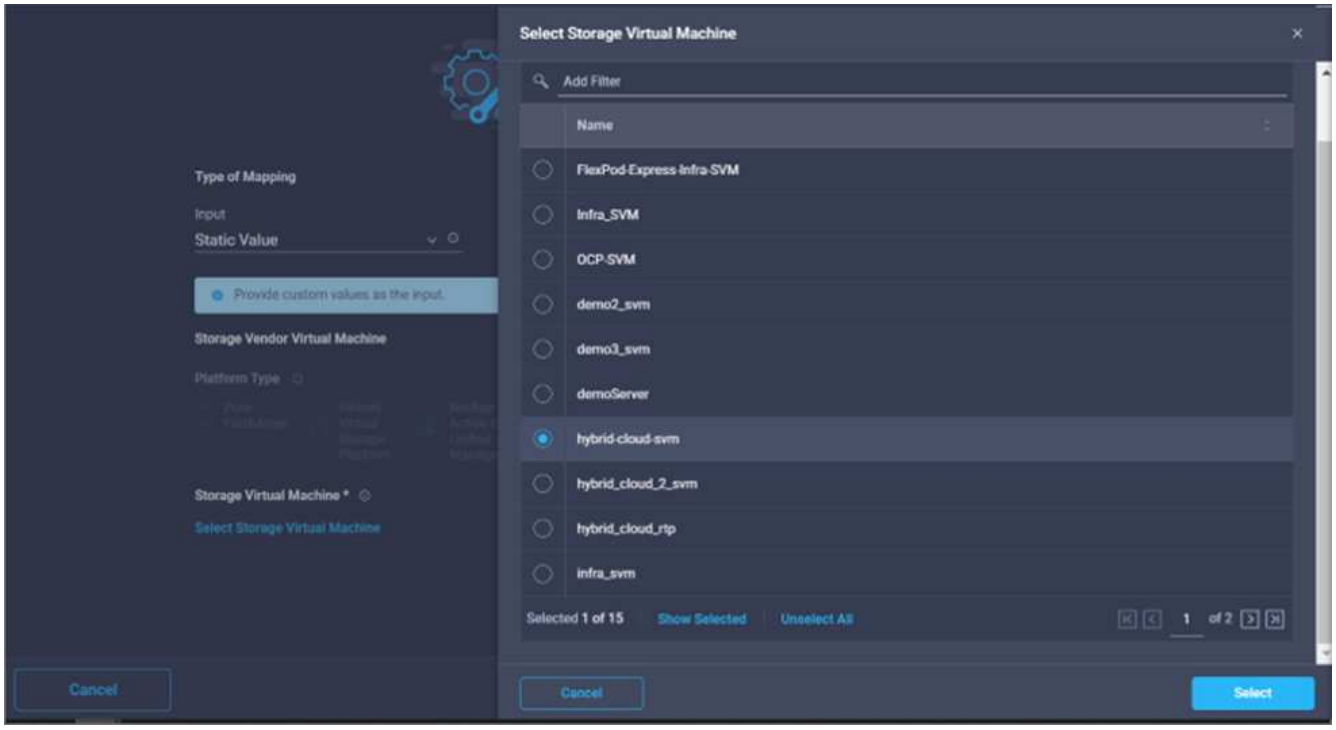
5. Klicken Sie im Bereich **Aufgabeneigenschaften** auf **Eingaben**.
6. Klicken Sie im Feld **Speichergerät** auf **Karte**.



7. Wählen Sie **statischer Wert** und klicken Sie auf **Speichergerät auswählen**. Wählen Sie dasselbe hinzugefügte Speicherziel aus, während Sie die vorherige Aufgabe zur Erstellung eines neuen Speichervolumens erstellen.
8. Klicken Sie Auf **Karte**.

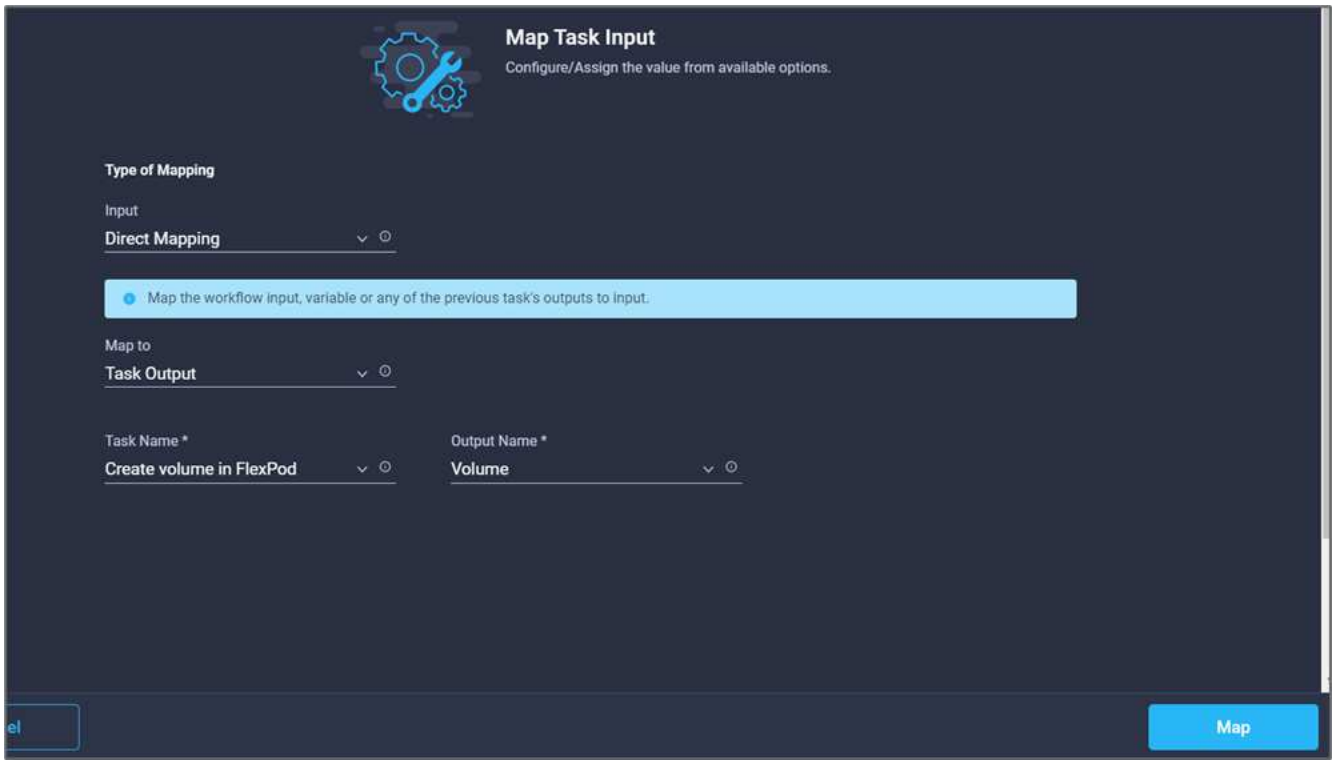


9. Klicken Sie im Feld **Storage Vendor Virtual Machine** auf **Map**.
10. Wählen Sie **statischer Wert** und klicken Sie auf **Storage Virtual Machine auswählen**. Wählen Sie dieselbe virtuelle Speichermaschine aus, die beim Erstellen der vorherigen Aufgabe zur Erstellung eines neuen Speichervolumes hinzugefügt wurde.

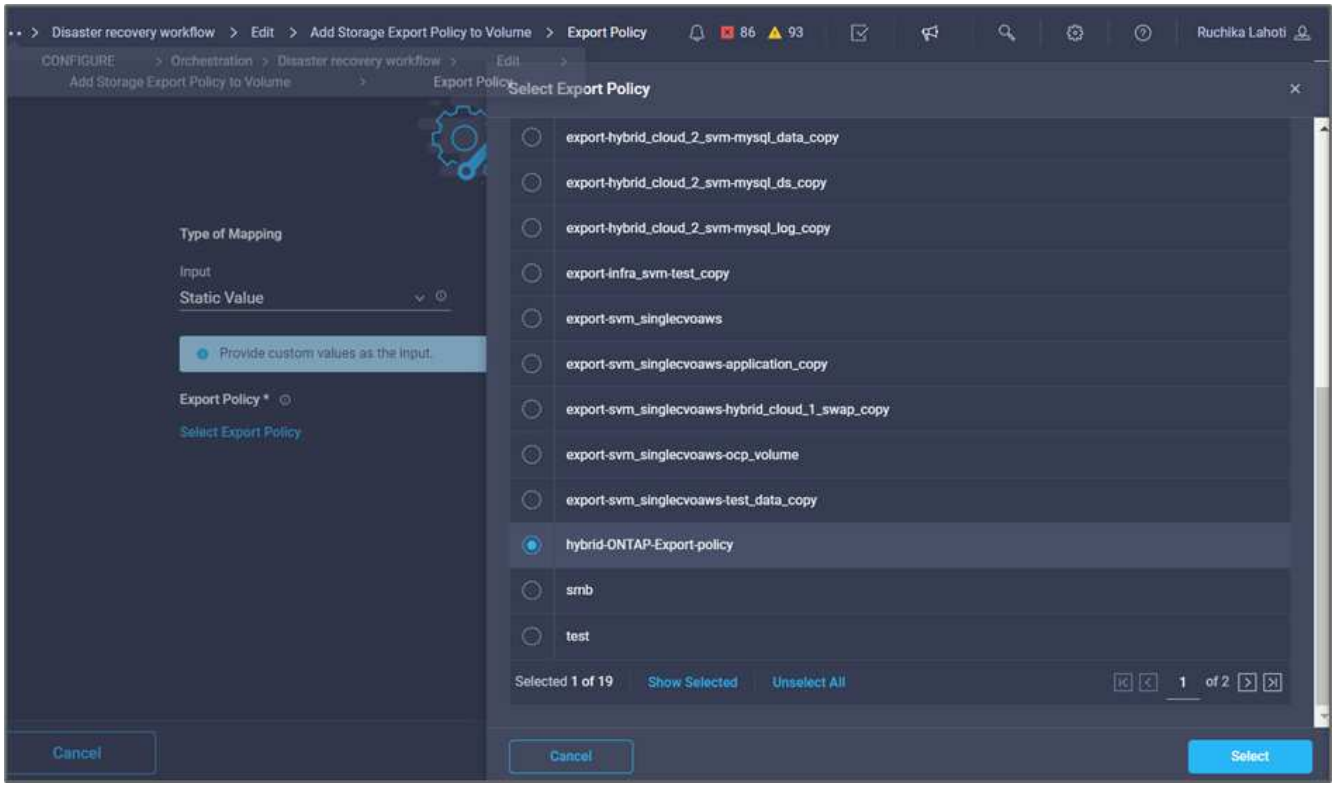


11. Klicken Sie Auf **Karte**.
12. Klicken Sie im Feld **Volumen** auf **Karte**.
13. Klicken Sie auf **Aufgabenname** und dann auf **Volumen in FlexPod erstellen**. Klicken Sie auf **Ausgabename** und dann auf **Volumen**.

> In Cisco Intersight Cloud Orchestrator können Sie die Ausgabe einer früheren Aufgabe als Input für eine neue Aufgabe bereitstellen. In diesem Beispiel wurden die **Volumen**-Details aus der Task **Create Volume in FlexPod** als Input für die Aufgabe **Add Storage Export Policy** bereitgestellt.



14. Klicken Sie Auf **Karte**.
15. Klicken Sie im Feld **Richtlinie exportieren** auf **Karte**.
16. Wählen Sie **statischer Wert** und klicken Sie auf **Exportrichtlinie auswählen**. Wählen Sie die erstellte Exportrichtlinie aus.

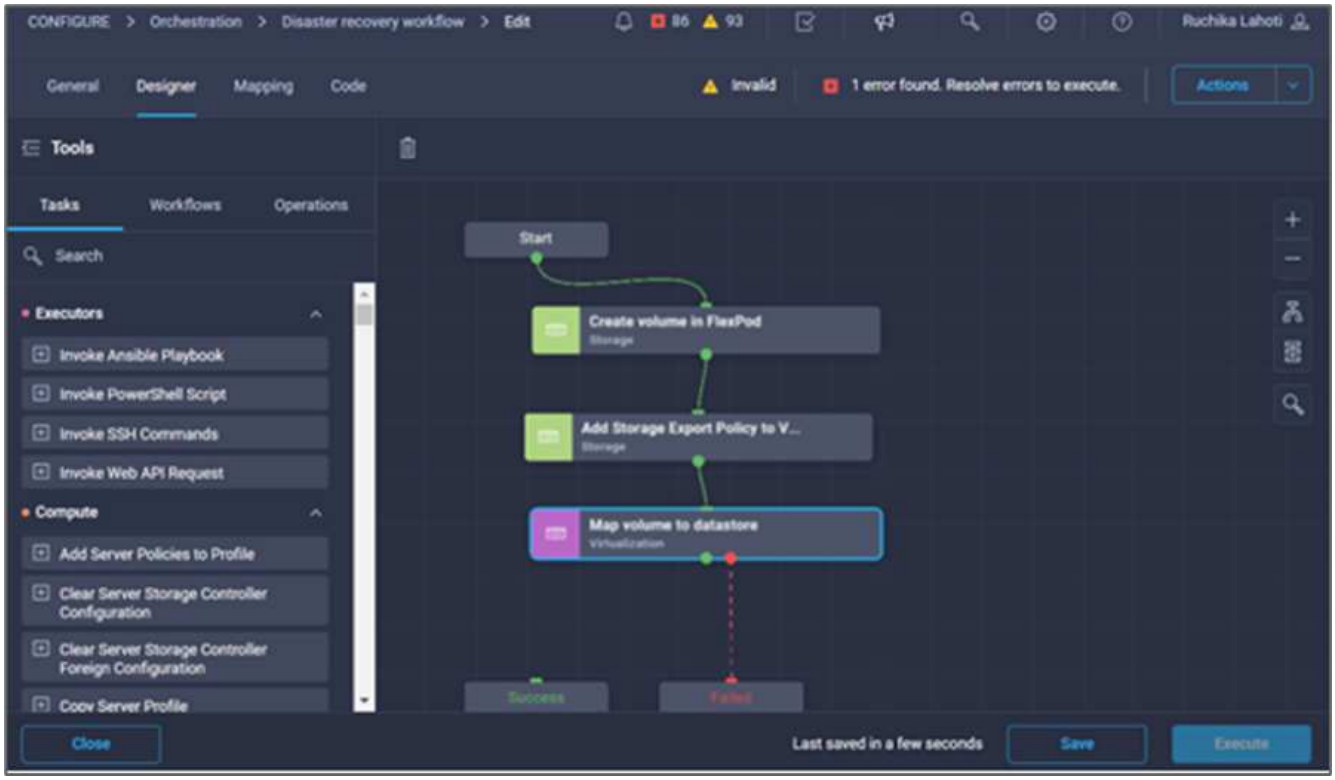


17. Klicken Sie auf **Karte** und dann auf **Speichern**.

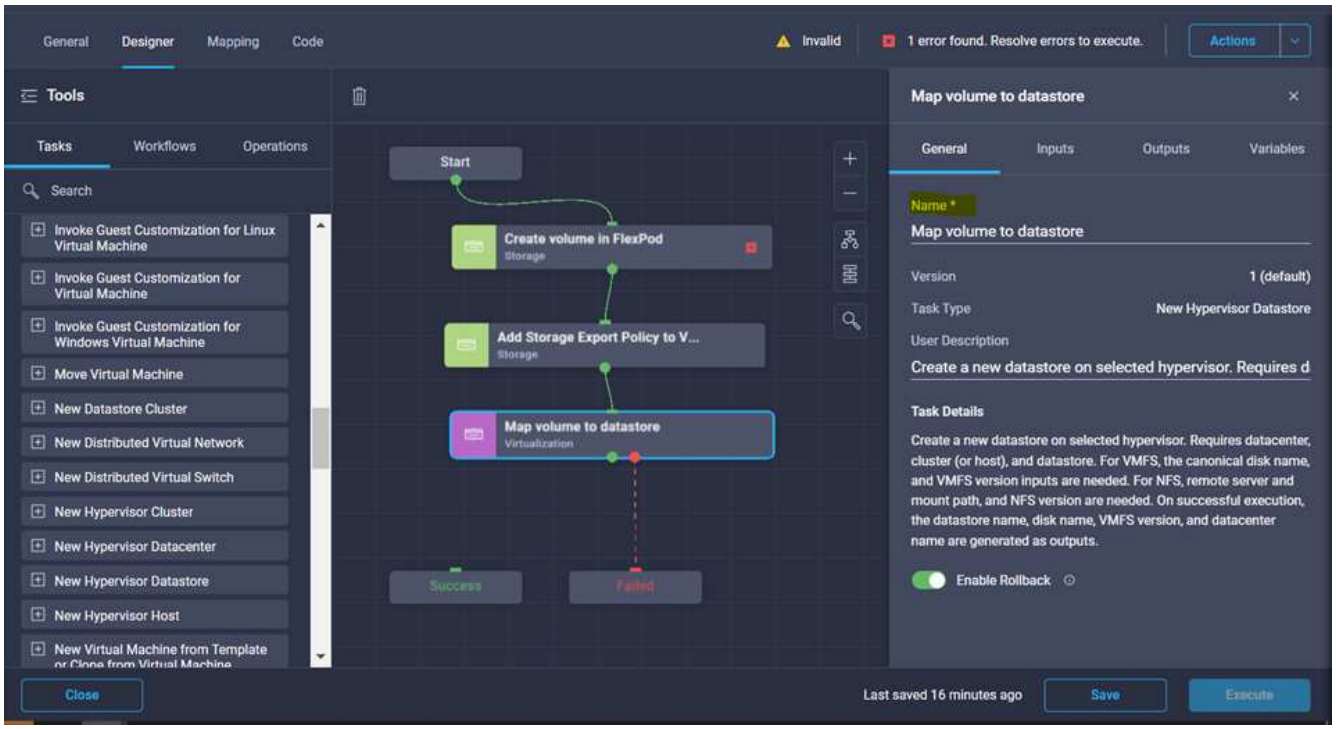
Damit ist das Hinzufügen einer Exportrichtlinie zum Volume abgeschlossen. Als Nächstes erstellen Sie einen neuen Datenspeicher, der das erstellte Volume zugeordnet.

Prozedur 4: FlexPod Volume zu Datastore zuordnen

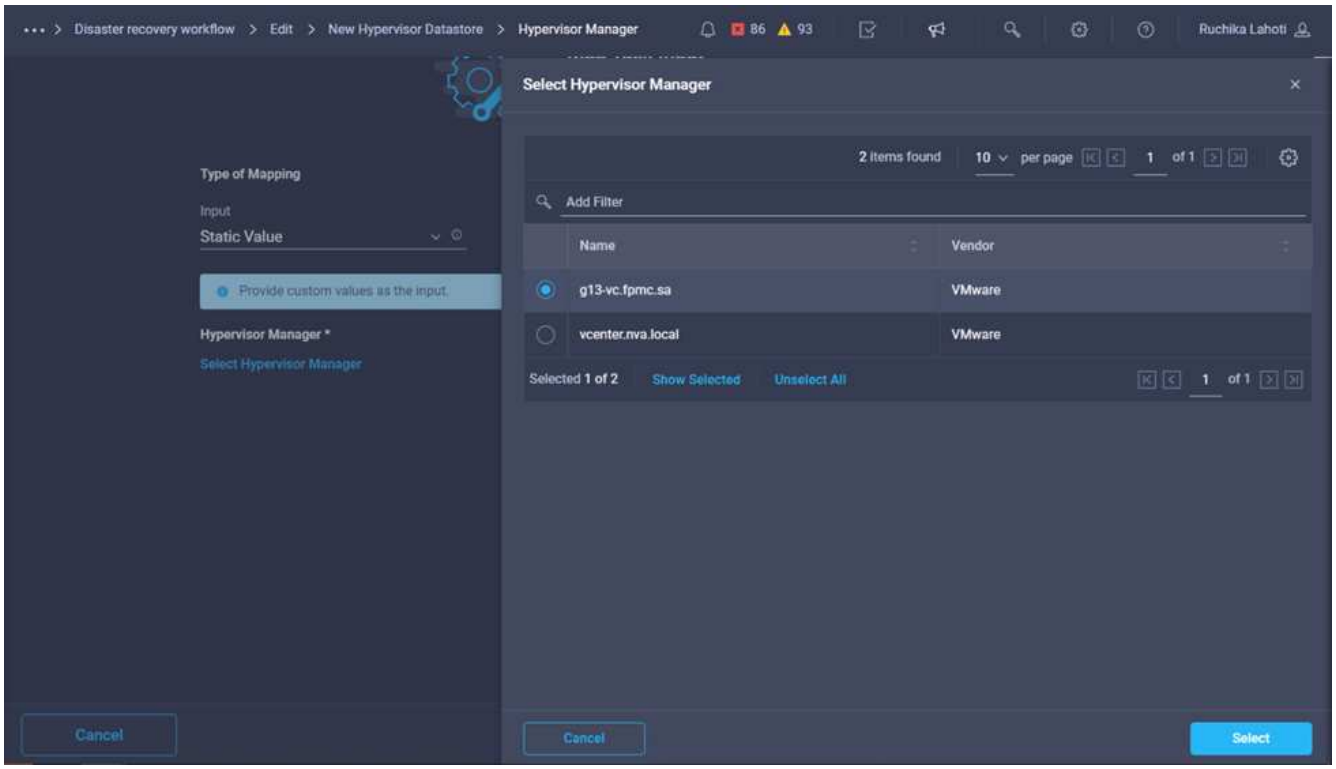
1. Gehen Sie zur Registerkarte **Designer** und klicken Sie im Abschnitt **Tools** auf **Tasks**.
2. Ziehen Sie die Aufgabe **Virtualisierung > Neuer Hypervisor Datastore** aus dem Abschnitt **Tools** im Bereich **Design**.
3. Verwenden Sie Connector, um eine Verbindung zwischen den Aufgaben **Add Storage Export Policy** und **New Hypervisor Datastore** herzustellen. Klicken Sie Auf **Speichern**.



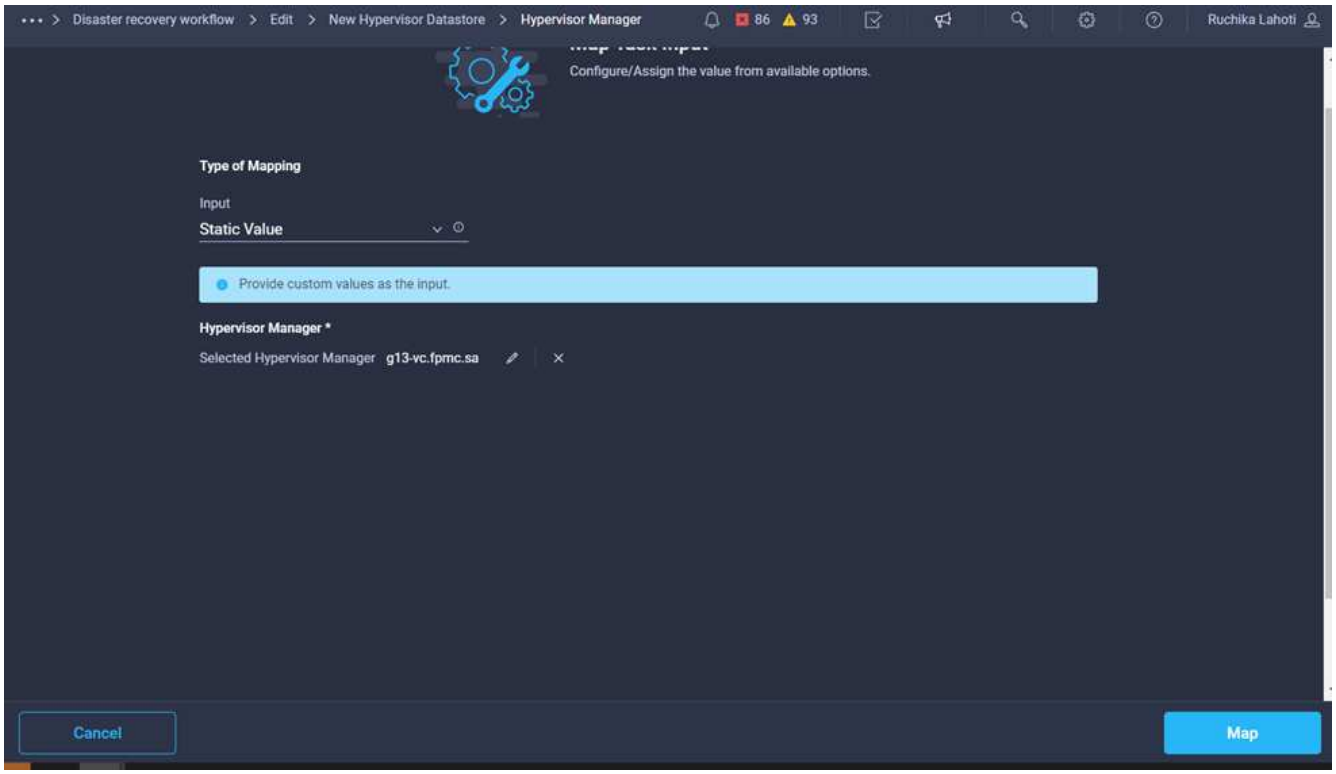
4. Klicken Sie Auf **Neuer Hypervisor Datastore**. Klicken Sie im Bereich **Aufgabeneigenschaften** auf die Registerkarte **Allgemein**. Optional können Sie den Namen und die Beschreibung für diese Aufgabe ändern. In diesem Beispiel lautet der Name der Aufgabe **Datenträger in Datastore** zuordnen.



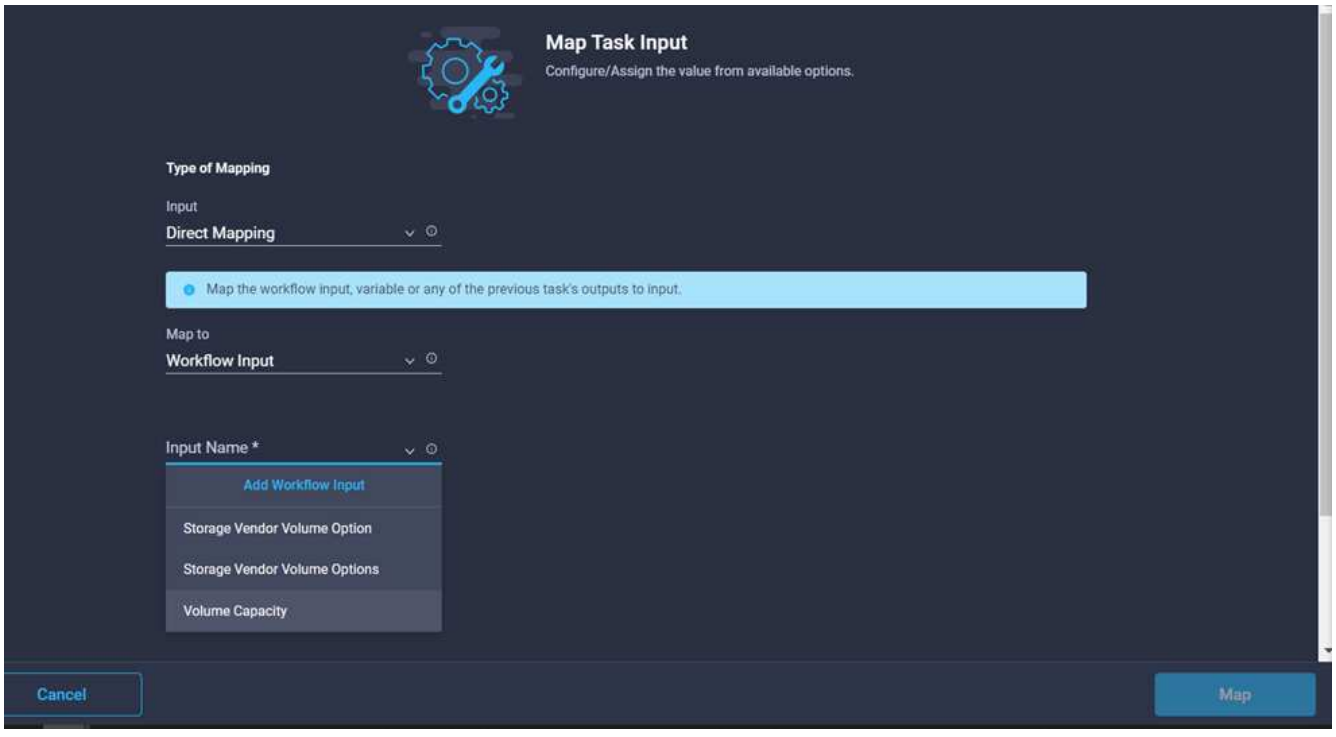
5. Klicken Sie im Bereich **Aufgabeneigenschaften** auf **Eingaben**.
6. Klicken Sie im Feld **Hypervisor Manager** auf **Karte**.
7. Wählen Sie **statischer Wert** und klicken Sie auf **Hypervisor Manager auswählen**. Klicken Sie auf das VMware vCenter Ziel.



8. Klicken Sie Auf **Karte**.



9. Klicken Sie im Feld **Data Center** auf **Karte**. Dies ist das dem neuen Datenspeicher zugeordnete Datacenter.
10. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Workflow-Eingabe**.
11. Klicken Sie auf **Eingabename** und dann auf **Workflow-Eingabe erstellen**.



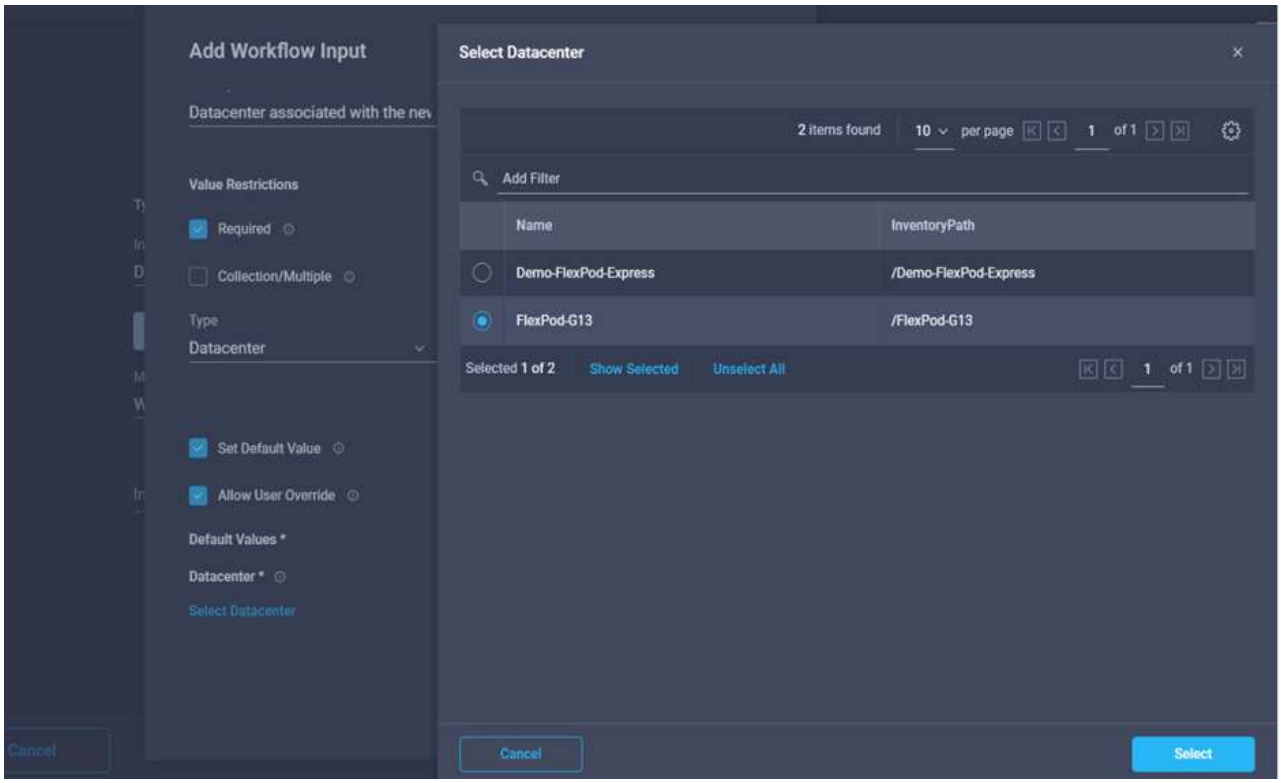
12. Führen Sie im Add Input Wizard die folgenden Schritte aus:
    a. Geben Sie einen Anzeigenamen und einen Referenznamen an (optional).

b. Wählen Sie **Datacenter** als Typ aus.

c. Klicken Sie auf **Standardwert festlegen und überschreiben**.

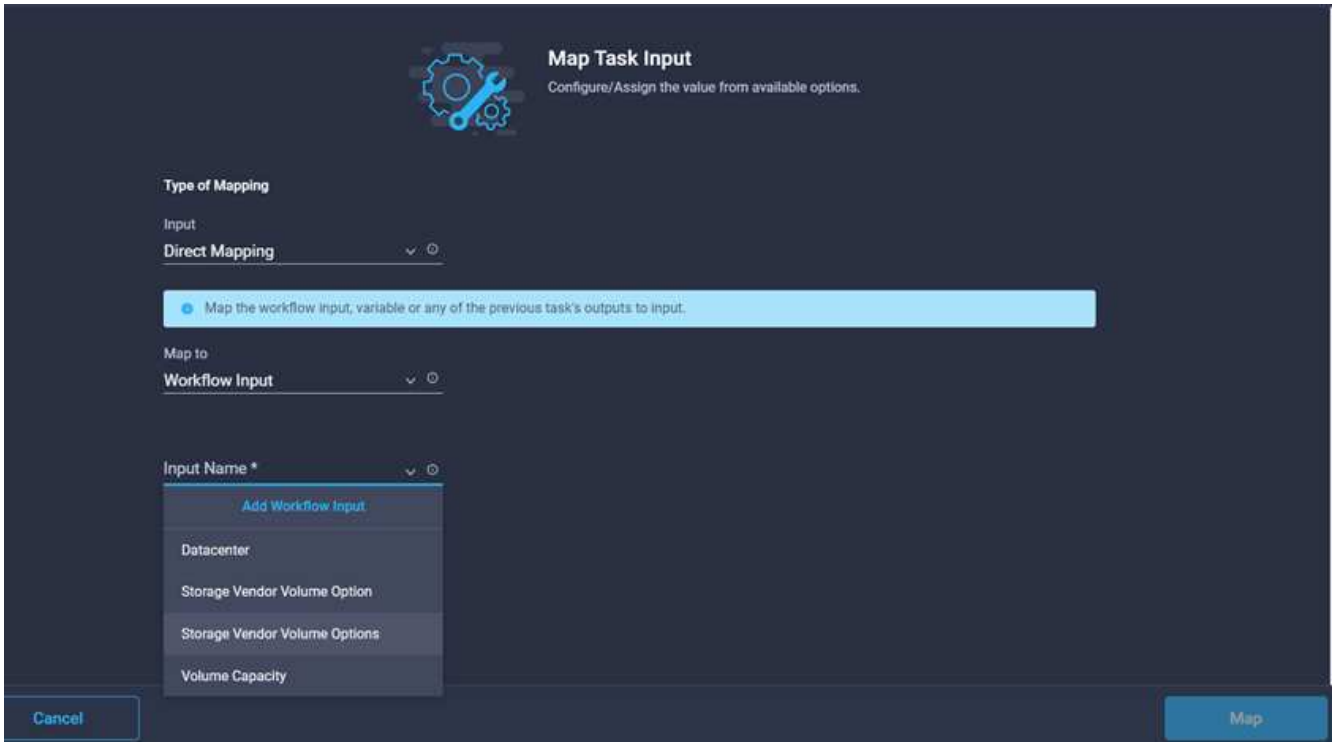
d. Klicken Sie Auf **Datacenter Auswählen**.

e. Klicken Sie auf das dem neuen Datenspeicher zugeordnete Rechenzentrum und dann auf **Auswählen**.

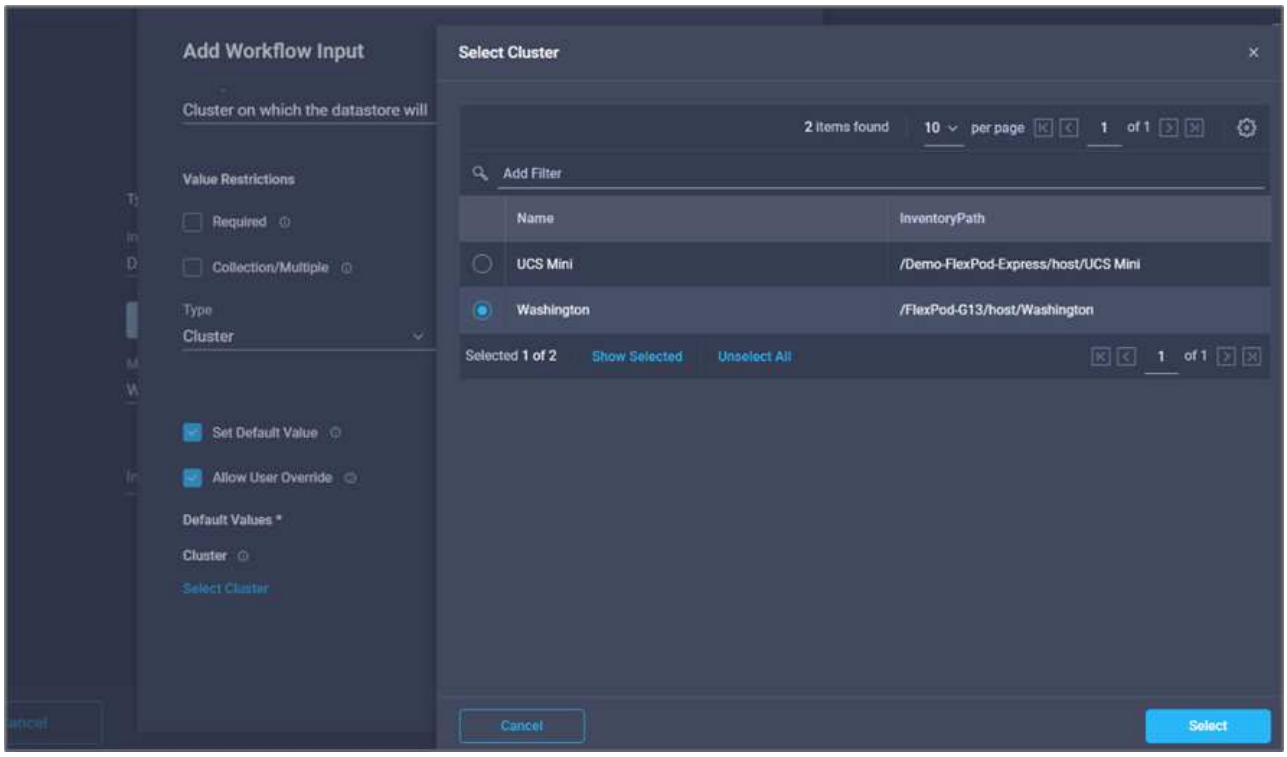


- Klicken Sie Auf **Hinzufügen**.

13. Klicken Sie Auf **Karte**.
14. Klicken Sie im Feld **Cluster** auf **Karte**.
15. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Workflow-Eingabe**.

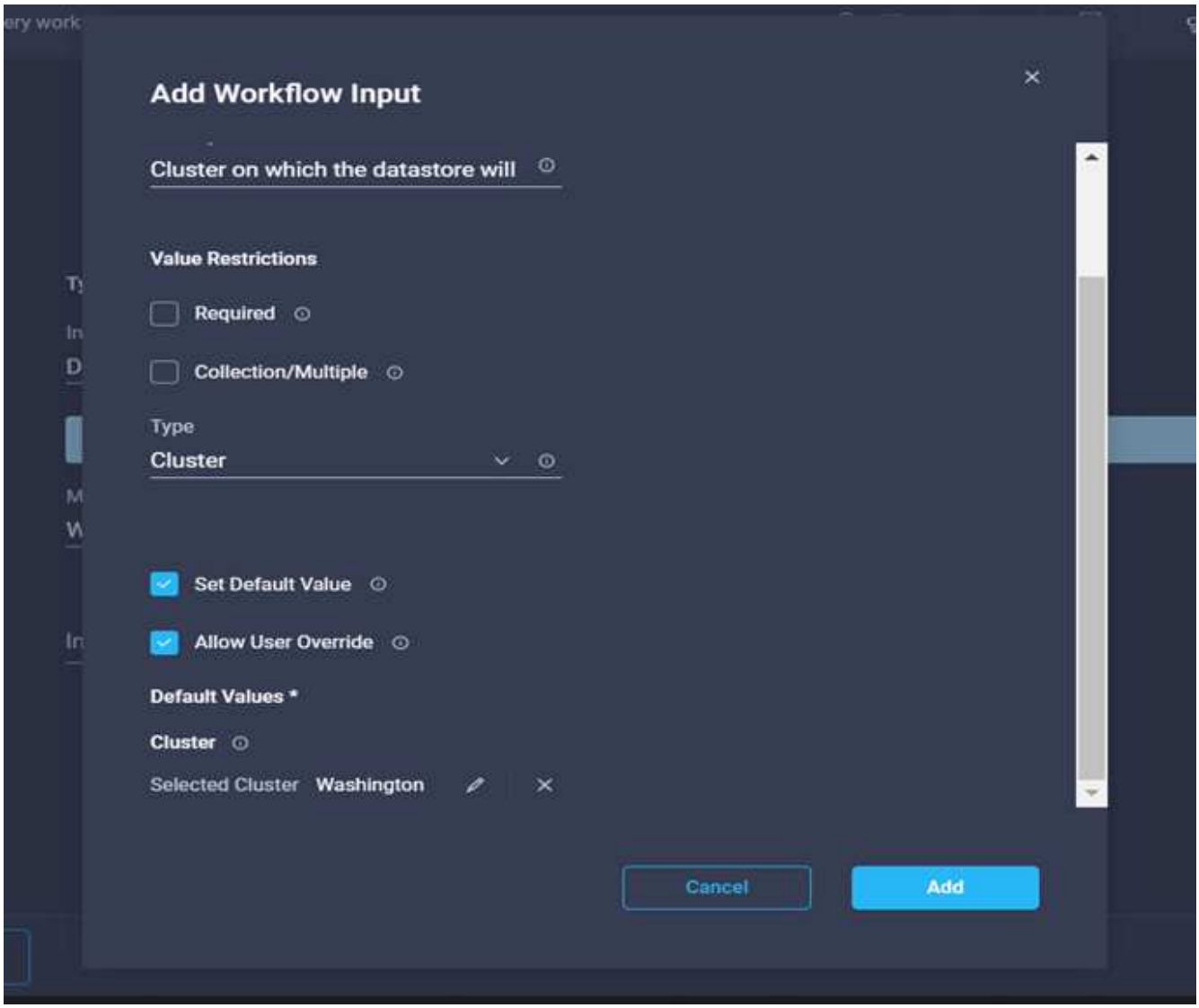


16. Führen Sie im Add Input Wizard die folgenden Schritte aus:
    a. Geben Sie einen Anzeigenamen und einen Referenznamen an (optional).
    b. Klicken Sie Auf * Erforderlich*.
    c. Wählen Sie als Typ Cluster aus.
    d. Klicken Sie auf **Standardwert festlegen und überschreiben**.
    e. Klicken Sie Auf **Cluster Auswählen**.
    f. Klicken Sie auf den Cluster, der dem neuen Datenspeicher zugeordnet ist.
    g. Klicken Sie Auf **Auswählen**.

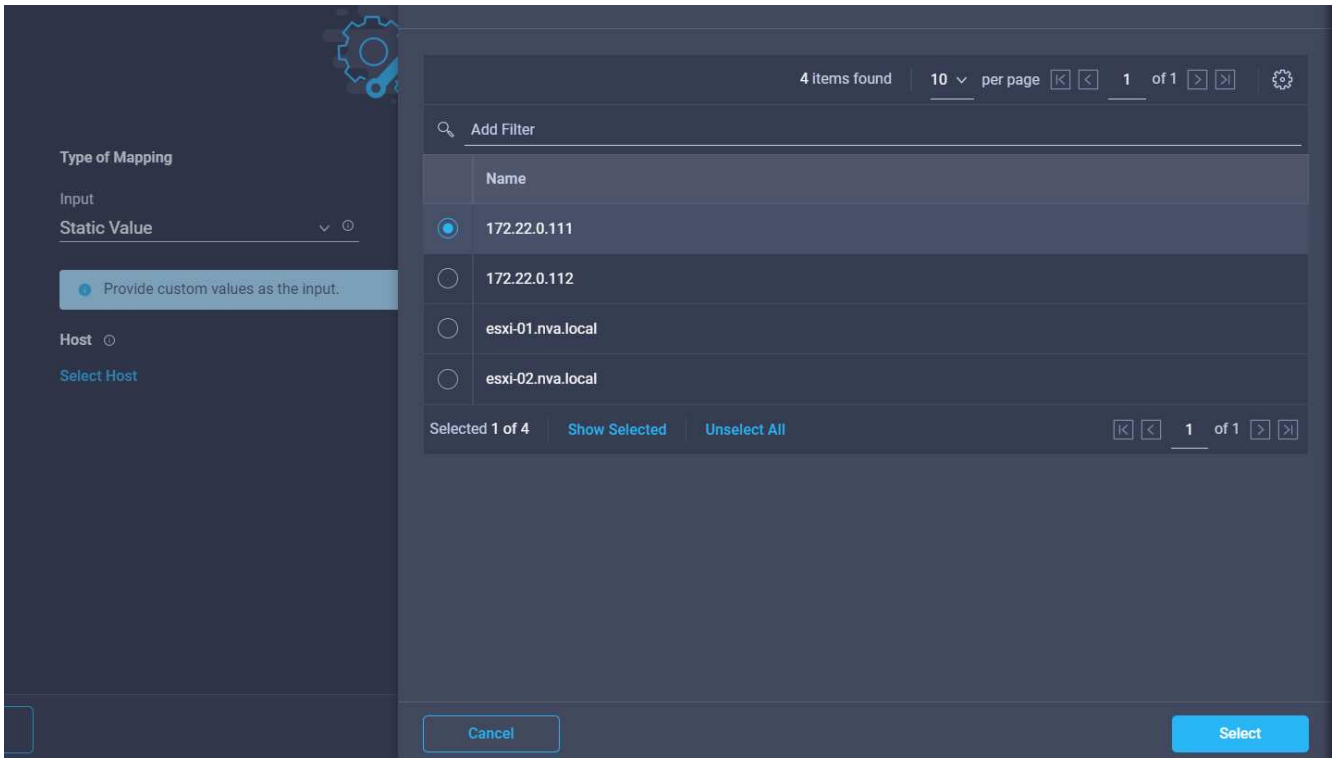


h. Klicken Sie Auf **Hinzufügen**.

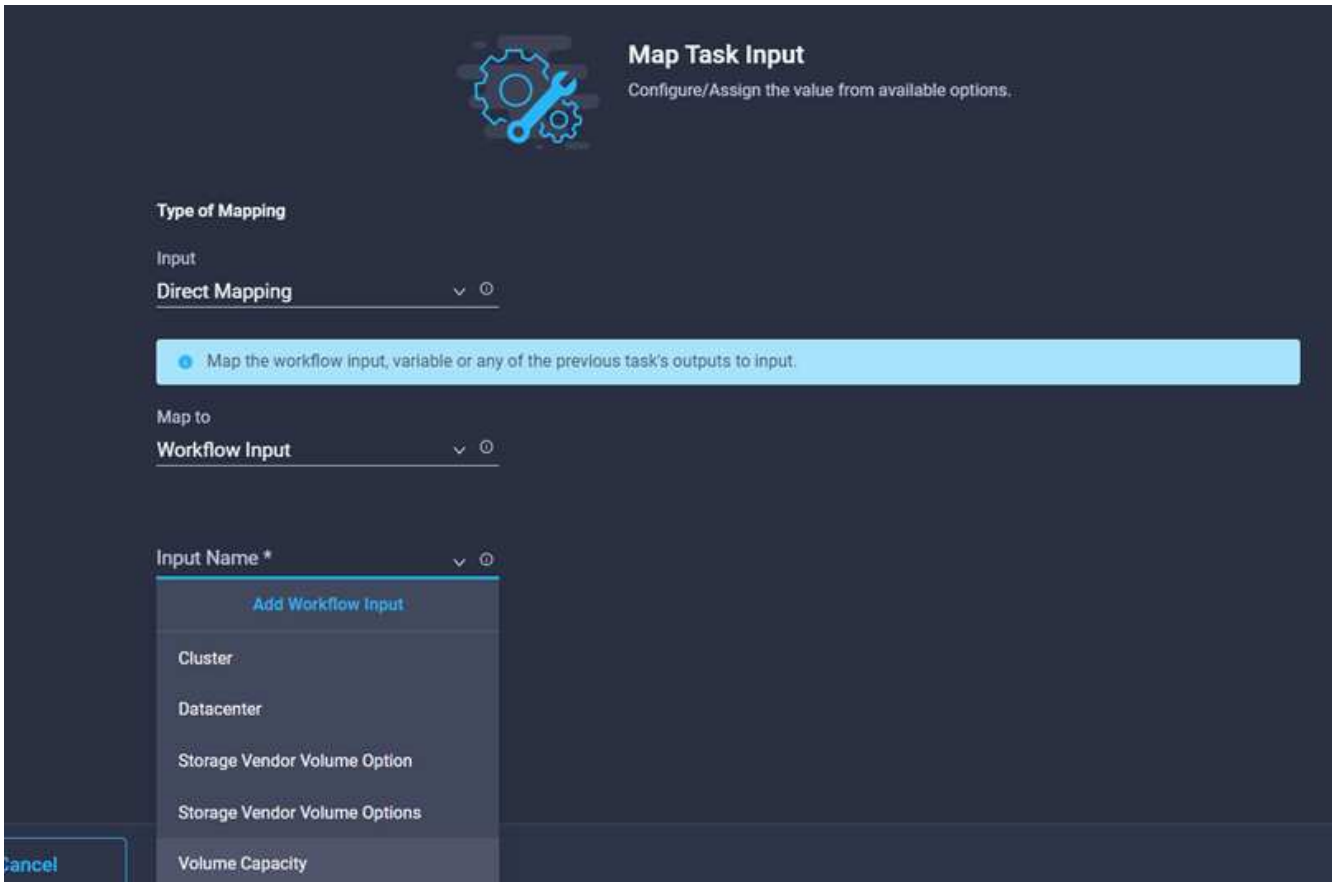
17. Klicken Sie Auf **Karte**.
18. Klicken Sie im Feld **Host** auf **Karte**.



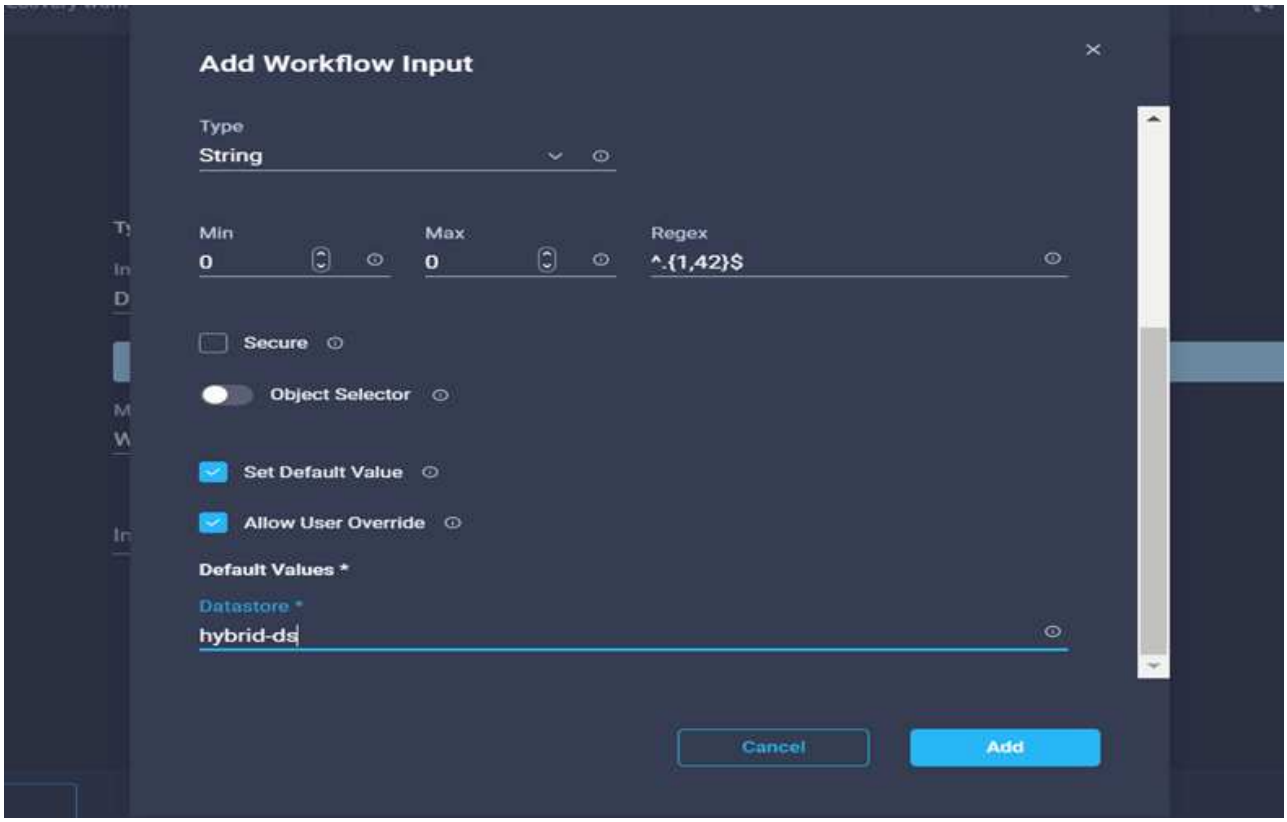
19. Wählen Sie **statischer Wert** und klicken Sie auf den Host, auf dem der Datenspeicher gehostet werden soll. Wenn ein Cluster angegeben wird, wird der Host ignoriert.



20. Klicken Sie auf **Auswählen und Karte**.
21. Klicken Sie im Feld **Datastore** auf **Map**.
22. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Workflow-Eingabe**.
23. Klicken Sie auf **Eingabename** und **Workflow-Eingabe erstellen**.

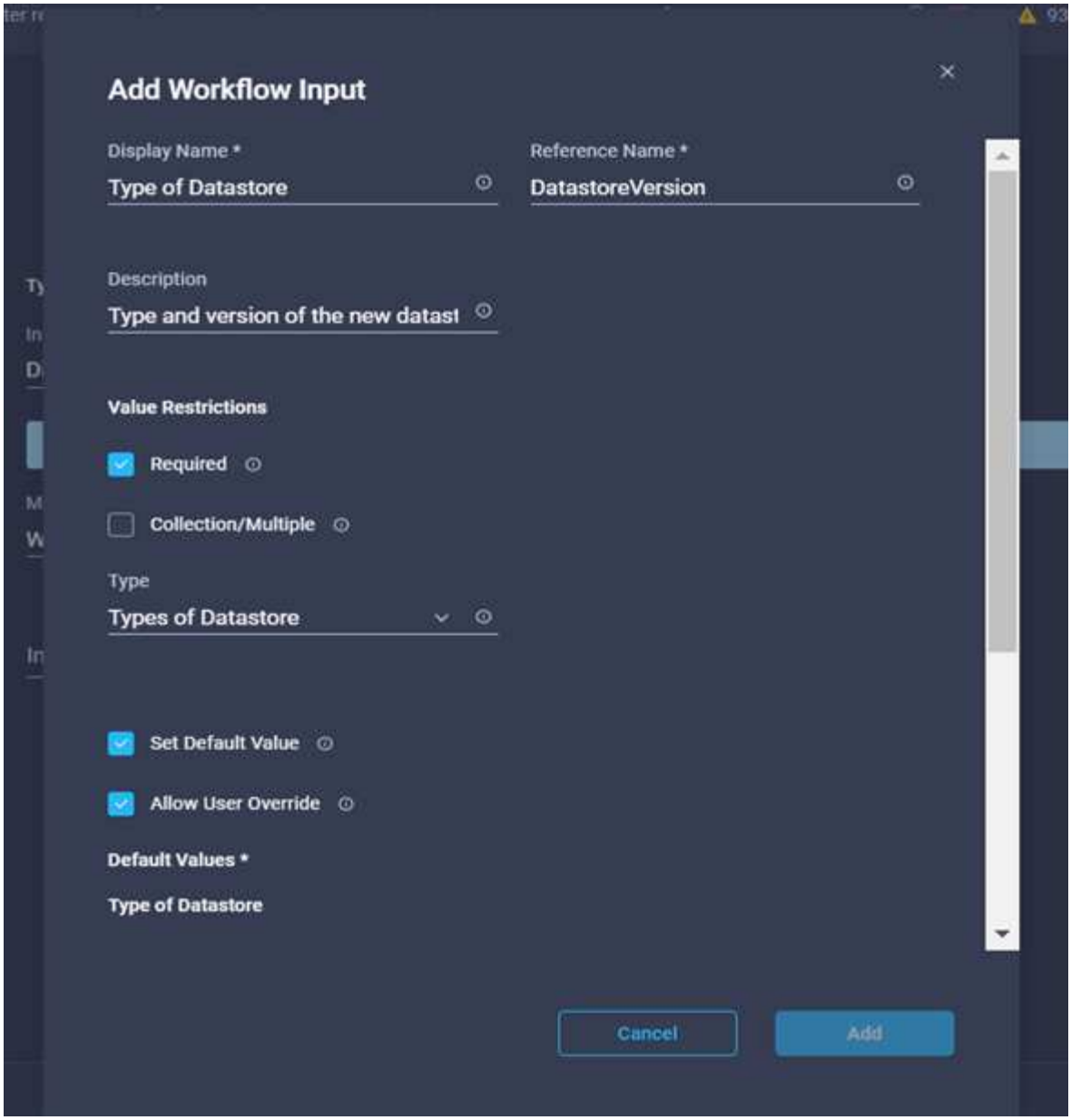


24. Im Add Input Wizard:
    a. Geben Sie einen Anzeigenamen und einen Referenznamen an (optional).
    b. Klicken Sie Auf * Erforderlich*.
    c. Klicken Sie auf **Standardwert festlegen und überschreiben**.
    d. Geben Sie einen Standardwert für den Datastore ein und klicken Sie auf **Hinzufügen**.



25. Klicken Sie Auf **Karte**.
26. Klicken Sie im Eingabefeld **Datenspeichertyp** auf **Karte**.
27. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Workflow-Eingabe**.
28. Klicken Sie auf **Eingabename** und **Workflow-Eingabe erstellen**.

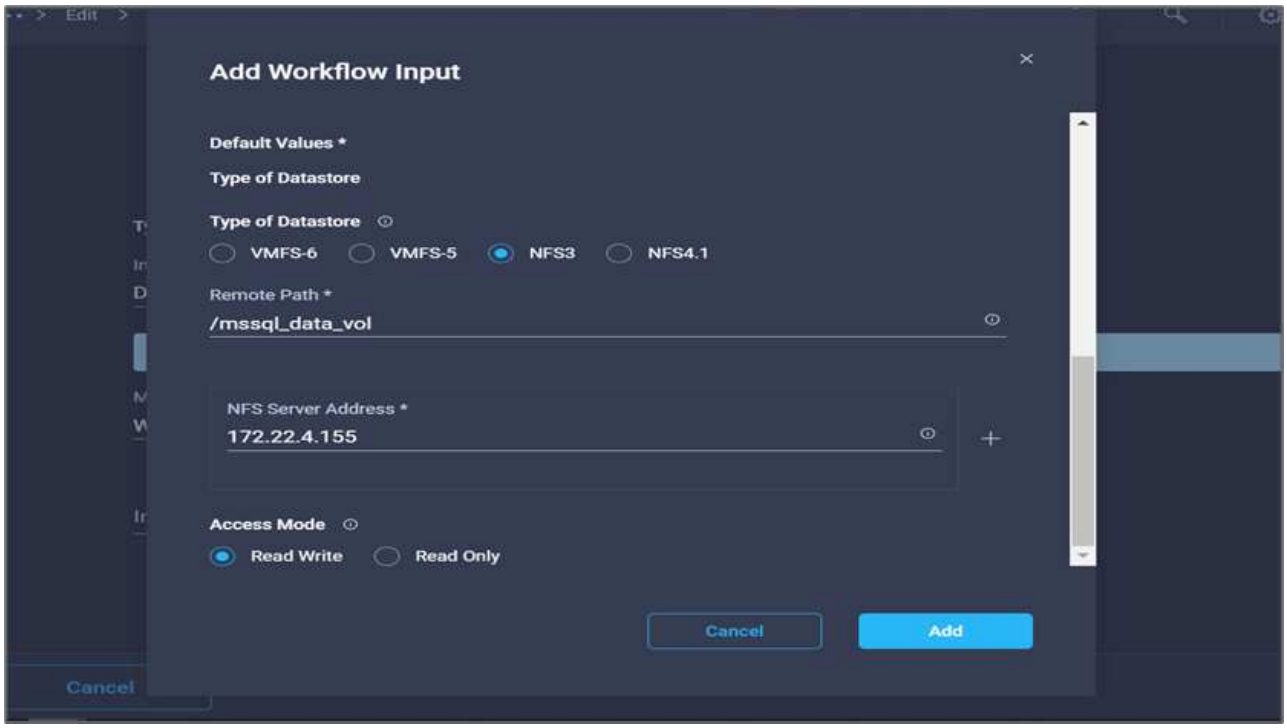
29. Führen Sie im Add Input Wizard die folgenden Schritte aus:
    a. Geben Sie einen Anzeigenamen und einen Referenznamen an (optional) und klicken Sie auf **erforderlich**.
    b. Stellen Sie sicher, dass Sie den Typ **Types of Datastore** auswählen und auf **Standardwert festlegen und überschreiben** klicken.



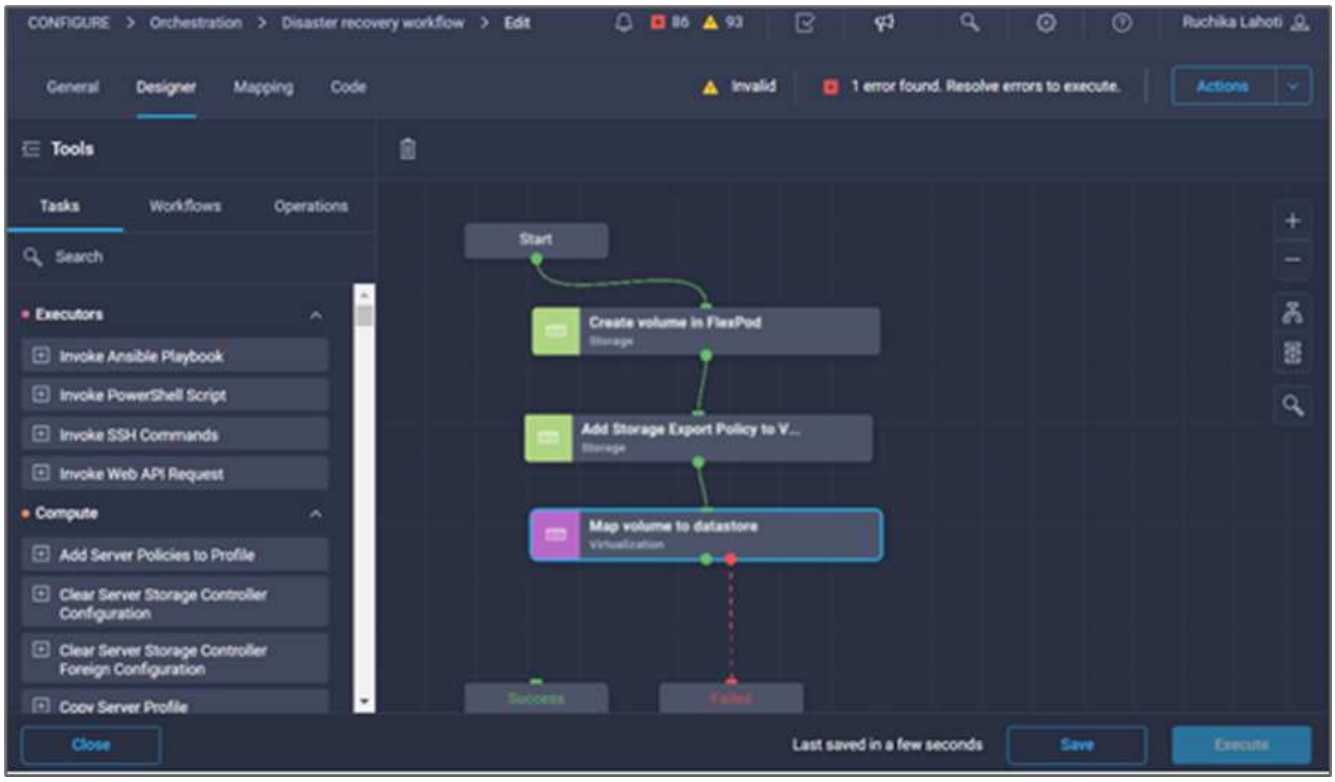
c. Geben Sie den Remote-Pfad an. Dies ist der Remote-Pfad des NFS Mount-Punkts.

d. Geben Sie die Hostnamen oder IP-Adressen des Remote-NFS-Servers in NFS-Serveradresse an.

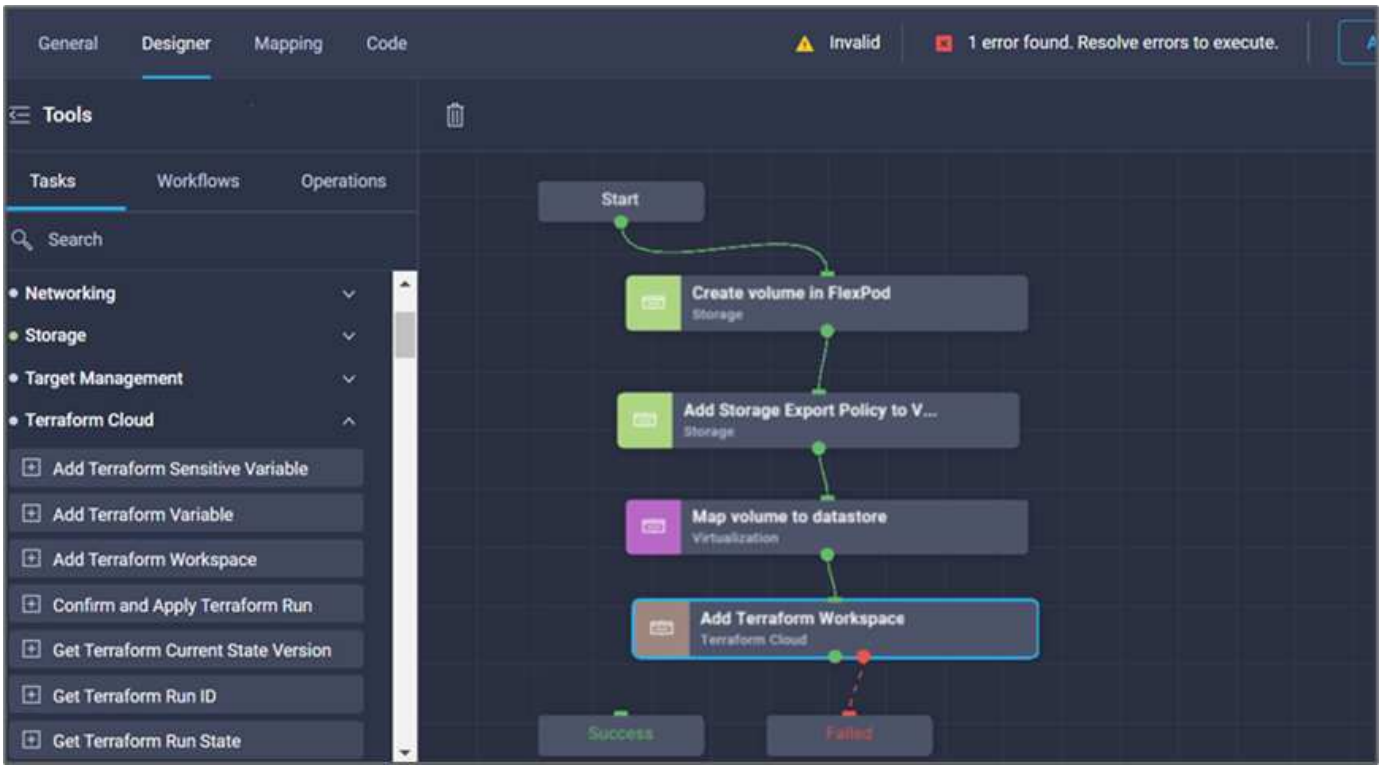
e. Klicken Sie auf den **Zugriffsmodus**. Der Zugriffsmodus gilt für den NFS-Server. Klicken Sie auf schreibgeschützt, wenn Volumes als schreibgeschützt exportiert werden. Klicken Sie Auf **Hinzufügen**.



30. Klicken Sie Auf **Karte**.
31. Klicken Sie Auf **Speichern**.

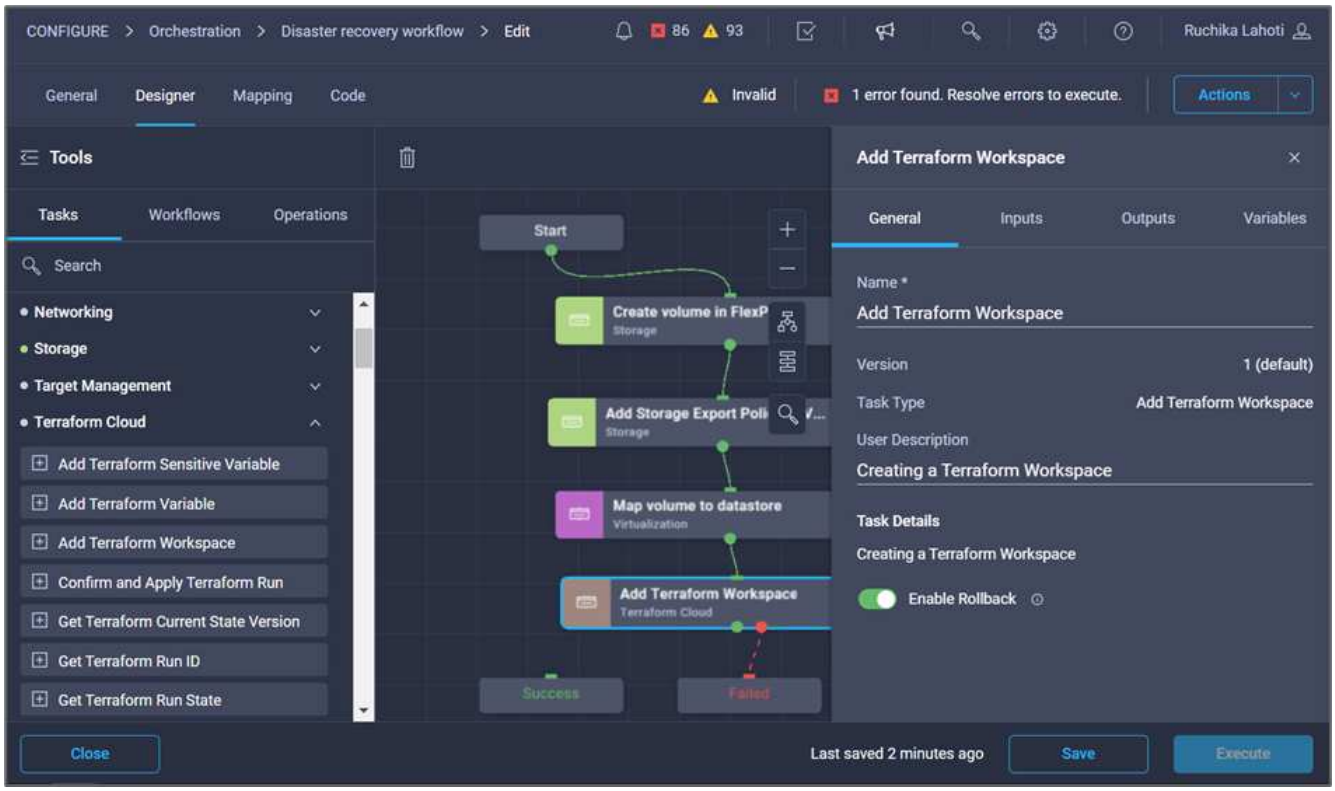


Damit ist die Erstellung des Datastores abgeschlossen. Alle im On- Premises-FlexPod-Datacenter ausgeführten Aufgaben werden abgeschlossen.

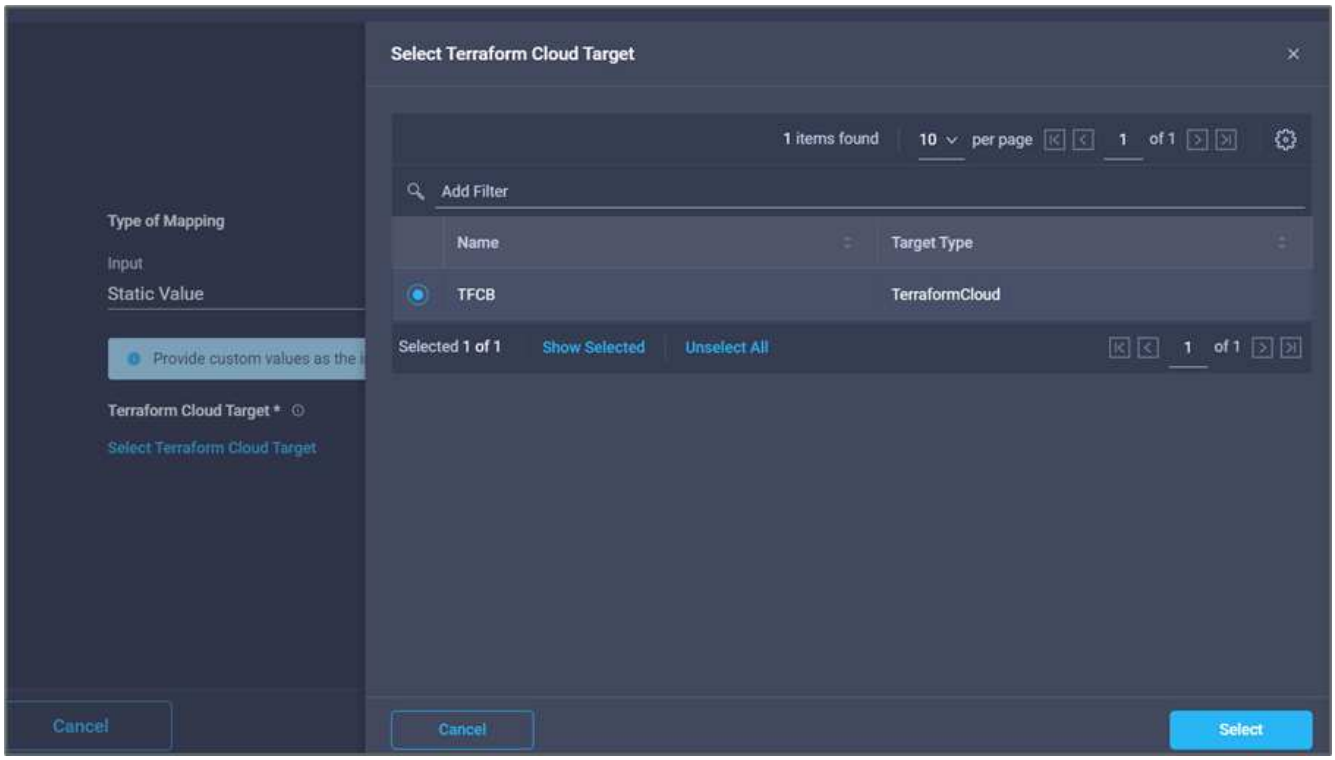


Prozedur 5: Fügen Sie einen neuen Terraform-Arbeitsbereich hinzu

1. Gehen Sie zur Registerkarte **Designer** und klicken Sie im Abschnitt **Tools** auf **Tasks**.
2. Ziehen Sie die Aufgabe **Terraform Cloud > Terraform Workspace** hinzufügen aus dem Abschnitt Extras im Designbereich.
3. Verwenden Sie Connector, um die Aufgaben **Kartenvolumen mit Datastore** und **Terraform Workspace hinzufügen** zu verbinden und klicken Sie auf **Speichern**.
4. Klicken Sie Auf **Terraform Workspace Hinzufügen**. Klicken Sie im Bereich Aufgabeneigenschaften auf die Registerkarte **Allgemein**. Optional können Sie den Namen und die Beschreibung für diese Aufgabe ändern.

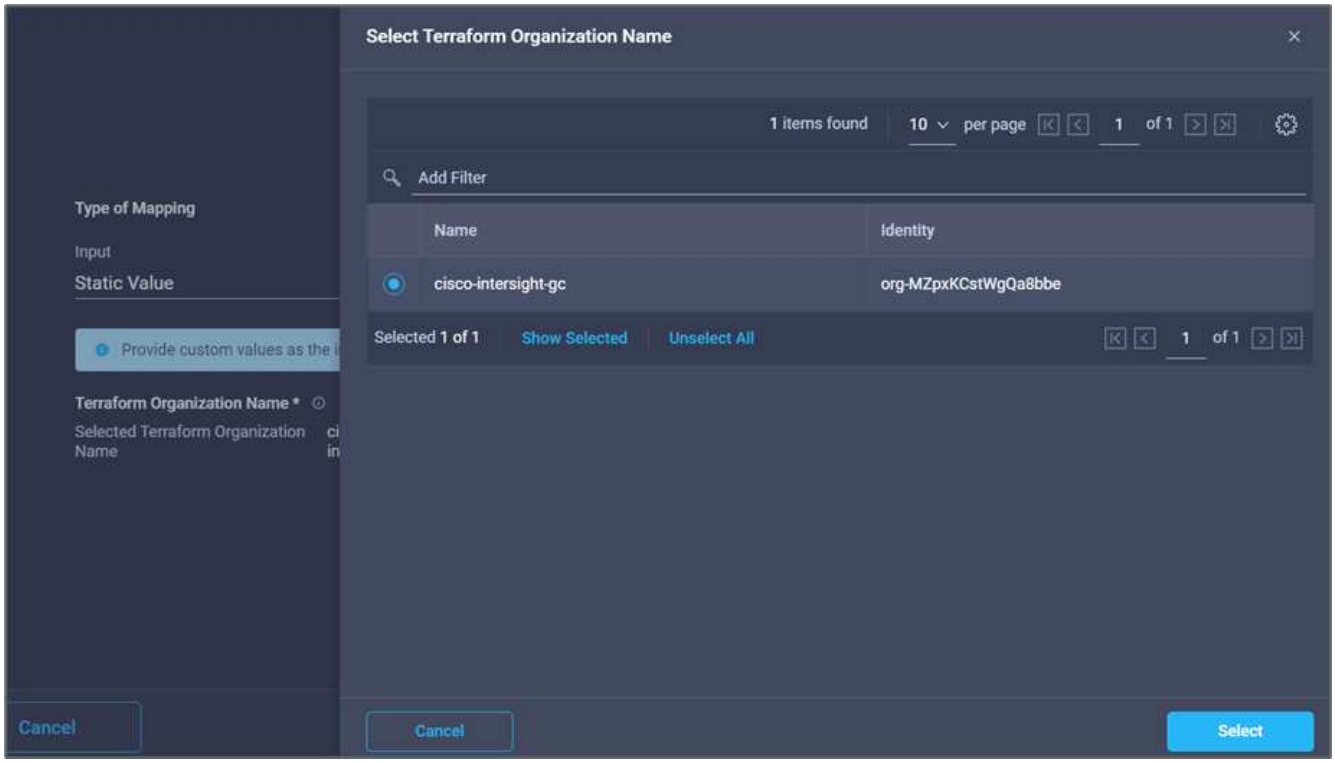


5. Klicken Sie im Bereich Aufgabeneigenschaften auf **Eingaben**.
6. Klicken Sie im Eingabefeld **Terraform Cloud Target** auf **Karte**.
7. Wählen Sie **statischer Wert** und klicken Sie auf **Terraform Cloud Target**. Wählen Sie das Terraform Cloud for Business-Konto aus, das wie in erläutert hinzugefügt wurde "Konfigurieren Sie Cisco Intersight Service für HashiCorp Terraform".“.

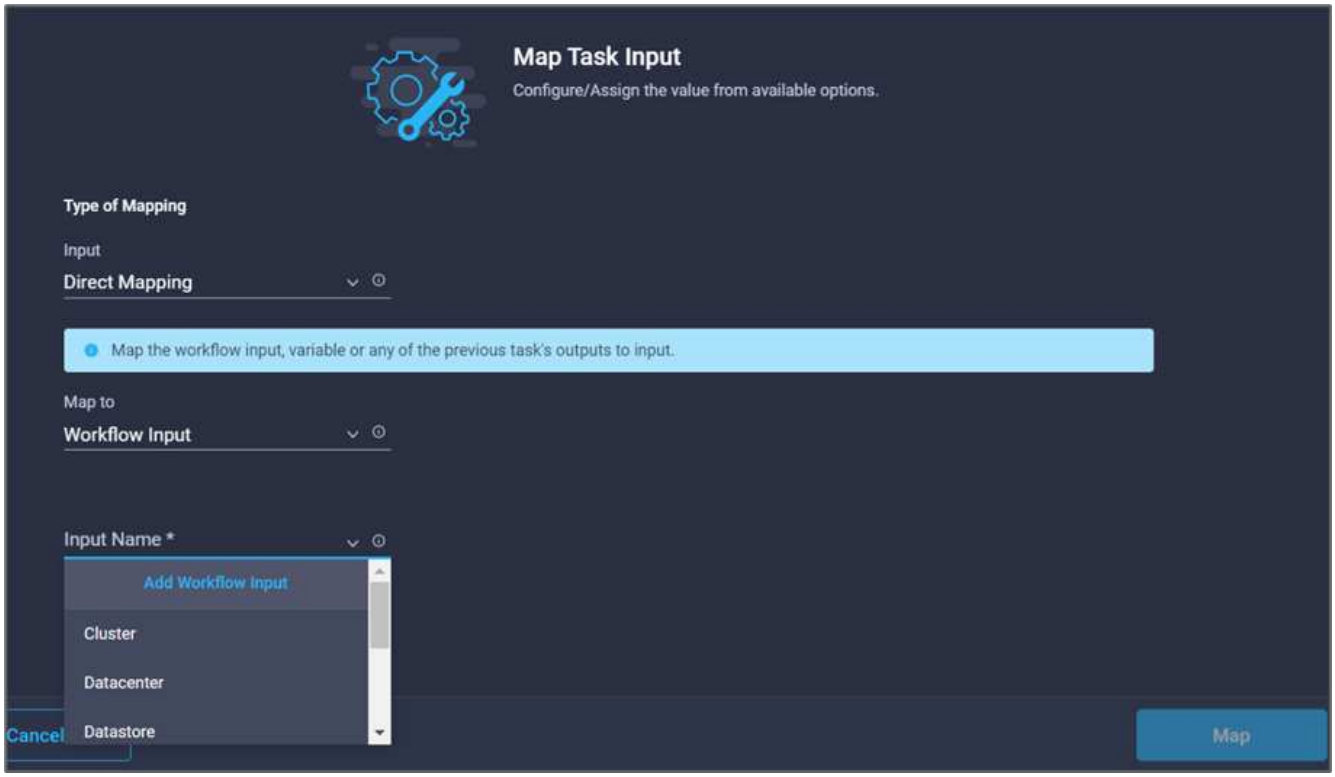


8. Klicken Sie Auf **Karte**.

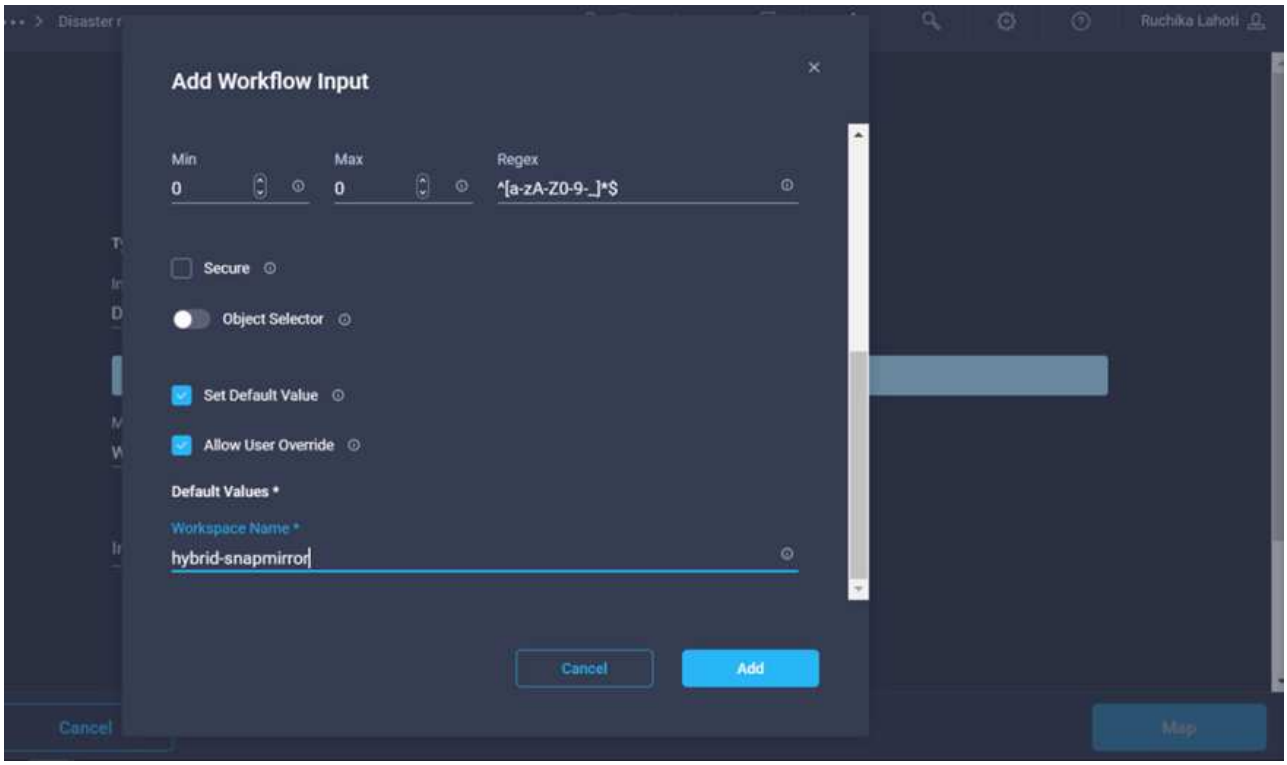
9. Klicken Sie im Eingabefeld **Terraform Organisationsname** auf **Karte**.
10. Wählen Sie **statischer Wert** und klicken Sie dann auf **Terraform-Organisation auswählen**. Wählen Sie den Namen der Terraform-Organisation aus, der Sie in Ihrem Terraform Cloud for Business-Account gehören.



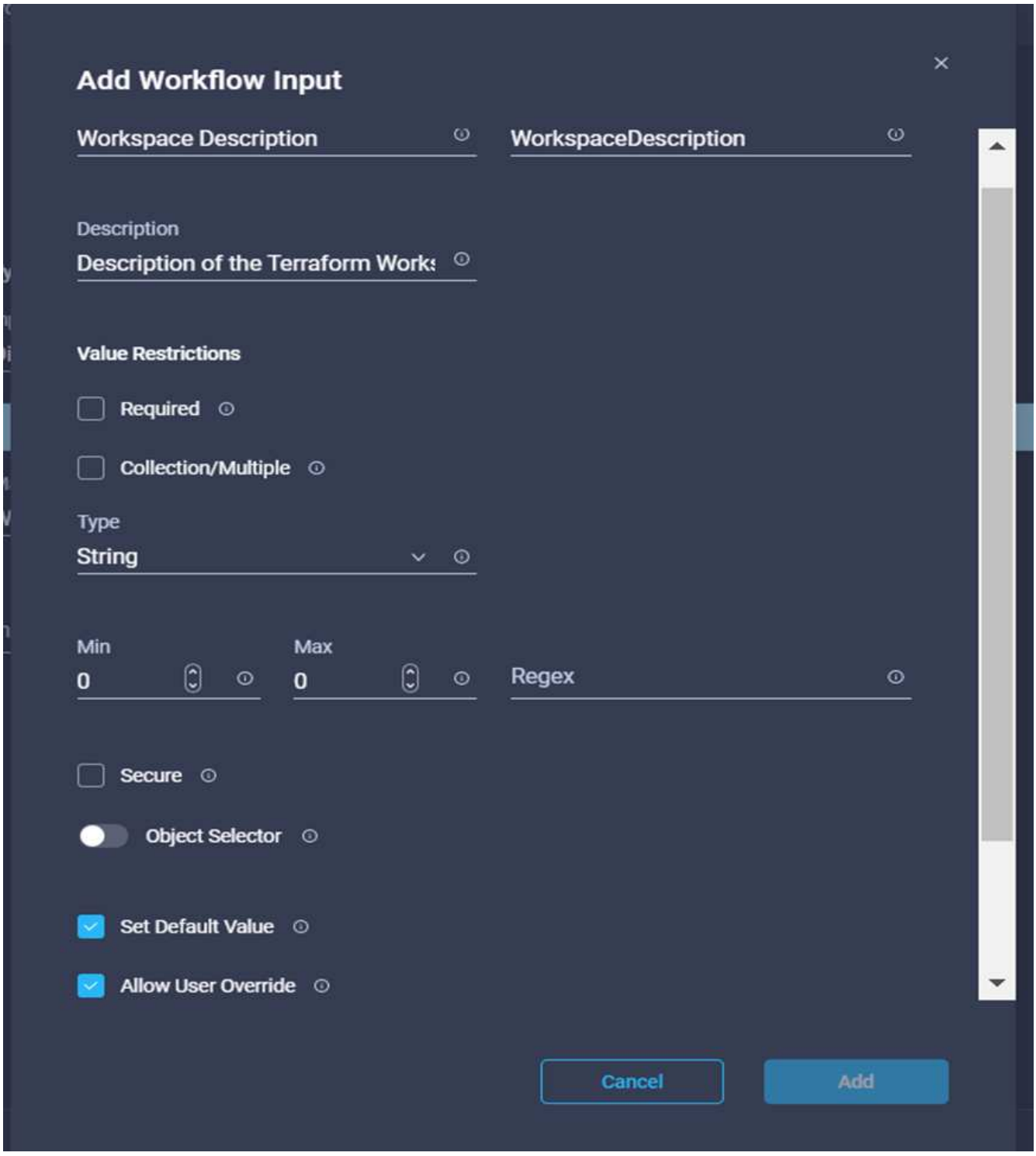
11. Klicken Sie Auf **Karte**.
12. Klicken Sie im Feld * Terraform Workspace Name* auf **Karte**. Dies ist der neue Workspace im Terraform Cloud for Business Account.
13. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Workflow-Eingabe**.
14. Klicken Sie auf **Eingabename** und **Workflow-Eingabe erstellen**.



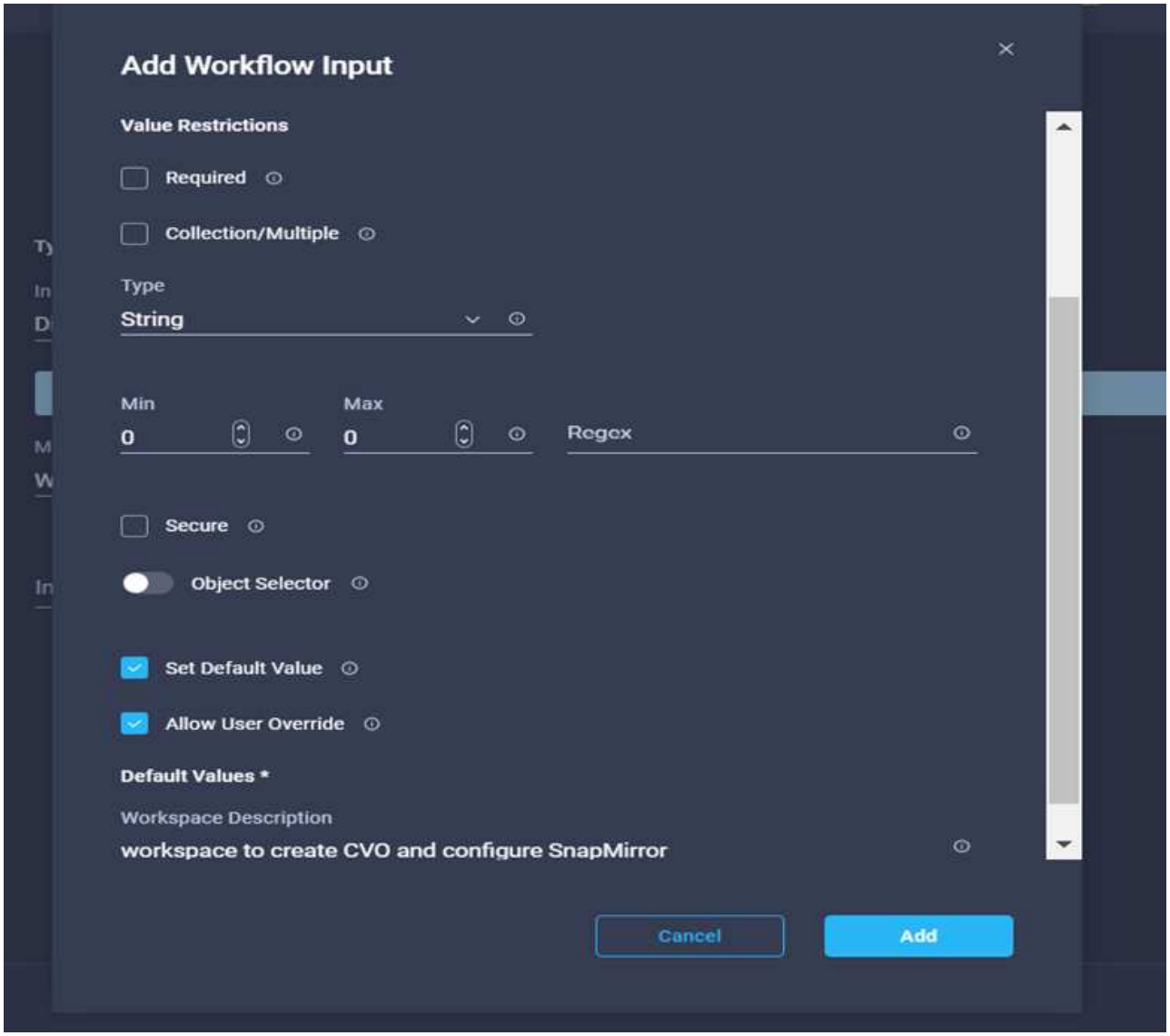
15. Führen Sie im Add Input Wizard die folgenden Schritte aus:
    a. Geben Sie einen Anzeigenamen und einen Referenznamen an (optional).
    b. Klicken Sie Auf * Erforderlich*.
    c. Achten Sie darauf, **String** für **Typ** auszuwählen.
    d. Klicken Sie auf **Standardwert festlegen und überschreiben**.
    e. Geben Sie einen Standardnamen für den Arbeitsbereich an.
    f. Klicken Sie Auf **Hinzufügen**.



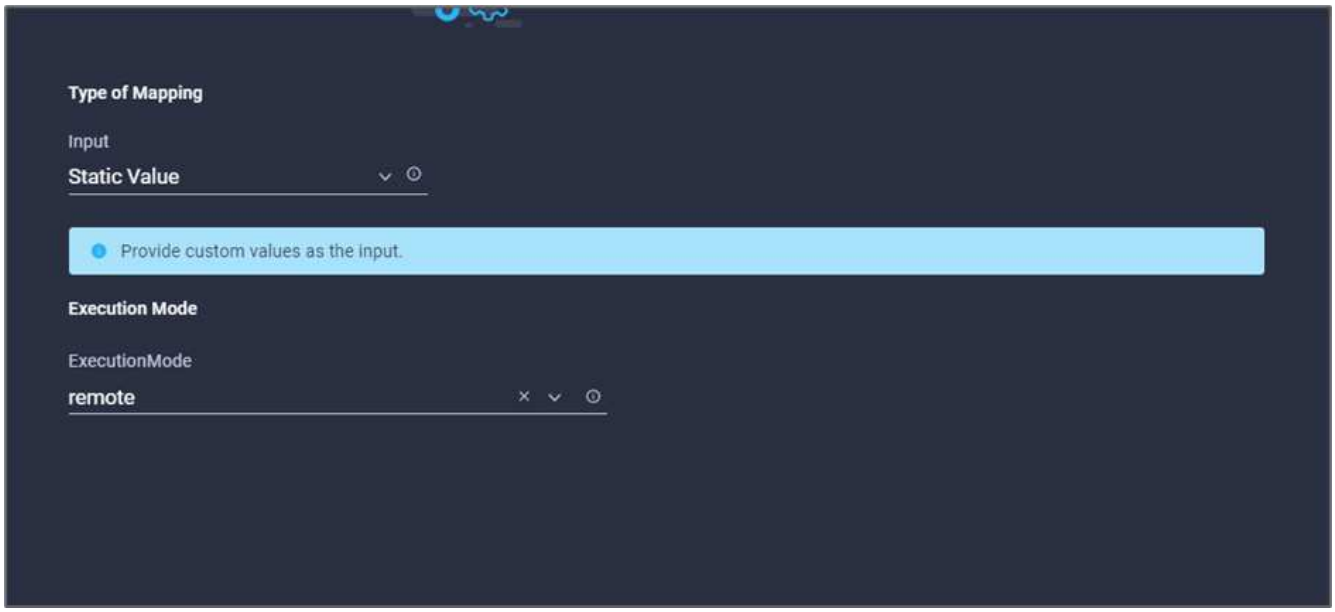
16. Klicken Sie Auf **Karte**.
17. Klicken Sie im Feld **Workspace Beschreibung** auf **Karte**.
18. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Workflow-Eingabe**.
19. Klicken Sie auf **Eingabename** und **Workflow-Eingabe erstellen**.



20. Führen Sie im Add Input Wizard die folgenden Schritte aus:
    a. Geben Sie einen Anzeigenamen und einen Referenznamen an (optional).
    b. Achten Sie darauf, **String** für **Typ** auszuwählen.
    c. Klicken Sie auf **Standardwert festlegen und überschreiben**.
    d. Geben Sie eine Beschreibung des Arbeitsbereichs ein, und klicken Sie auf **Hinzufügen**.



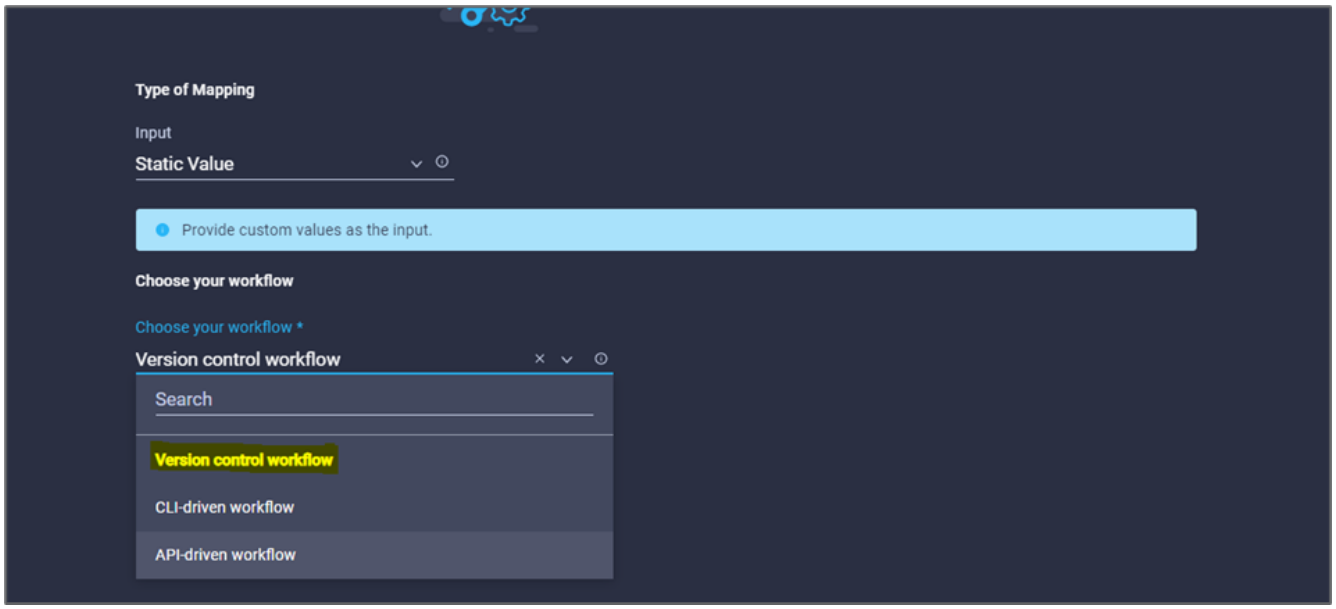
21. Klicken Sie Auf **Karte**.
22. Klicken Sie im Feld **Ausführungsmodus** auf **Karte**.
23. Wählen Sie **statischer Wert**, klicken Sie auf **Ausführungsmodus** und dann auf **Remote**.



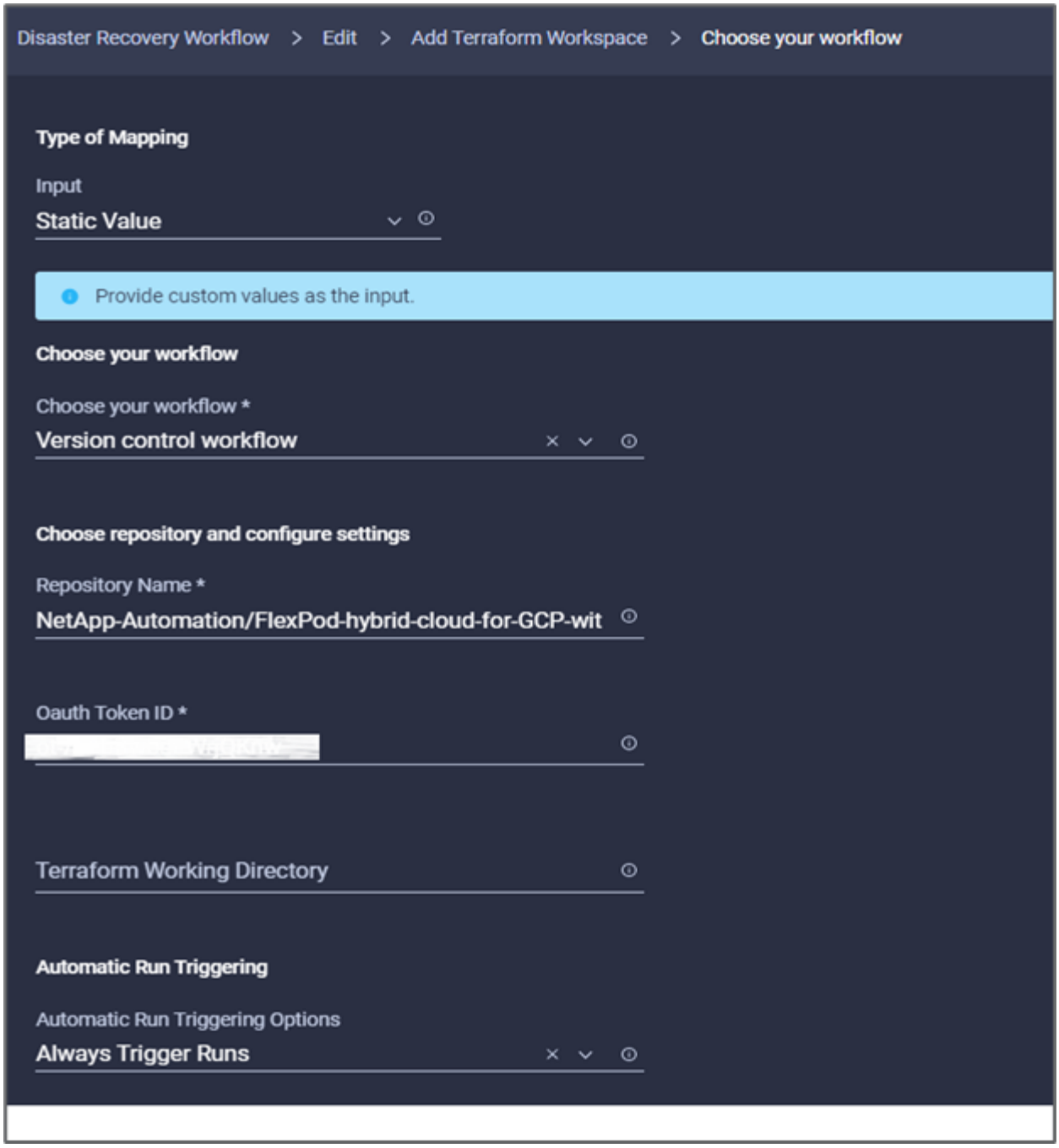
24. Klicken Sie Auf **Karte**.
25. Klicken Sie im Feld **Methode anwenden** auf **Karte**.
26. Wählen Sie **statischer Wert** und klicken Sie auf **Methode anwenden**. Klicken Sie Auf **Manuelle Anwendung**.

27. Klicken Sie Auf **Karte**.
28. Klicken Sie im Feld **Benutzeroberfläche** auf **Karte**.
29. Wählen Sie **statischer Wert** und klicken Sie auf **Benutzeroberfläche**. Klicken Sie auf **Konsole-UI**.

30. Klicken Sie Auf **Karte**.
31. Klicken Sie im Eingabefeld auf **Karte** und wählen Sie Ihren Workflow aus.
32. Wählen Sie **statischer Wert** aus, und klicken Sie auf **Wählen Sie Ihren Workflow**. Klicken Sie Auf **Versionskontrollworkflow**.



33. Geben Sie die folgenden GitHub Repository-Details an:
    a. Geben Sie unter **Repository-Name** den Namen des Repositorys ein, der im Abschnitt aufgeführt ist "„Voraussetzungen für die Umgebung einrichten“".
    b. Geben Sie die OAuth Token-ID wie im Abschnitt beschrieben an "„Voraussetzungen für die Umgebung einrichten“".
    c. Wählen Sie die Option **Automatisches Ausführen-Triggering** aus.



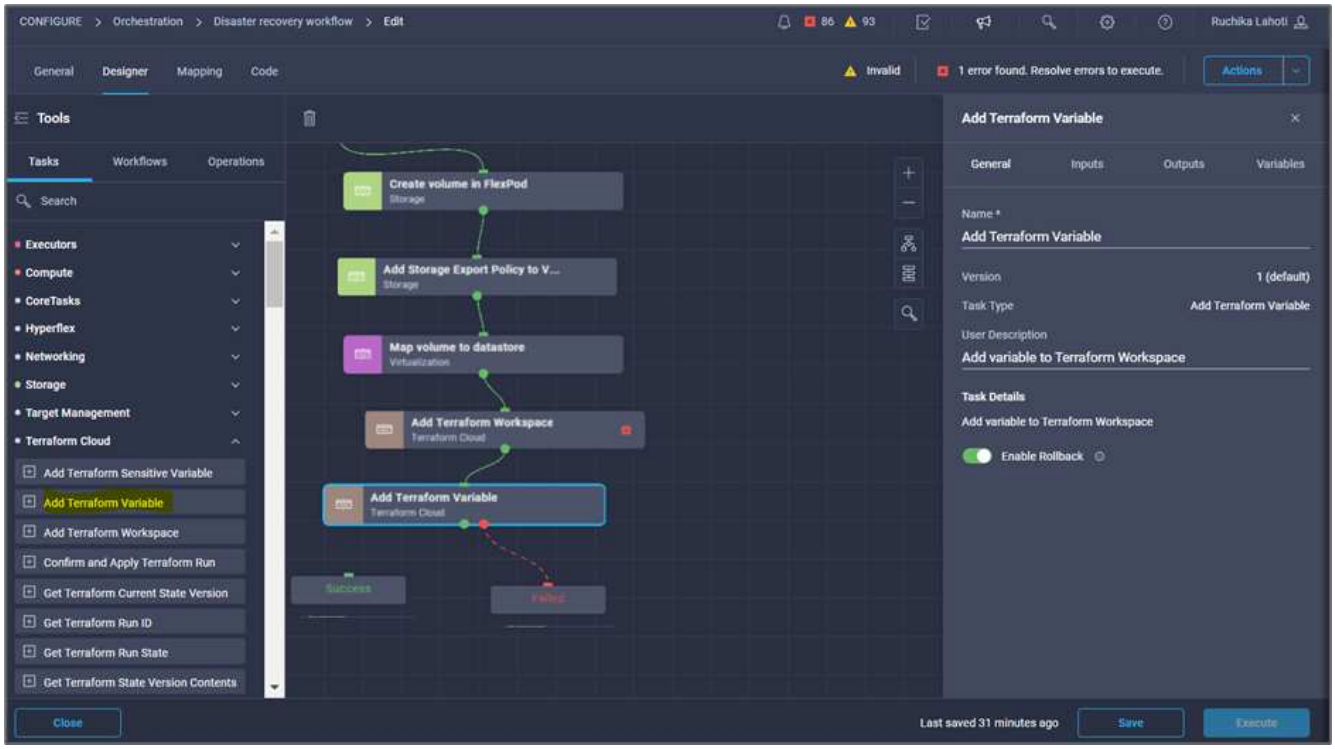
34. Klicken Sie Auf **Karte**.
35. Klicken Sie Auf **Speichern**.

Damit ist die Erstellung eines Workspace in einem Terraform Cloud for Business-Konto abgeschlossen.

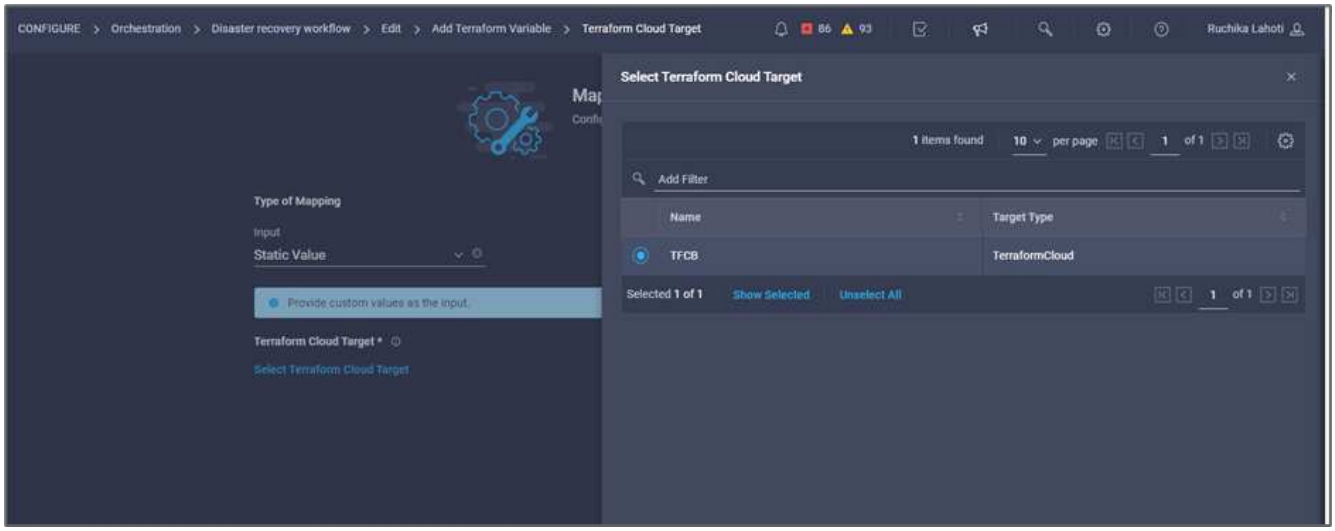
Prozedur 6: Fügen Sie dem Arbeitsbereich nicht-sensible Variablen hinzu

1. Gehen Sie zur Registerkarte **Designer** und klicken Sie auf den Abschnitt **Workflows aus Tools**.
2. Ziehen Sie den Workflow **Terraform > Terraform Variablen** hinzufügen aus dem Abschnitt **Tools** im Bereich **Design**.
3. Verwenden Sie den Connector, um die Aufgaben **Terraform Workspace hinzufügen** und **Terraform-Variablen hinzufügen** zu verbinden. Klicken Sie Auf **Speichern**.

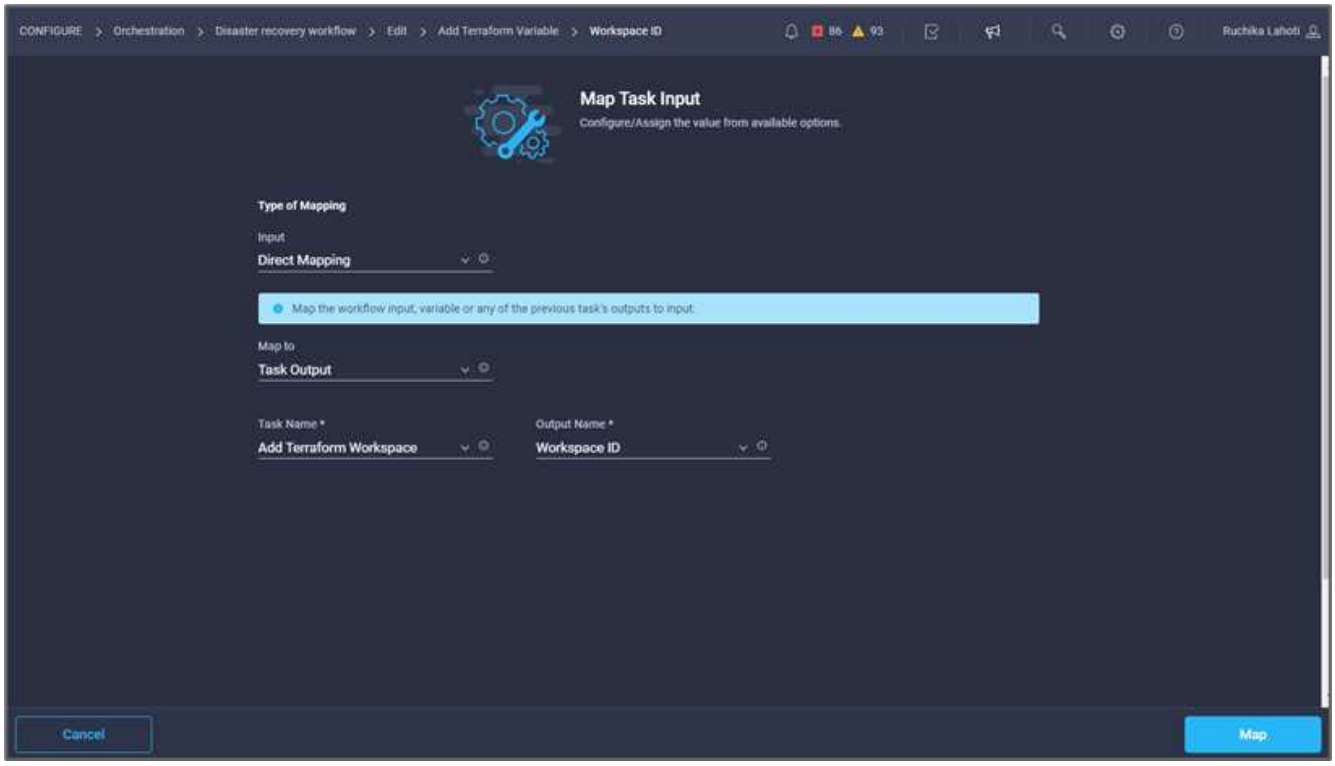
4. Klicken Sie Auf **Terraform-Variablen Hinzufügen**. Klicken Sie im Bereich **Workflow-Eigenschaften** auf die Registerkarte **Allgemein**. Optional können Sie den Namen und die Beschreibung für diese Aufgabe ändern.



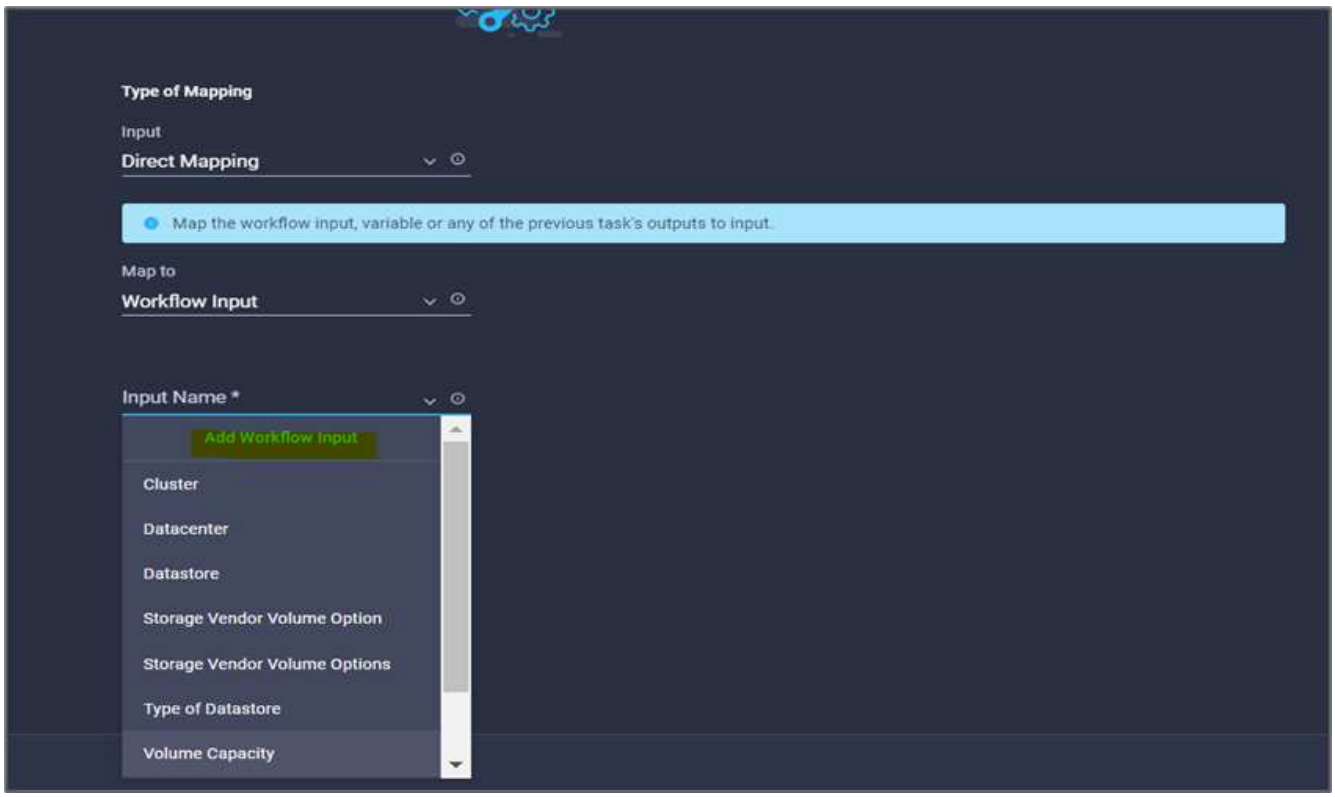
5. Klicken Sie im Bereich **Workflow-Eigenschaften** auf **Eingaben**.
6. Klicken Sie im Feld **Terraform Cloud Target** auf **Karte**.
7. Wählen Sie **statischer Wert** und klicken Sie auf **Terraform Cloud Target**. Wählen Sie das Terraform Cloud for Business-Konto aus, das wie in erläutert hinzugefügt wurde "Konfigurieren Sie Cisco Intersight Service für HashiCorp Terraform".“.



8. Klicken Sie Auf **Karte**.
9. Klicken Sie im Feld **Terraform Organisationsname *auf *Karte**.
10. Wählen Sie **statischer Wert** und klicken Sie auf **Terraform-Organisation auswählen**. Wählen Sie den Namen der Terraform-Organisation aus, der Sie in Ihrem Terraform Cloud for Business-Account gehören.

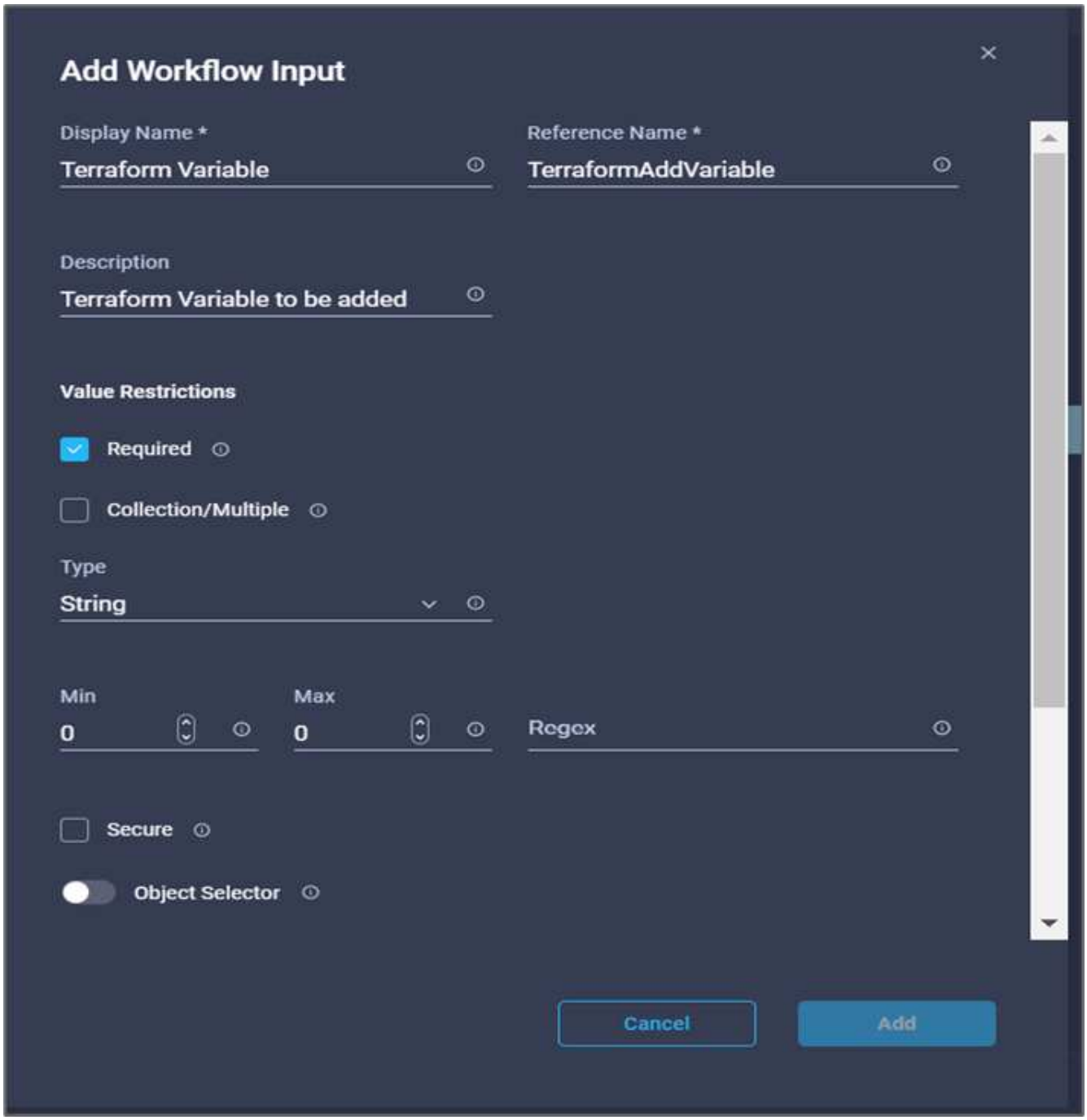


11. Klicken Sie Auf **Karte**.
12. Klicken Sie im Feld * Terraform Workspace Name* auf **Karte**.
13. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Aufgabenausgabe**.
14. Klicken Sie auf **Aufgabenname** und klicken Sie auf **Terraform Workspace hinzufügen**.



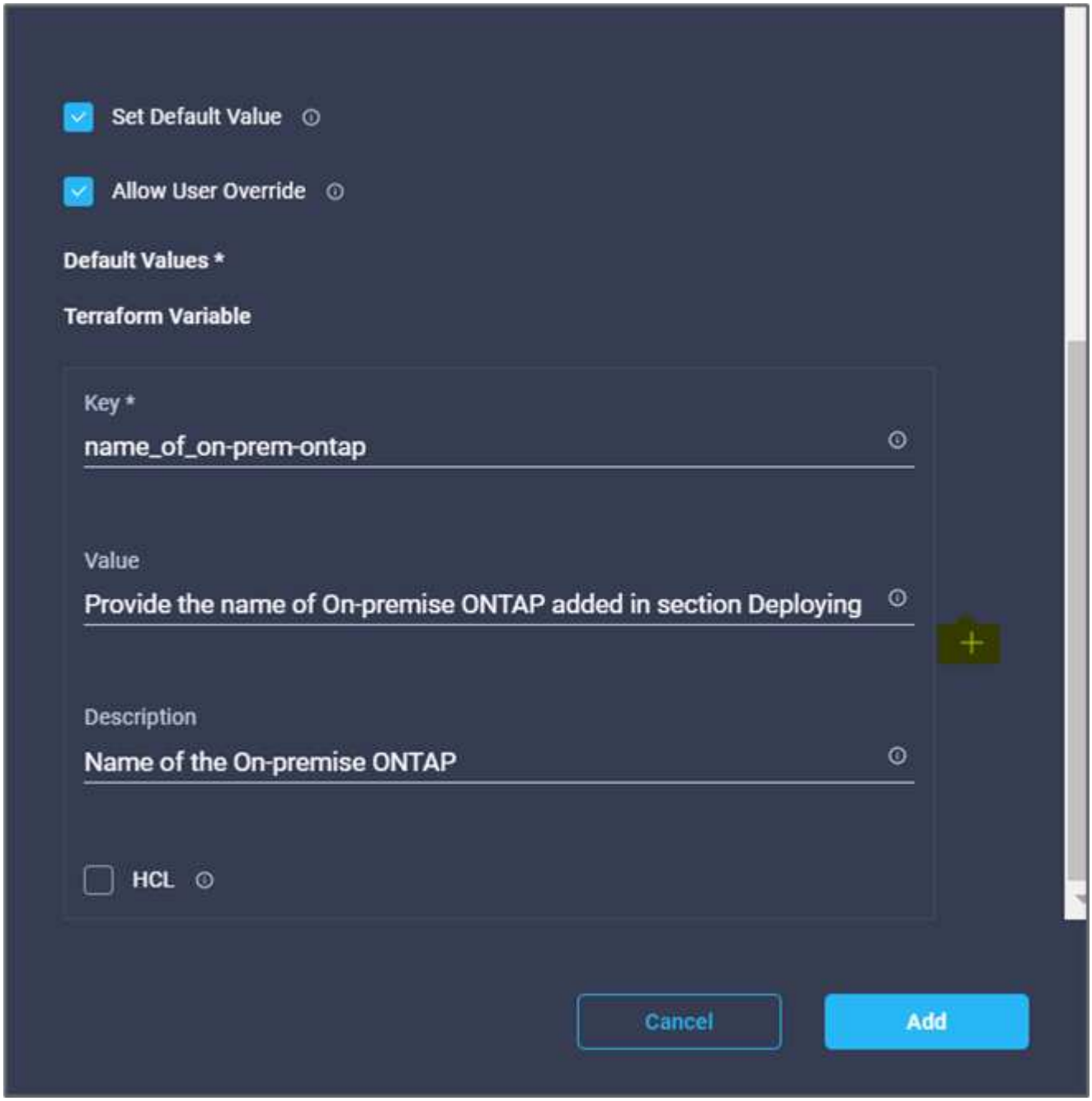
15. Klicken Sie auf **Ausgabename** und dann auf **Workspace Name**.

16. Klicken Sie Auf **Karte**.
17. Klicken Sie im Feld **Variablen hinzufügen Optionen** auf **Karte**.
18. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Workflow-Eingabe**.
19. Klicken Sie auf **Eingabename** und **Workflow-Eingabe erstellen**.



20. Führen Sie im Add Input Wizard die folgenden Schritte aus:
    a. Geben Sie einen Anzeigenamen und einen Referenznamen an (optional).
    b. Achten Sie darauf, **String** für den **Typ** auszuwählen.
    c. Klicken Sie auf **Standardwert festlegen und überschreiben**.
    d. Klicken Sie auf **Variablentyp** und dann auf **nicht-sensible Variablen**.

21. Geben Sie im Abschnitt **Terraform-Variablen** folgende Informationen ein:
    - **Schlüssel.** `name_of_on-prem-ontap`
    - **Wert.** geben Sie den Namen von On-Premise ONTAP an.
    - **Beschreibung.** Name des On-Premise ONTAP.
22. Klicken Sie auf **+**, um weitere Variablen hinzuzufügen.

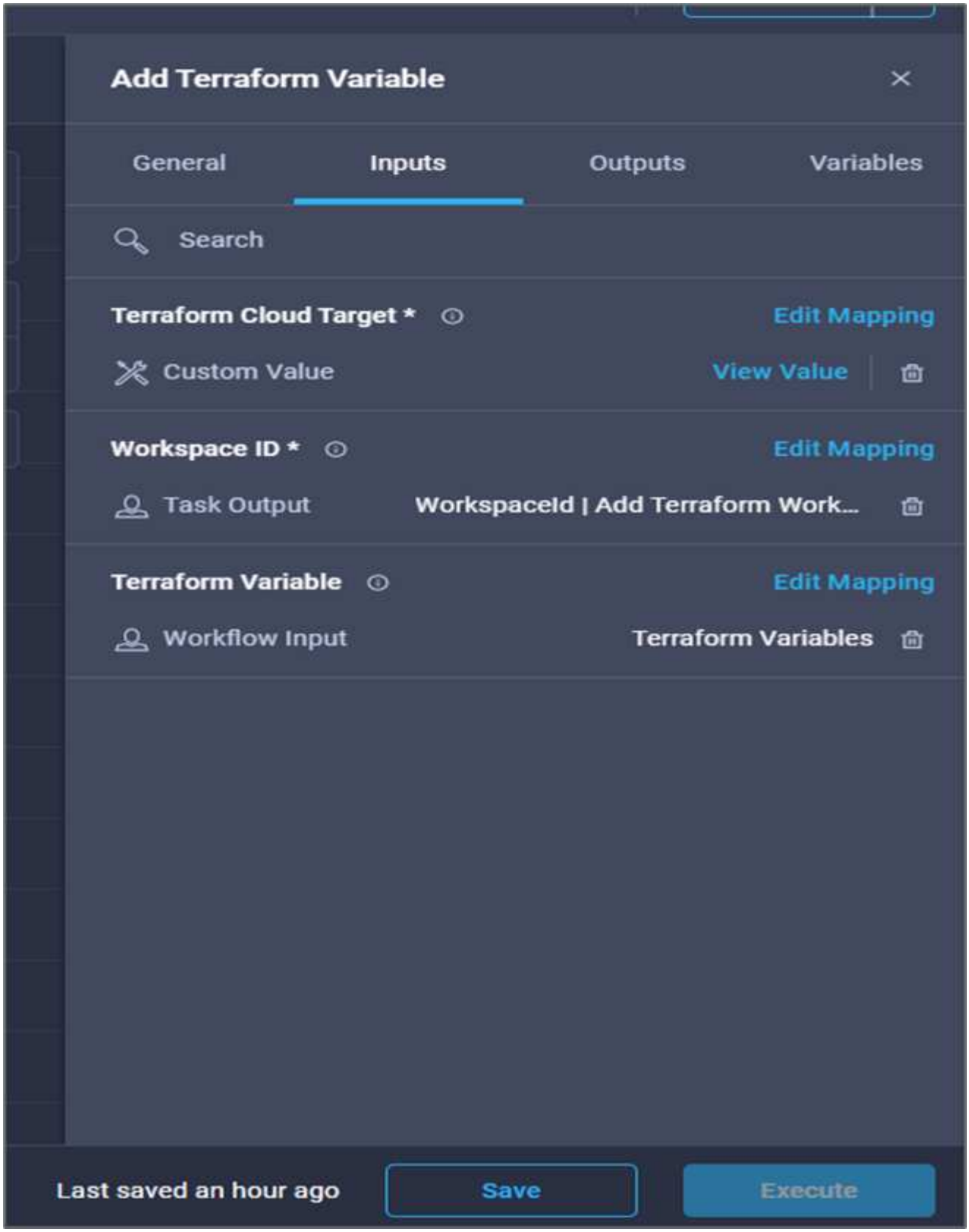


23. Fügen Sie alle Terraform-Variablen wie in der folgenden Tabelle dargestellt hinzu. Sie können auch einen Standardwert angeben.

Terraform Variablenname	Beschreibung
Name_von_On-Prem-ontap	Name des On-Premises-ONTAP (FlexPod)

Terraform Variablenname	Beschreibung
On-Prem-ontap_Cluster_ip	Die IP-Adresse der Managementoberfläche des Storage-Clusters
On-Prem-ontap_user_Name	Admin-Benutzername für das Storage-Cluster
Zone	GCP-Region, in der die Arbeitsumgebung erstellt wird
Subnetz_id	GCP-Subnetz-id, an der die Arbeitsumgebung erstellt wird
vpc_id	Die VPC-ID, mit der die Arbeitsumgebung erstellt wird
Capacity_package_Name	Der zu verwendende Lizenztyp
Quell-Volume	Der Name des Quell-Volume
Source_Storage_vm_Name	Der Name der Quell-SVM
Ziel_Volume	Name des Volumes auf Cloud Volumes ONTAP
Schedule_of_Replication	Der Standardwert ist 1 Stunde
Name_von_Volume_to_create_on_cvo	Name des Cloud Volume
Workspace_id	Workspace_id, in der die Arbeitsumgebung erstellt wird
Projekt_id	Die Projekt_id, in der die Arbeitsumgebung erstellt wird
Name_des_cvo_Clusters	Der Name der Cloud Volumes ONTAP-Arbeitsumgebung
gcp_Service_Account	gcp_Service_Account der Cloud Volumes ONTAP-Arbeitsumgebung

24. Klicken Sie auf **Karte** und dann auf **Speichern**.



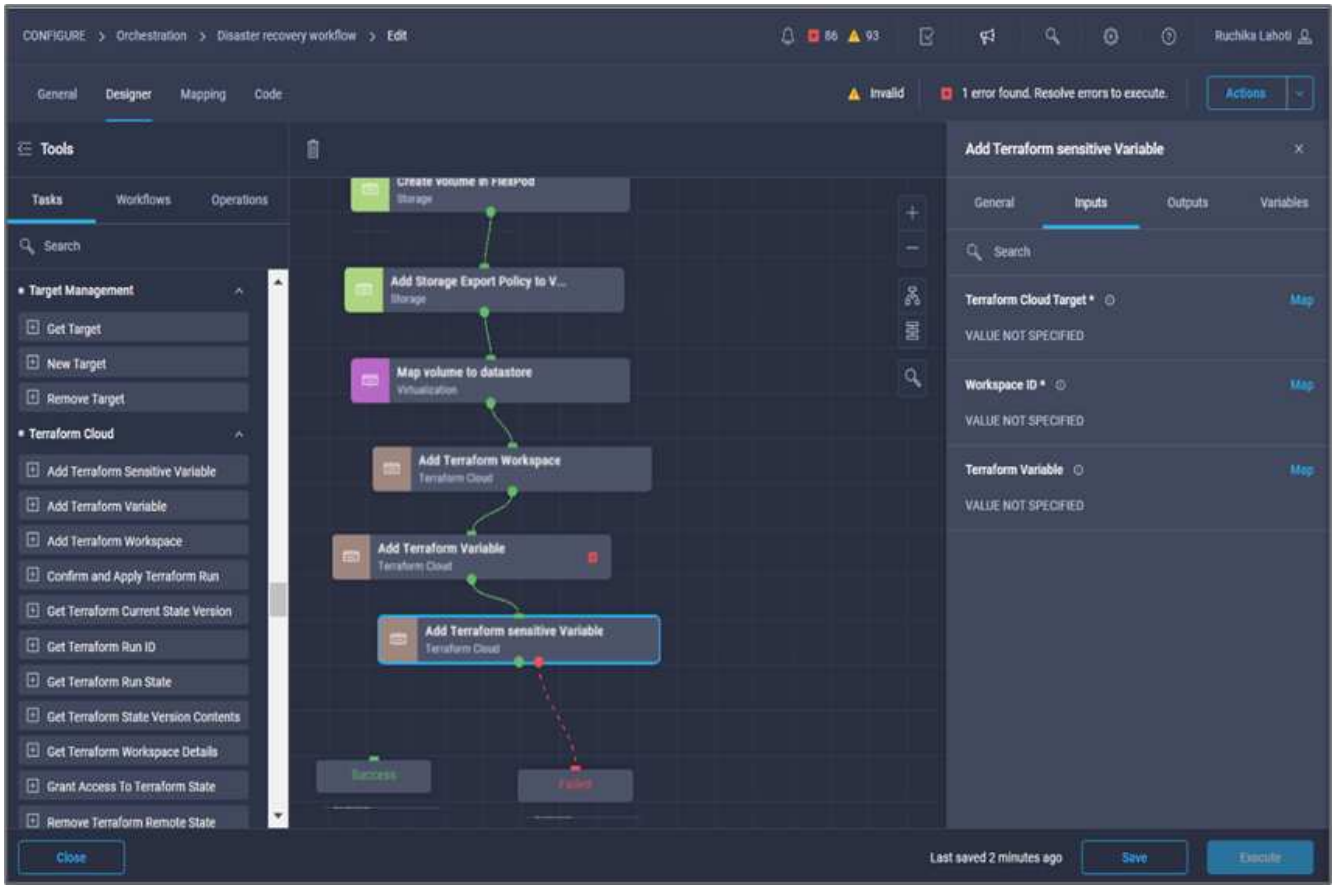
Damit ist das Hinzufügen der erforderlichen Terraform-Variablen zum Arbeitsbereich abgeschlossen. Fügen Sie anschließend die erforderlichen sensiblen Terraform-Variablen zum Arbeitsbereich hinzu. Sie können beide auch zu einer einzigen Aufgabe kombinieren.

Prozedur 7: Fügen Sie sensible Variablen zu einem Arbeitsbereich hinzu

1. Gehen Sie zur Registerkarte **Designer** und klicken Sie im Abschnitt **Tools** auf **Workflows**.
2. Ziehen Sie den Workflow **Terraform > Terraform Variablen** hinzufügen aus dem Abschnitt **Tools** im Bereich **Design**.
3. Verwenden Sie den Connector, um die beiden **Terraform Workspace**-Tasks hinzuzufügen. Klicken Sie Auf **Speichern**.

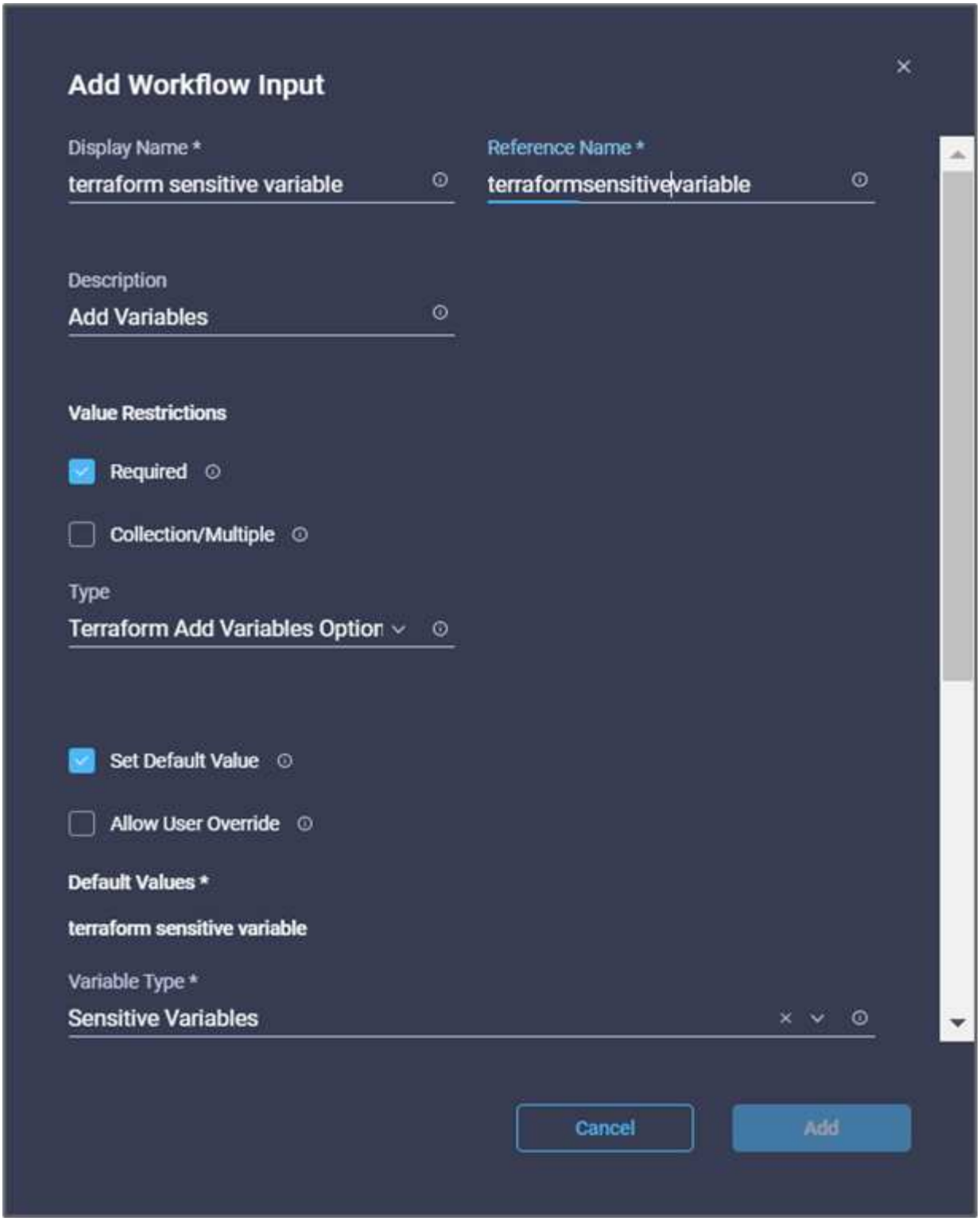
> Es wird eine Warnung angezeigt, die angibt, dass die beiden Aufgaben denselben Namen haben. Ignorieren Sie den Fehler für jetzt, da Sie den Aufgabennamen im nächsten Schritt ändern.

4. Klicken Sie Auf **Terraform-Variablen Hinzufügen**. Klicken Sie im Bereich **Workflow-Eigenschaften** auf die Registerkarte **Allgemein**. Ändern Sie den Namen in **Terraform sensible Variablen hinzufügen**.



5. Klicken Sie im Bereich **Workflow-Eigenschaften** auf **Eingaben**.
6. Klicken Sie im Feld **Terraform Cloud Target** auf **Karte**.
7. Wählen Sie **statischer Wert** und klicken Sie auf **Terraform Cloud Target**. Wählen Sie das Terraform Cloud for Business-Konto aus, das im Abschnitt hinzugefügt wurde "Konfigurieren Sie Cisco Intersight Service für HashiCorp Terraform".“
8. Klicken Sie Auf **Karte**.
9. Klicken Sie im Feld * Terraform Organization Name* auf **Karte**.
10. Wählen Sie **statischer Wert** und klicken Sie auf **Terraform-Organisation auswählen**. Wählen Sie den Namen der Terraform-Organisation aus, der Sie in Ihrem Terraform Cloud for Business-Account gehören.

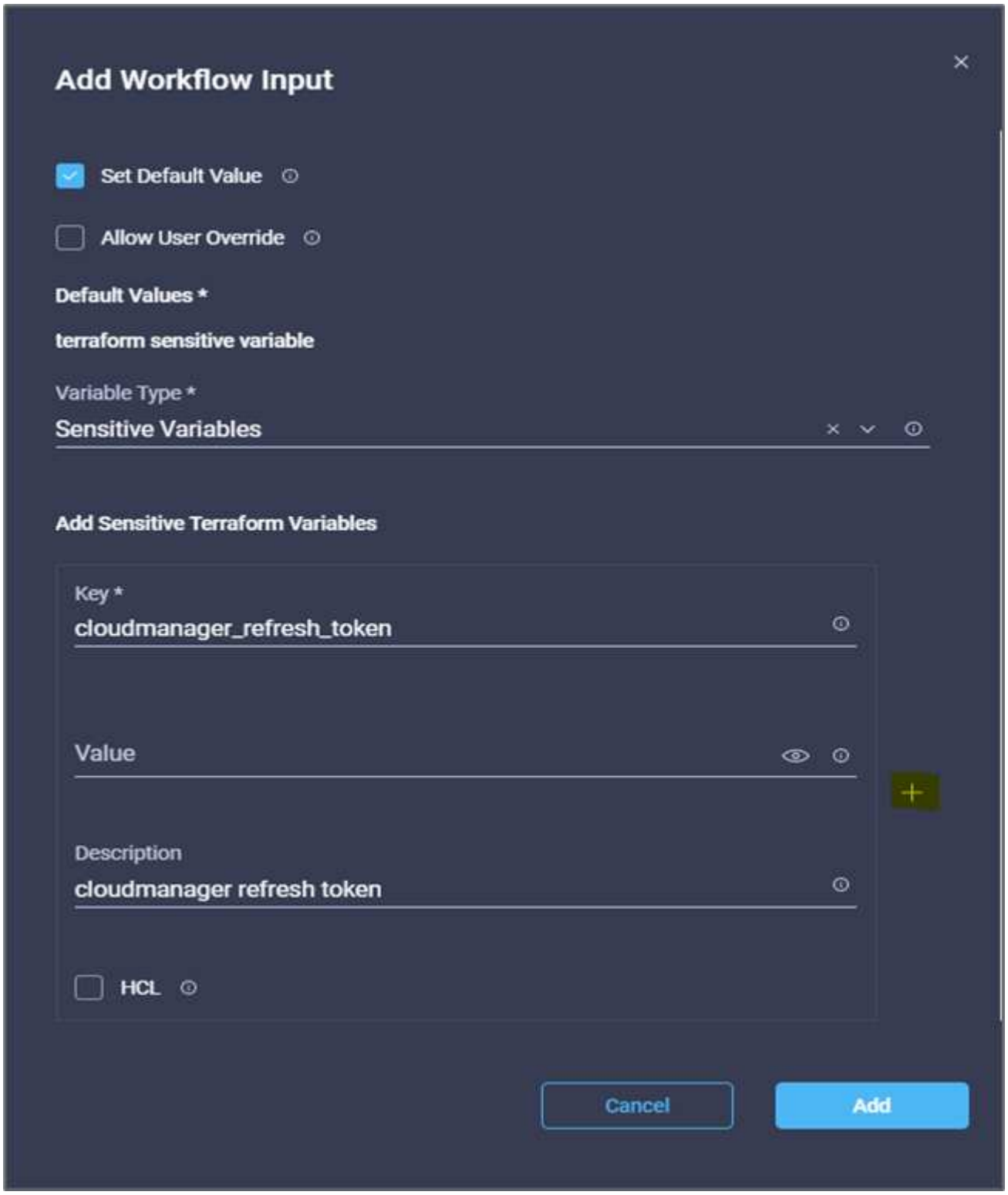
11. Klicken Sie Auf **Karte**.
12. Klicken Sie im Feld * Terraform Workspace Name* auf **Karte**.
13. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Aufgabenausgabe**.
14. Klicken Sie auf **Aufgabenname** und dann auf **Terraform Workspace hinzufügen**.
15. Klicken Sie auf **Ausgabename** und dann auf die Ausgabe **Workspace Name**.
16. Klicken Sie Auf **Karte**.
17. Klicken Sie im Feld **Variablen hinzufügen Optionen** auf **Karte**.
18. Wählen Sie **direkte Zuordnung** und klicken Sie dann auf **Workflow-Eingabe**.
19. Klicken Sie auf **Eingabename** und **Workflow-Eingabe erstellen**.
20. Führen Sie im Add Input Wizard die folgenden Schritte aus:
    a. Geben Sie einen Anzeigenamen und einen Referenznamen an (optional).
    b. Achten Sie darauf, **Terraform Variablen hinzufügen Optionen** für den Typ auszuwählen.
    c. Klicken Sie Auf **Standardwert Festlegen**.
    d. Klicken Sie auf **Variablentyp** und dann auf **sensible Variablen**.
    e. Klicken Sie Auf **Hinzufügen**.



21. Geben Sie im Abschnitt **Terraform-Variablen** folgende Informationen ein:

    - **Schlüssel.** `cloudmanager_refresh_token`.
    - **Wert.** Geben Sie das Aktualisierungs-Token für den NetApp Cloud Manager-API-Betrieb ein.
    - **Beschreibung.** Token aktualisieren.

Weitere Informationen zum Abrufen eines Aktualisierungstoken für den Betrieb der NetApp Cloud Manager API finden Sie im Abschnitt "„Voraussetzungen für die Umgebung einrichten.“"



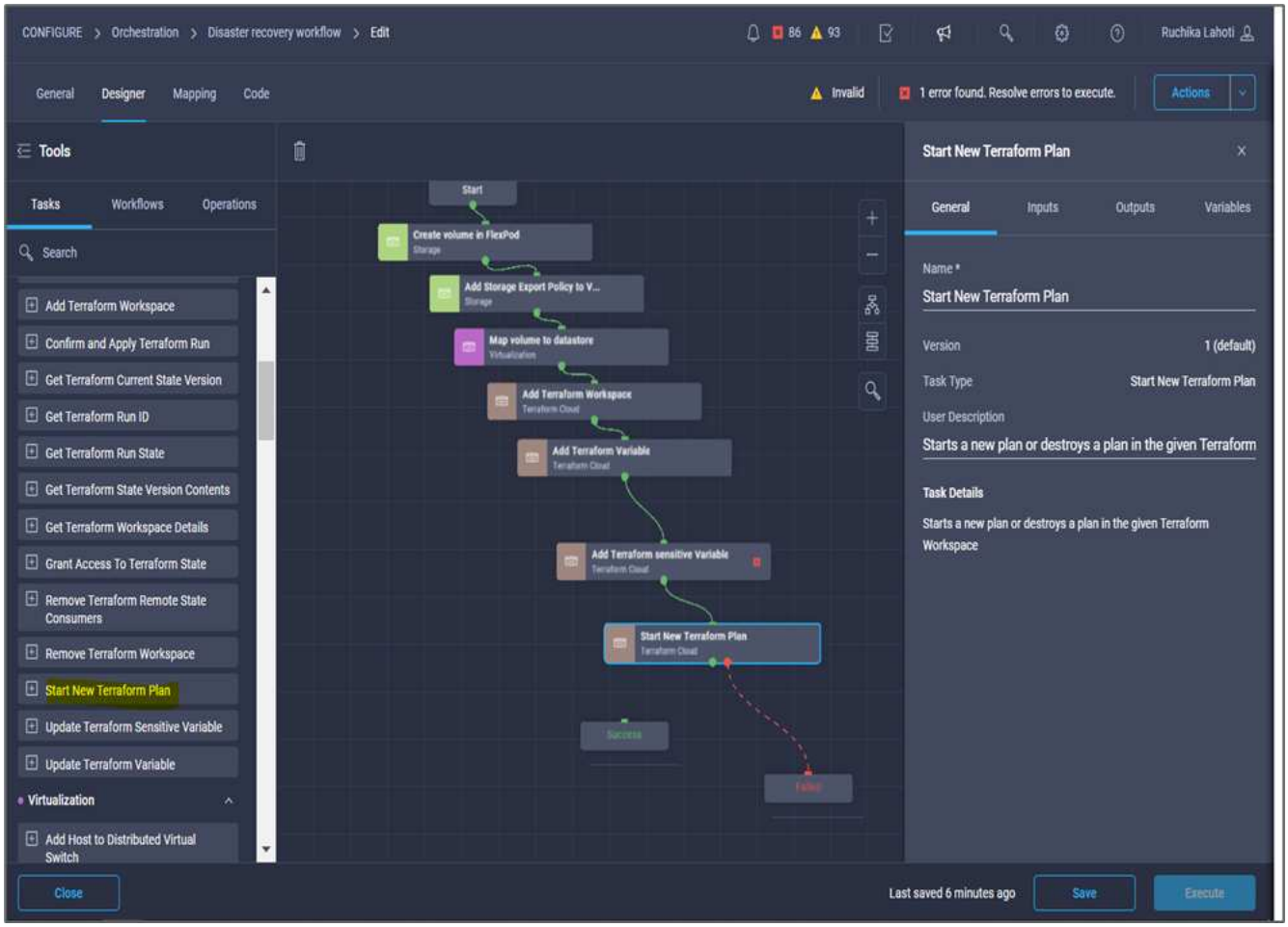
22. Fügen Sie alle Terraform-empfindlichen Variablen hinzu, wie in der nachstehenden Tabelle dargestellt. Sie können auch einen Standardwert angeben.

Terraform-sensibler Variablenname	Beschreibung
CloudManager_Refresh_Token	Token aktualisieren. Erhalten Sie sie von:
Connector_id	Die Client-ID des Cloud Manager Connectors. Beschaffen Sie sie von
cvo_admin_password	Das Admin-Passwort für Cloud Volumes ONTAP
On-Prem-ontap_user_password	Admin-Passwort für das Storage-Cluster

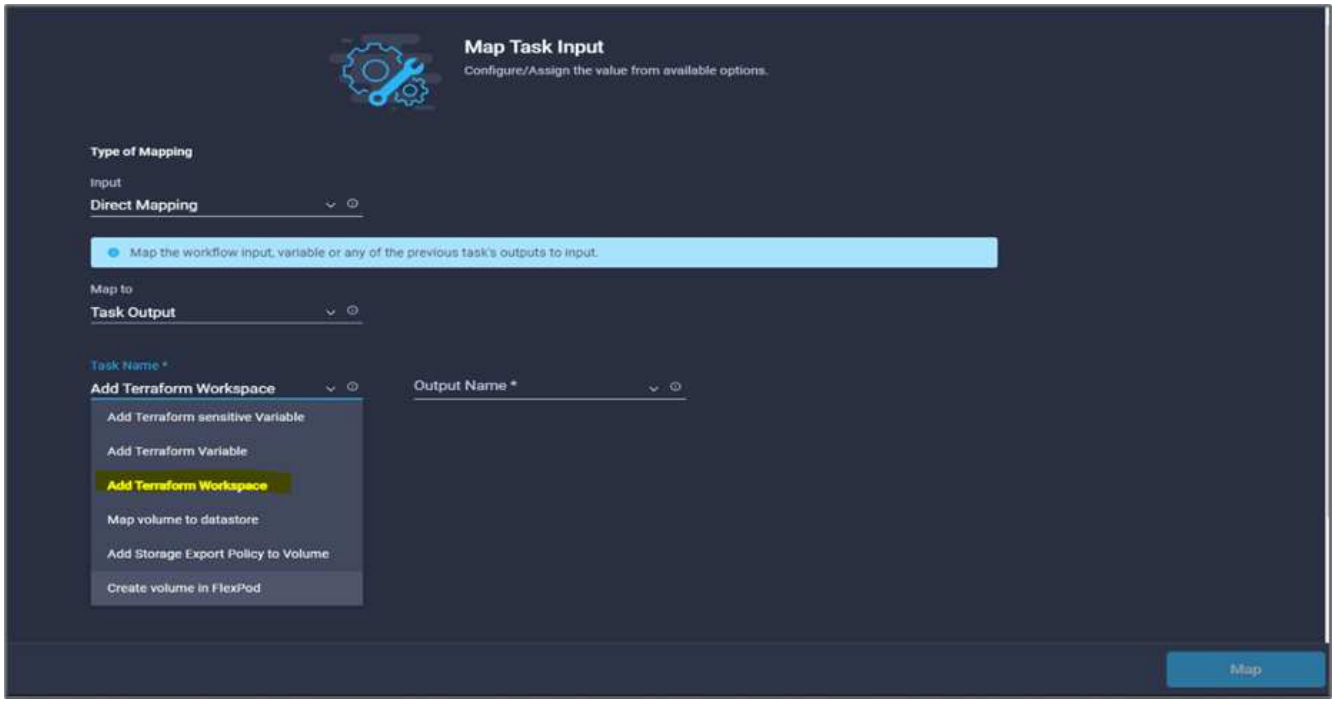
23. Klicken Sie auf **Karte**.damit ist die Aufgabe abgeschlossen, dem Arbeitsbereich die erforderlichen Terraform-empfindlichen Variablen hinzuzufügen. Starten Sie dann einen neuen Terraform-Plan im konfigurierten Arbeitsbereich.

Verfahren 8: Starten Sie einen neuen Terraform-Plan

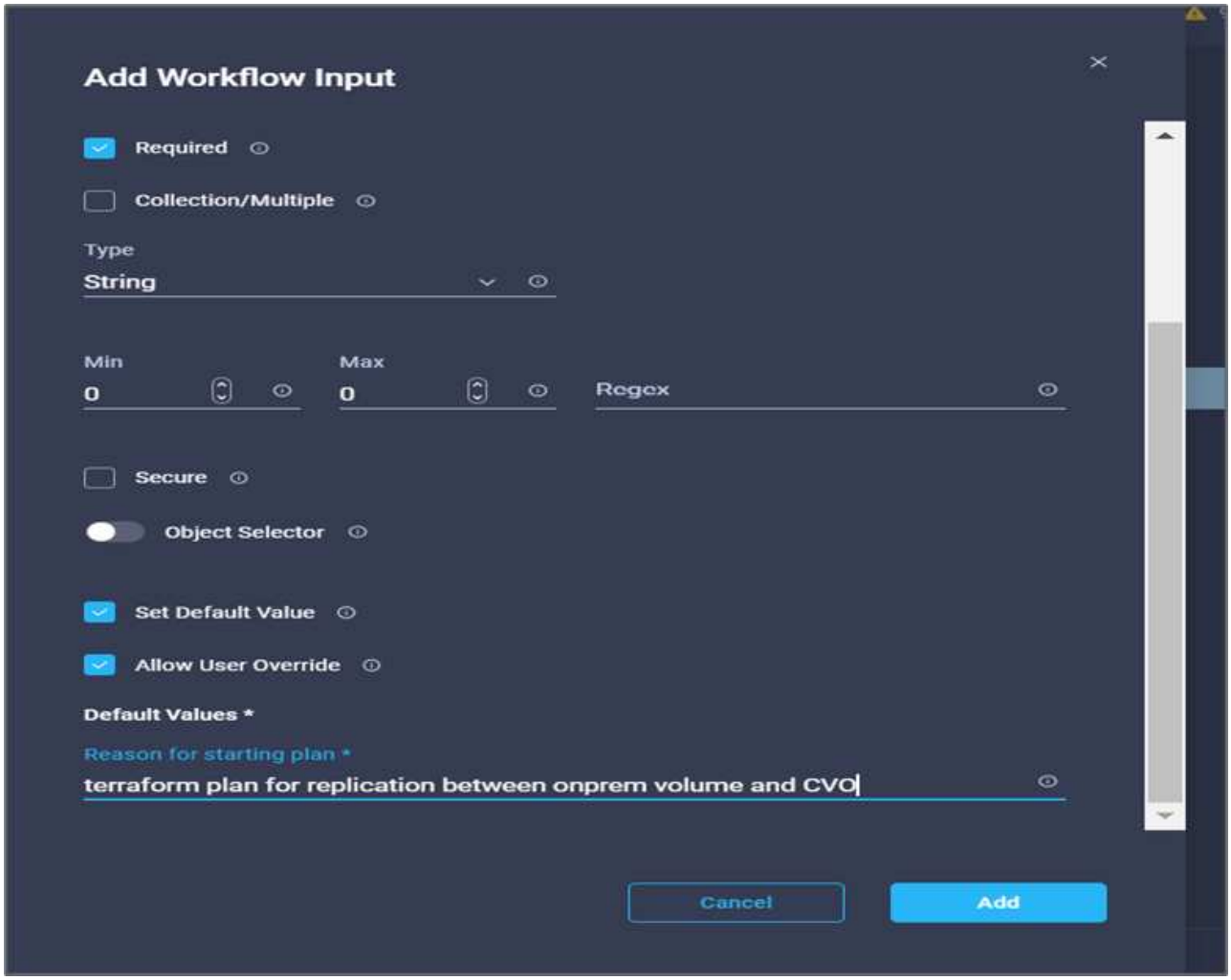
1. Gehen Sie zur Registerkarte **Designer** und klicken Sie im Abschnitt **Tools** auf **Tasks**.
2. Ziehen Sie die Aufgabe **Terraform Cloud > Neue Terraform Plan** aus dem Abschnitt **Tools** im Bereich **Design**.
3. Verwenden Sie den Connector, um zwischen den Aufgaben zu verbinden **Terraform sensible Variablen hinzufügen** und **Neue Terraform-Planaufgaben starten**. Klicken Sie Auf **Speichern**.
4. Klicken Sie Auf **Neuer Terraform-Plan** Starten. Klicken Sie im Bereich **Aufgabeneigenschaften** auf die Registerkarte **Allgemein**. Optional können Sie den Namen und die Beschreibung für diese Aufgabe ändern.



5. Klicken Sie im Bereich **Aufgabeneigenschaften** auf **Eingaben**.
6. Klicken Sie im Feld **Terraform Cloud Target** auf **Karte**.
7. Wählen Sie **statischer Wert** und klicken Sie auf **Terraform Cloud Target**. Wählen Sie das Terraform Cloud for Business-Konto aus, das im Abschnitt „Konfigurieren von Cisco Intersight Service für HashiCorp Terraform“ hinzugefügt wurde.
8. Klicken Sie Auf **Karte**.
9. Klicken Sie im Feld **Workspace-ID** auf **Karte**.
10. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Aufgabenausgabe**.
11. Klicken Sie auf **Aufgabenname** und dann auf **Terraform Workspace hinzufügen**.



12. Klicken Sie auf **Ausgabename**, **Workspace-ID** und dann auf **Karte**.
13. Klicken Sie im Feld **Grund für Startplan** auf **Karte**.
14. Wählen Sie **direkte Zuordnung** und klicken Sie dann auf **Workflow-Eingabe**.
15. Klicken Sie auf **Eingabename** und dann auf **Workflow-Eingabe erstellen**.
16. Führen Sie im Add Input Wizard die folgenden Schritte aus:
    a. Geben Sie einen Anzeigenamen und einen Referenznamen an (optional).
    b. Achten Sie darauf, **String** für den **Typ** auszuwählen.
    c. Klicken Sie auf **Standardwert festlegen und überschreiben**.
    d. Geben Sie einen Standardwert für **Grund für den Start von Plan** ein und klicken Sie auf **Hinzufügen**.



17. Klicken Sie Auf **Karte**.
18. Klicken Sie im Feld **Planoperation** auf **Karte**.
19. Wählen Sie **statischer Wert** und klicken Sie auf **Planvorgang**. Klicken Sie auf **Neuer Plan**.

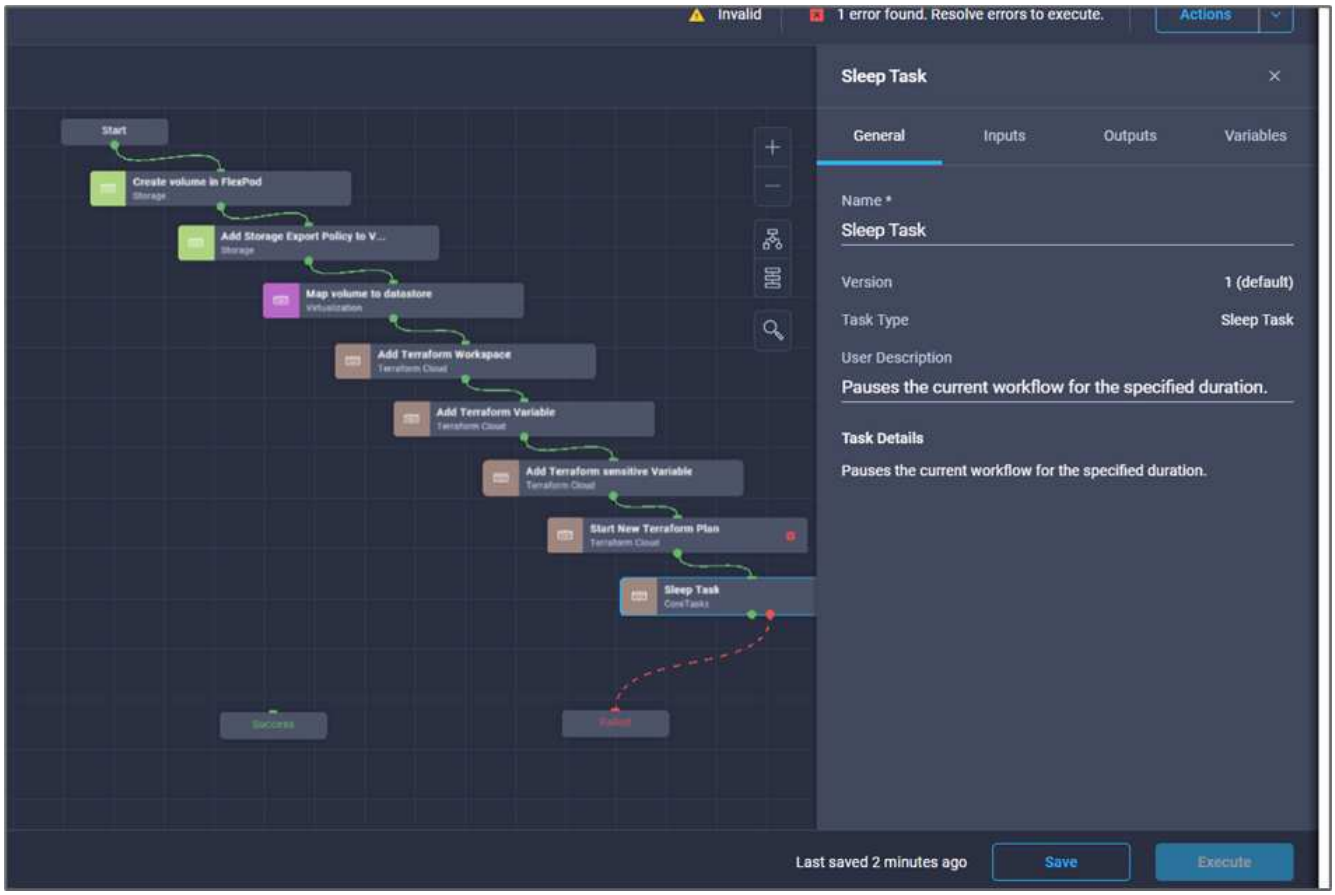
20. Klicken Sie Auf **Karte**.
21. Klicken Sie Auf **Speichern**.

Damit ist das Hinzufügen eines Terraform-Plans in Terraform Cloud for Business-Accounts abgeschlossen. Erstellen Sie dann für einige Sekunden eine Schlafaufgabe.

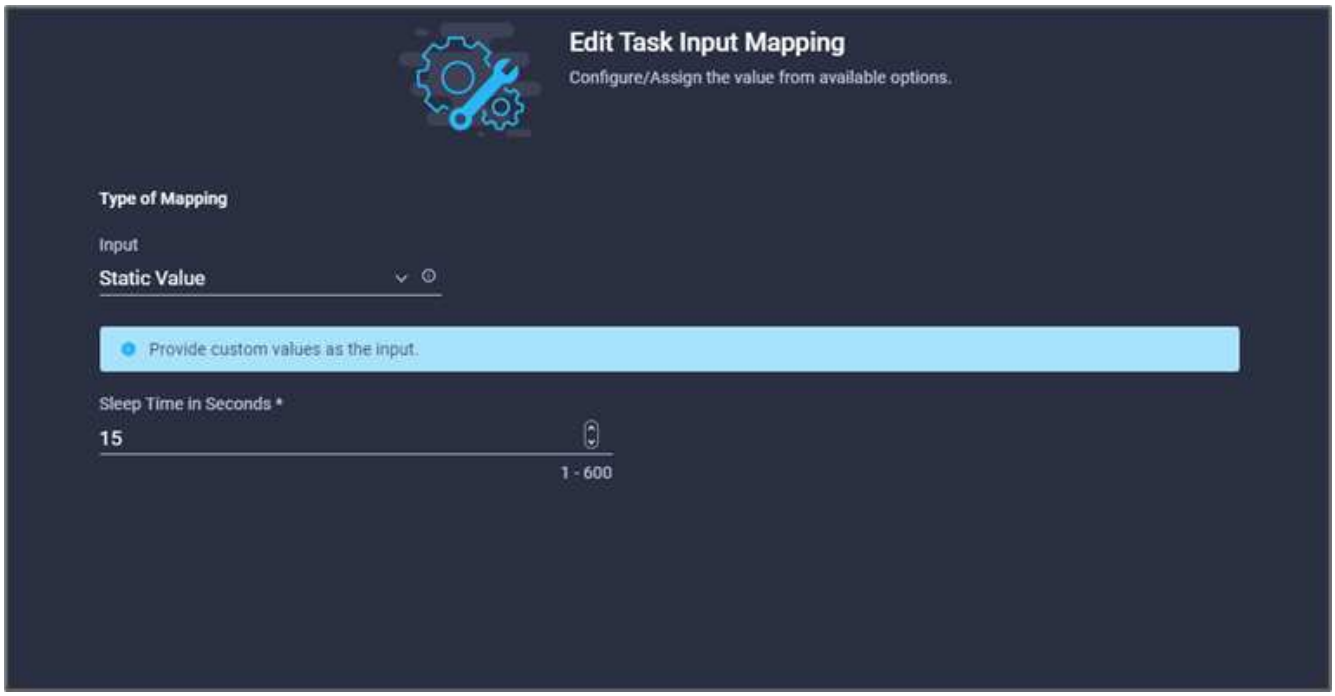
Prozedur 9: Sleep-Task für die Synchronisation

Terraform Apply erfordert RunID, die im Rahmen der Terraform Plan-Aufgabe generiert wird. Wenn Sie ein paar Sekunden zwischen dem Terraform-Plan und den Aktionen Terraform Apply warten, werden zeitliche Probleme vermieden.

1. Gehen Sie zur Registerkarte **Designer** und klicken Sie im Abschnitt **Tools** auf **Tasks**.
2. Ziehen Sie die Option **Core Tasks > Sleep Task** aus dem Abschnitt **Tools** im Bereich **Design**.
3. Verwenden Sie den Konnektor, um die Aufgaben zu verbinden **Neuer Terraform Plan** und **Sleep Task**. Klicken Sie Auf **Speichern**.



4. Klicken Sie Auf **Sleep Task**. Klicken Sie im Bereich **Aufgabeneigenschaften** auf die Registerkarte **Allgemein**. Optional können Sie den Namen und die Beschreibung für diese Aufgabe ändern. In diesem Beispiel lautet der Name der Aufgabe **Synchronize**.
5. Klicken Sie im Bereich **Aufgabeneigenschaften** auf **Eingaben**.
6. Klicken Sie im Feld **Schlafzeit in Sekunden** auf **Karte**.
7. Wählen Sie **statischer Wert** und geben Sie **15** in für die **Schlafzeit in Sekunden** ein.

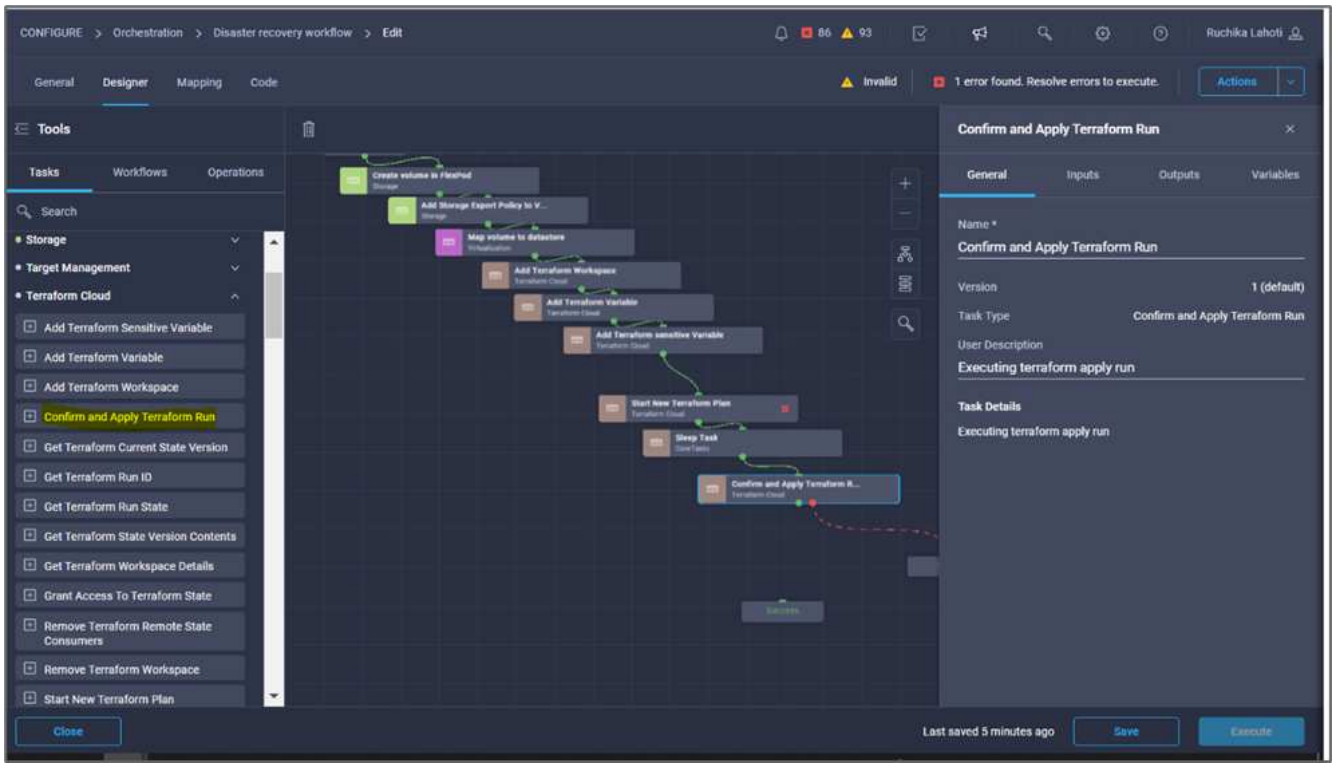


8. Klicken Sie Auf **Karte**.
9. Klicken Sie Auf **Speichern**.

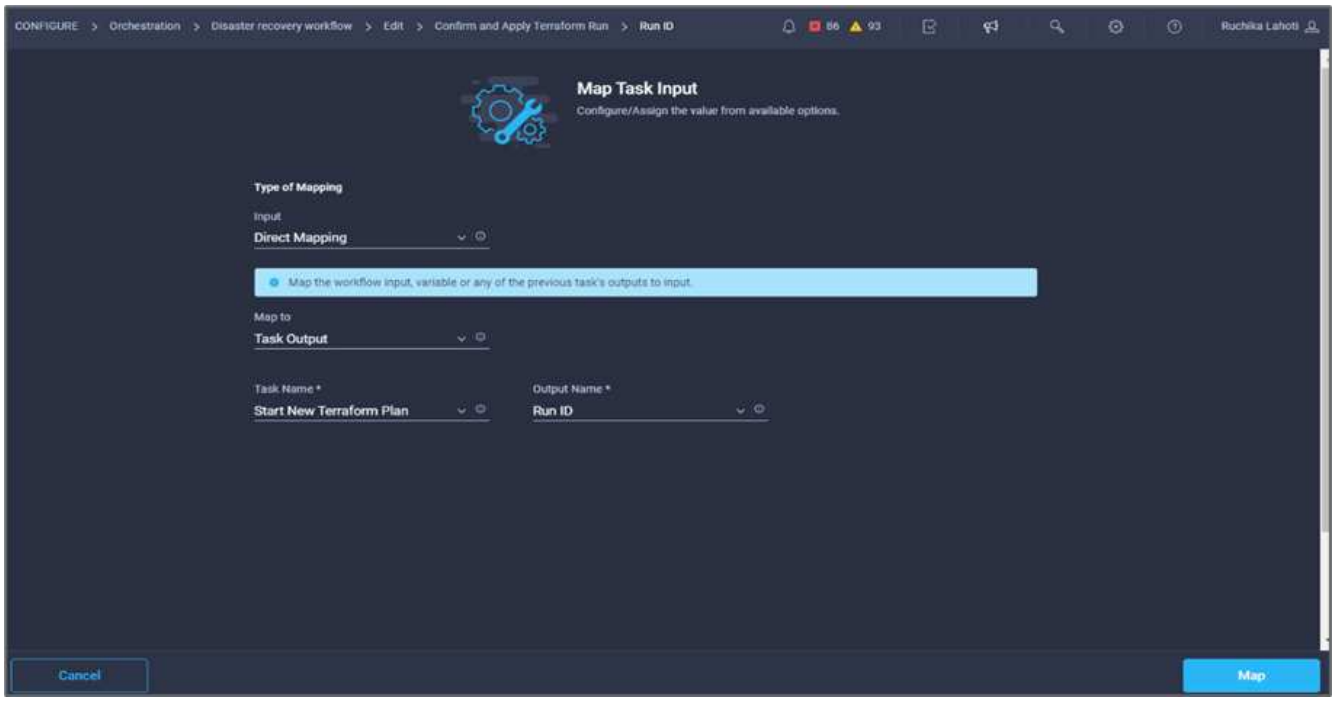
Damit ist die Schlafaufgabe abgeschlossen. Erstellen Sie als Nächstes die letzte Aufgabe dieses Workflows, indem Sie den Terraform-Lauf bestätigen und anwenden.

Prozedur 10: Terraform Run bestätigen und anwenden

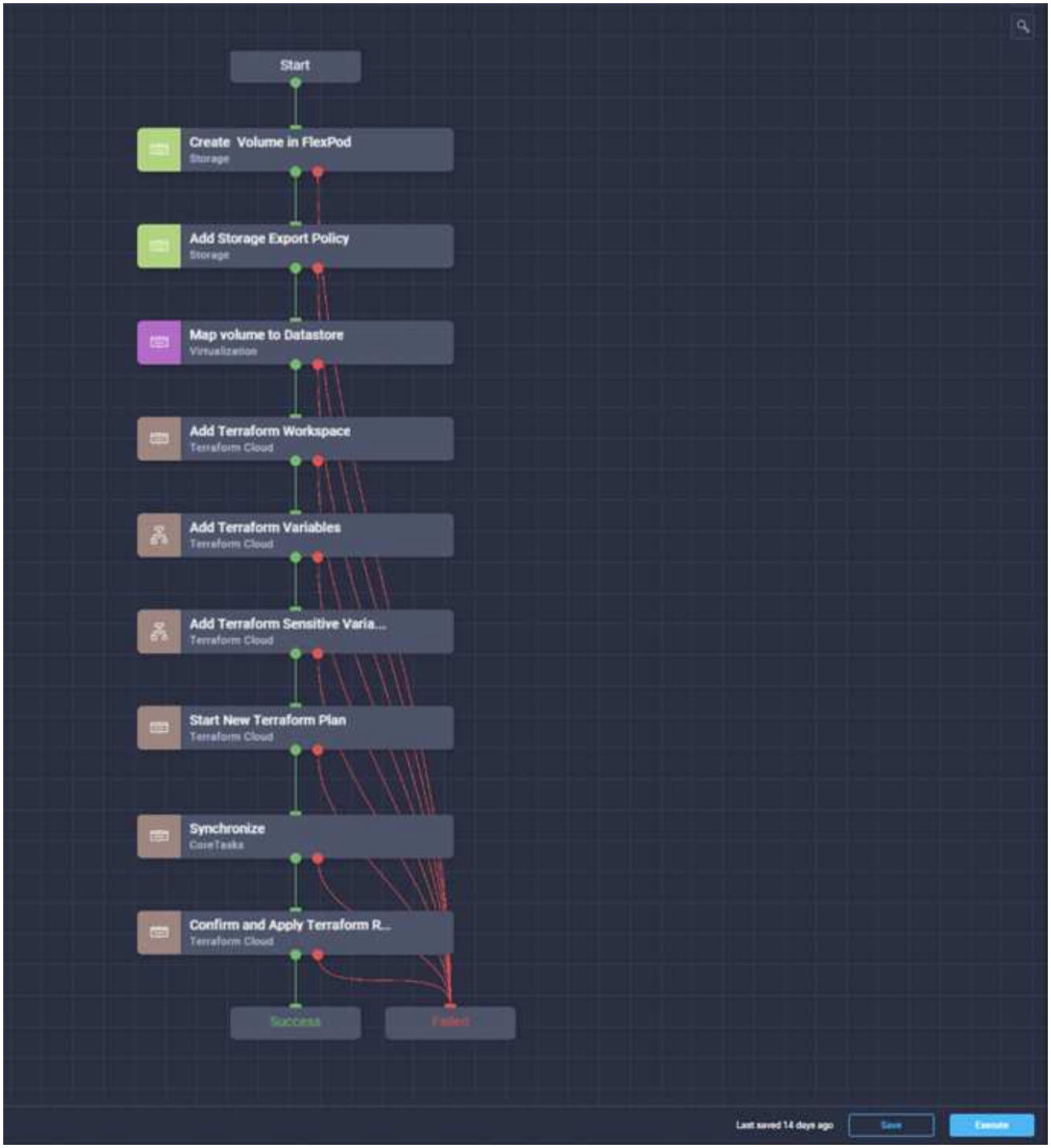
1. Gehen Sie zur Registerkarte **Designer** und klicken Sie im Abschnitt **Tools** auf **Tasks**.
2. Ziehen Sie die Aufgabe * Terraform Cloud > Bestätigen und anwenden Sie Terraform Run* aus dem Abschnitt **Tools** im Bereich **Design**.
3. Verwenden Sie den Anschluss, um die Aufgaben zu verbinden **Synchronisieren** und **Bestätigen und Anwenden von Terraform Run**. Klicken Sie Auf **Speichern**.
4. Klicken Sie auf **Bestätigen** und **Terraform Run anwenden**. Klicken Sie im Bereich **Aufgabeneigenschaften** auf die Registerkarte **Allgemein**. Optional können Sie den Namen und die Beschreibung für diese Aufgabe ändern.



5. Klicken Sie im Bereich **Aufgabeneigenschaften** auf **Eingaben**.
6. Klicken Sie im Feld **Terraform Cloud Target** auf **Karte**.
7. Wählen Sie **statischer Wert** und klicken Sie auf **Terraform Cloud Target**. Wählen Sie das Terraform Cloud for Business-Konto aus, das in hinzugefügt wurde "Konfigurieren Sie Cisco Intersight Service für HashiCorp Terraform".“
8. Klicken Sie Auf **Karte**.
9. Klicken Sie im Feld **Lauf-ID** auf **Karte**.
10. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Aufgabenausgabe**.
11. Klicken Sie auf **Aufgabenname** und klicken Sie auf **Neuer Terraform Plan**.
12. Klicken Sie auf **Ausgabename** und dann auf **Run ID**.



13. Klicken Sie Auf **Karte**.
14. Klicken Sie Auf **Speichern**.
15. Klicken Sie auf **Workflow automatisch ausrichten**, damit alle Aufgaben ausgerichtet sind. Klicken Sie Auf **Speichern**.



Hiermit ist die Aufgabe „Bestätigen und Anwenden von Terraform Run“ abgeschlossen. Verwenden Sie den Connector, um eine Verbindung zwischen der Aufgabe **Bestätigen und Anwenden Terraform Run** und den Aufgaben **Erfolg** und **failed** herzustellen.

Prozedur 11: Importieren eines von Cisco entwickelten Workflows

Mit Cisco Intersight Cloud Orchestrator können Sie Workflows von einem Cisco Intersight-Konto auf Ihr System exportieren und dann in ein anderes Konto importieren. Eine JSON-Datei wurde durch den Export des erstellten Workflows erstellt, der in Ihr Konto importiert werden kann.

Eine JSON-Datei für die Workflow-Komponente ist in verfügbar "GitHub Repository".

"Weiter: Terraform-Ausführung vom Controller."

Terraform-Ausführung vom Controller

"Früher: DR-Workflow."

Wir können den Terraform-Plan unter Verwendung eines Controllers ausführen. Wenn Sie Ihren Terraform-Plan bereits mithilfe eines ICO-Workflows ausgeführt haben, können Sie diesen Abschnitt überspringen.

Voraussetzungen

Die Einrichtung der Lösung beginnt mit einer Management-Workstation mit Zugang zum Internet und einer funktionierenden Installation von Terraform.

Ein Leitfaden zur Installation von Terraform finden Sie unter "Hier".

GitHub-Repo klonen

Der erste Schritt in diesem Prozess besteht darin, den GitHub Repo in einen neuen leeren Ordner auf der Management-Workstation zu klonen. Gehen Sie wie folgt vor, um das GitHub-Repository zu klonen:

1. Erstellen Sie auf der Management-Workstation einen neuen Ordner für das Projekt. Erstellen Sie einen neuen Ordner mit dem Namen `/root/snapmirror-cvo` Und den GitHub Repo hinein klonen.
2. Öffnen Sie eine Befehlszeilenschnittstelle oder Konsolenschnittstelle auf der Management-Workstation, und ändern Sie Verzeichnisse in den neuen Ordner, der gerade erstellt wurde.
3. Klonen Sie die GitHub-Sammlung mit dem folgenden Befehl:

```
Git clone https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO
```

1. Ändern Sie die Verzeichnisse in den neuen Ordner mit dem Namen `snapmirror-cvo`.

Terraform-Ausführung

- **Init.** Initialisieren Sie die (lokale) Terraform Umgebung. In der Regel nur einmal pro Sitzung ausgeführt.
- **Plan.** Vergleichen Sie den Terraform-Zustand mit dem AS-in-Zustand in der Cloud und erstellen und zeigen Sie einen Ausführungsplan an. Die Implementierung wird hierdurch nicht geändert (schreibgeschützt).
- **Gilt.** wendet den Plan aus der Planungsphase an. Das kann die Bereitstellung (Lese- und Schreibvorgänge) verändern.
- * Zerstöre.* Alle Ressourcen, die von dieser spezifischen Terraform Umgebung geregelt werden.

Weitere Informationen finden Sie unter "Hier".

"Weiter: Lösungsvalidierung."

Lösungsvalidierung

"Früher: Terraform-Ausführung vom Controller."

In diesem Abschnitt kommen wir zur Lösung mit einem Beispiel-Workflow für die Datenreplizierung zurück und können einige Messungen durchführen, um die Integrität der Datenreplizierung von der NetApp ONTAP Instanz, die in FlexPod auf NetApp Cloud Volumes ONTAP auf Google Cloud ausgeführt wird, zu überprüfen.

Wir haben in dieser Lösung den Cisco Intersight Workflow Orchestrator verwendet und werden diesen weiterhin für unseren Anwendungsfall verwenden.

Insbesondere die in dieser Lösung verwendeten Cisco Intersight-Workflows stellen nicht die gesamten Workflows dar, mit denen Cisco Intersight ausgestattet ist. Sie können individuelle Workflows auf Basis Ihrer spezifischen Anforderungen erstellen und über Cisco Intersight ausgelöst werden.

Für die Validierung eines erfolgreichen DR-Szenarios werden zunächst Daten von einem Volume in ONTAP verschoben, das Teil von FlexPod ist, und dann mithilfe von SnapMirror auf Cloud Volumes ONTAP verschoben. Anschließend können Sie versuchen, auf die Daten von der Google Cloud Computing-Instanz gefolgt von einer Datenintegritätsprüfung zuzugreifen.

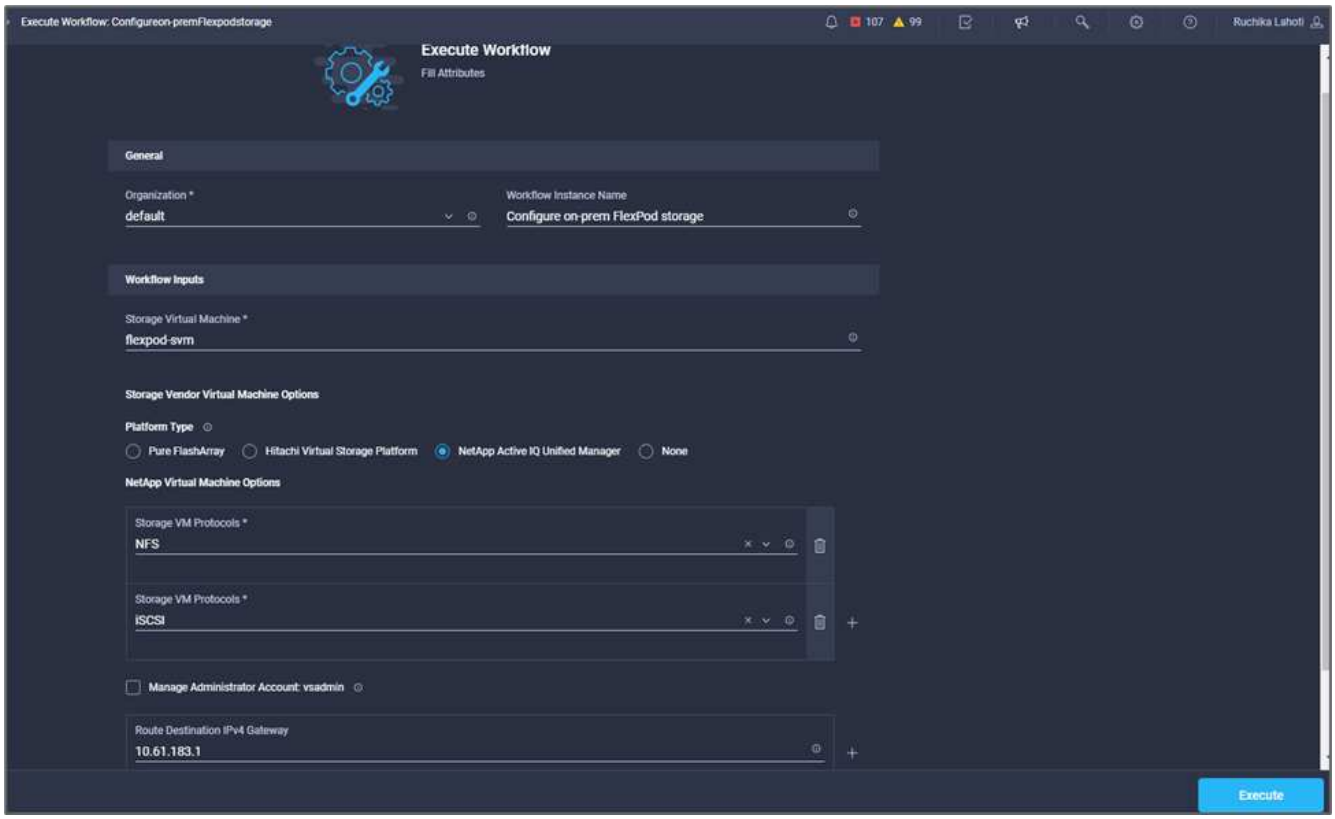
Die folgenden grundlegenden Schritte werden zur Überprüfung der Erfolgskriterien dieser Lösung herangezogen:

1. Generieren Sie eine SHA256-Prüfsumme auf dem Beispieldatensatz, der sich in einem ONTAP-Volume in FlexPod befindet.
2. Einrichten einer Volume-SnapMirror-Beziehung zwischen ONTAP in FlexPod und Cloud Volumes ONTAP
3. Replizieren des Beispieldatensatzes von FlexPod zu Cloud Volumes ONTAP
4. SnapMirror Beziehung aufheben und das Volume in Cloud Volumes ONTAP in die Produktion übertragen
5. Zuordnen des Cloud Volumes ONTAP Volumes mit dem Datensatz zu einer Computing-Instanz in Google Cloud
6. Erstellen Sie eine SHA256-Prüfsumme auf dem Beispieldatensatz in Cloud Volumes ONTAP.
7. Vergleichen Sie die Prüfsumme an Quelle und Ziel; vermutlich stimmen die Prüfsummen auf beiden Seiten überein.

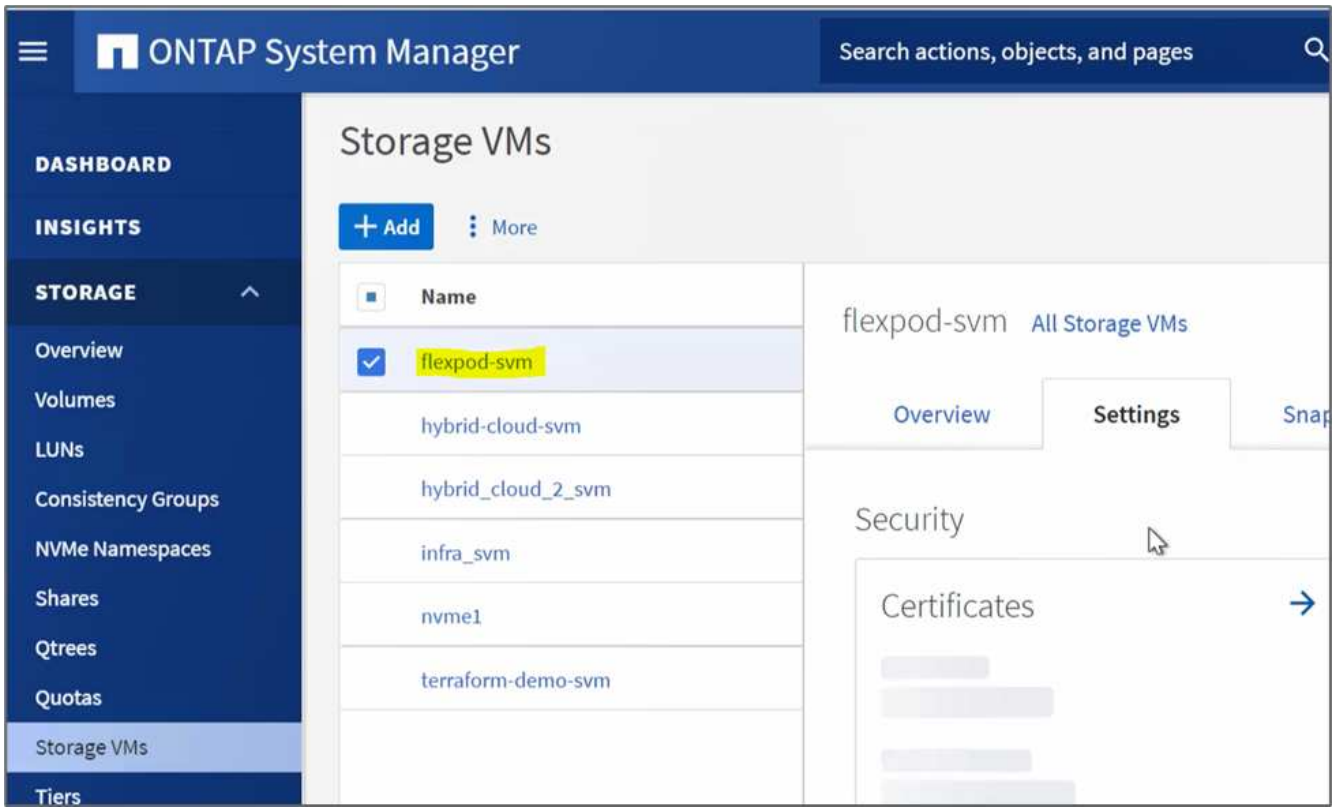
Um den lokalen Workflow auszuführen, gehen Sie wie folgt vor:

1. Erstellung eines Workflows in Intersight für On-Premises-FlexPod

2. Geben Sie die erforderlichen Eingaben an und führen Sie den Workflow aus.

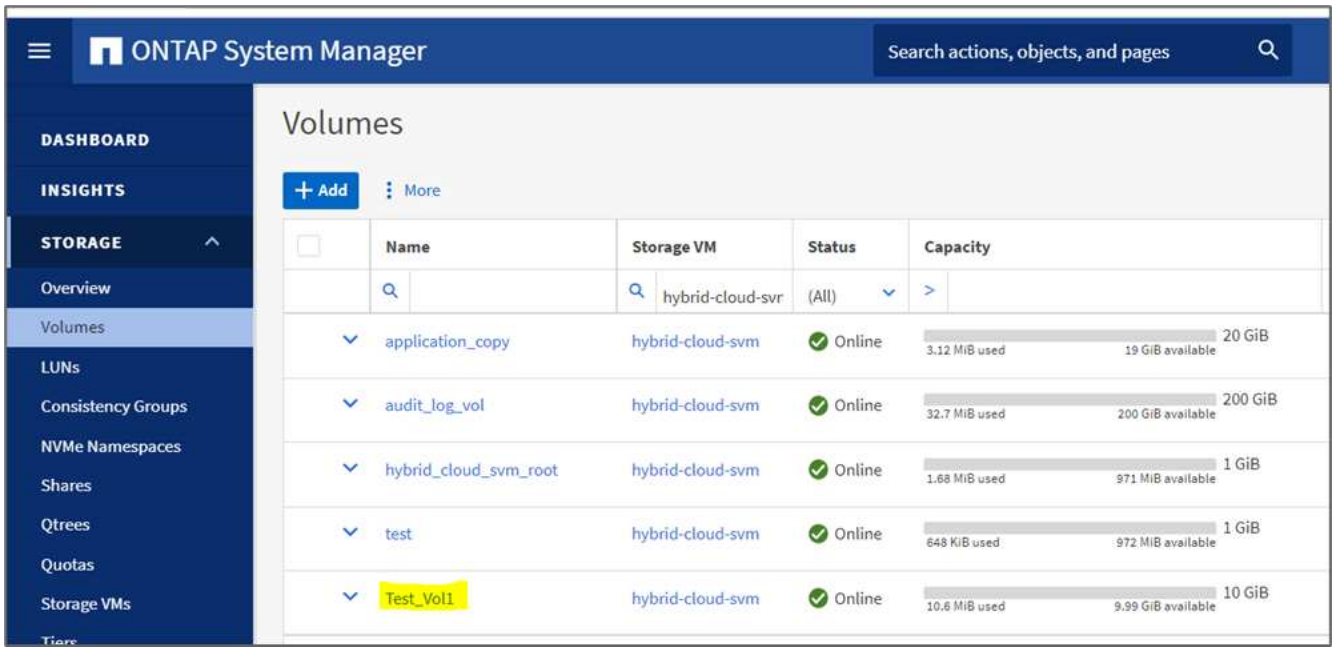


3. Überprüfen Sie die neu erstellte SVM im System Manager.



4. Erstellen und Ausführen eines weiteren Disaster-Recovery-Workflows, um ein Volume in FlexPod vor Ort zu erstellen und eine SnapMirror Beziehung zwischen diesem Volume in FlexPod und Cloud Volumes ONTAP herzustellen.

5. Überprüfen Sie das neu erstellte Volume im ONTAP System Manager.

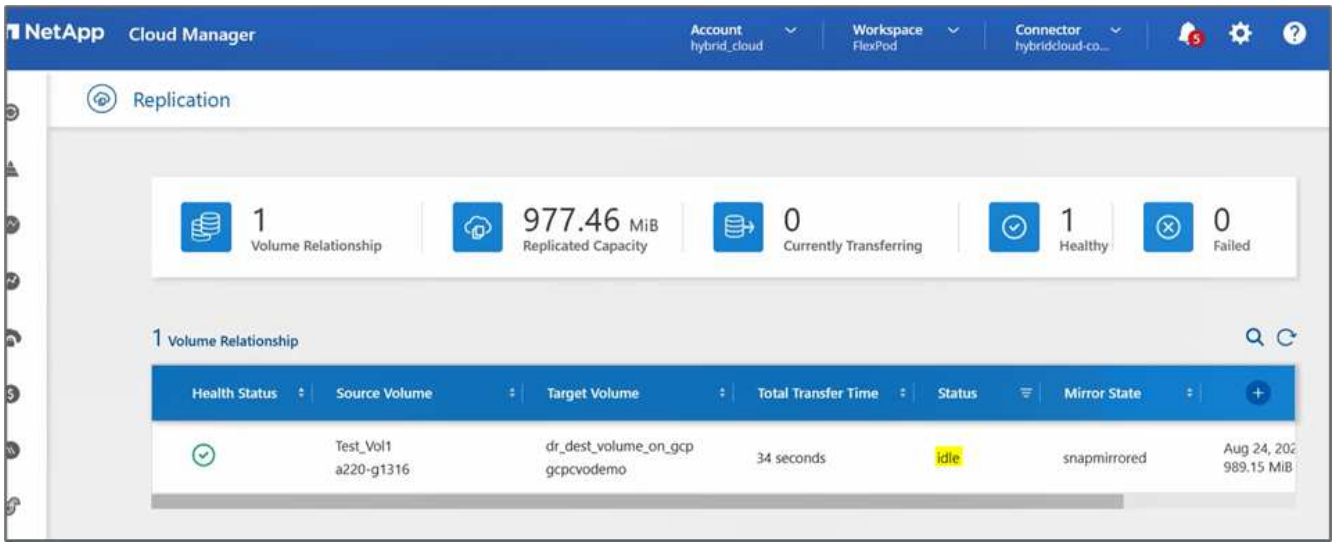


6. Mounten Sie dasselbe NFS-Volume auf eine lokale Virtual Machine, kopieren Sie dann den Beispieldatensatz und führen Sie die Prüfsumme durch.

```
root@hybridcloudbackup:/snapmirror_demo# mount -t nfs 172.22.4.157:/Test_Vol1 /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo# df -kh
Filesystem                Size  Used Avail Use% Mounted on
udev                      1.9G     0  1.9G   0% /dev
tmpfs                     394M  1.1M  393M   1% /run
/dev/sda2                  16G   11G  4.2G  72% /
tmpfs                     2.0G     0  2.0G   0% /dev/shm
tmpfs                     5.0M     0  5.0M   0% /run/lock
tmpfs                     2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1                 55M   55M     0 100% /snap/core18/1705
/dev/loop2                 69M   69M     0 100% /snap/lxd/14804
/dev/loop0                 28M   28M     0 100% /snap/snapd/7264
172.22.4.157:/Test_Vol1    10G  512K   10G   1% /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo#
```

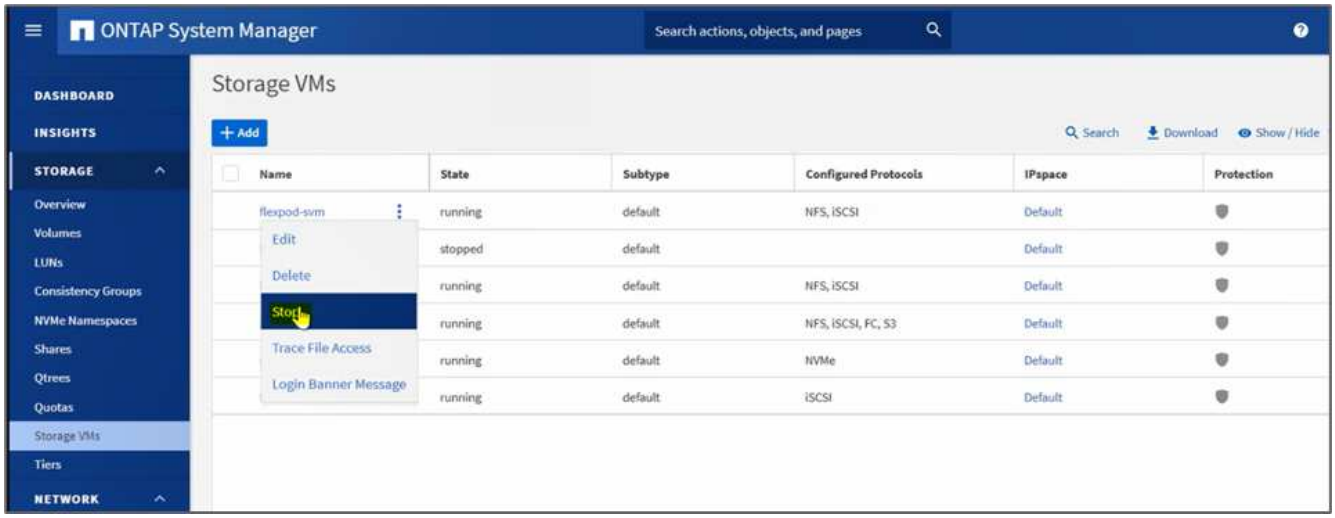
```
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo# sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo#
```

7. Überprüfen Sie den Replikationsstatus in Cloud Manager. Der Datentransfer kann je nach Datengröße einige Minuten dauern. Nach Abschluss des Vorgang kann der SnapMirror Status als **Idle** angezeigt werden.

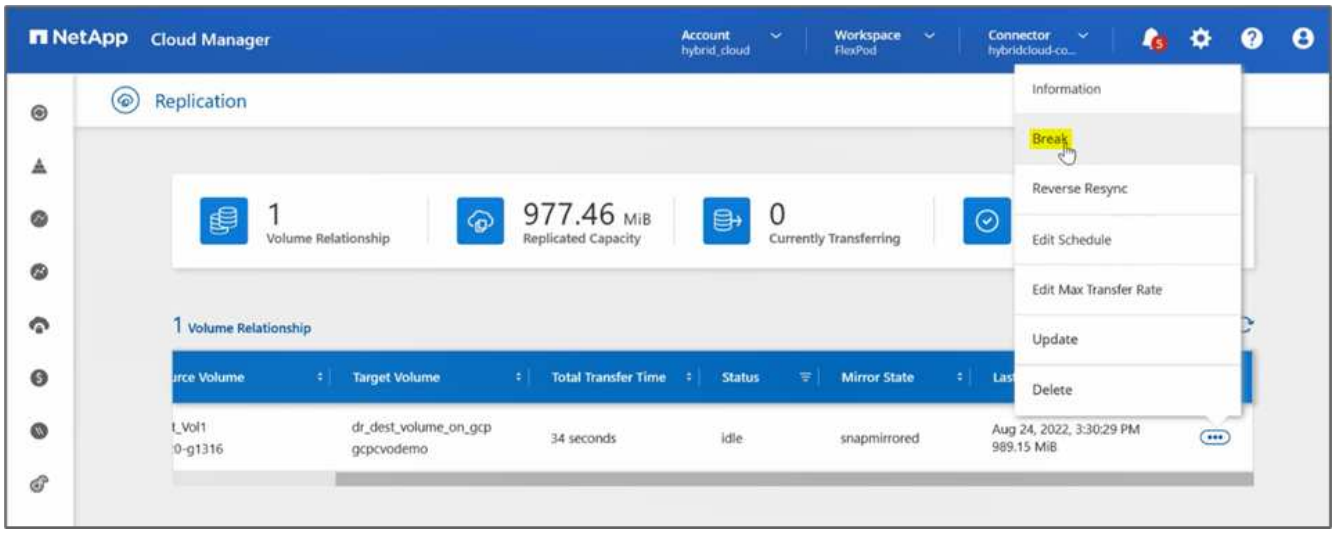


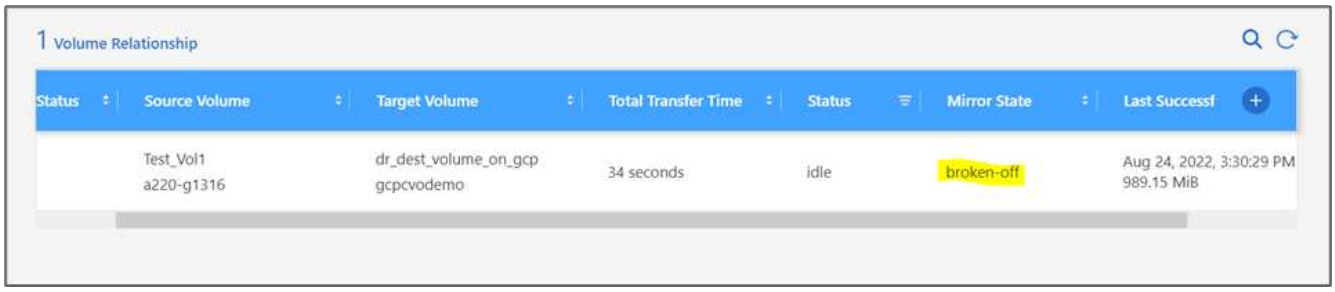
8. Wenn der Datentransfer abgeschlossen ist, simulieren Sie einen Notfall auf der Quellseite, indem Sie die SVM, die den hostet, anhalten `Test_vol1` Datenmenge:

   Nachdem die SVM angehalten wurde, führt der `Test_vol1` Das Volume ist im Cloud Manager nicht sichtbar.

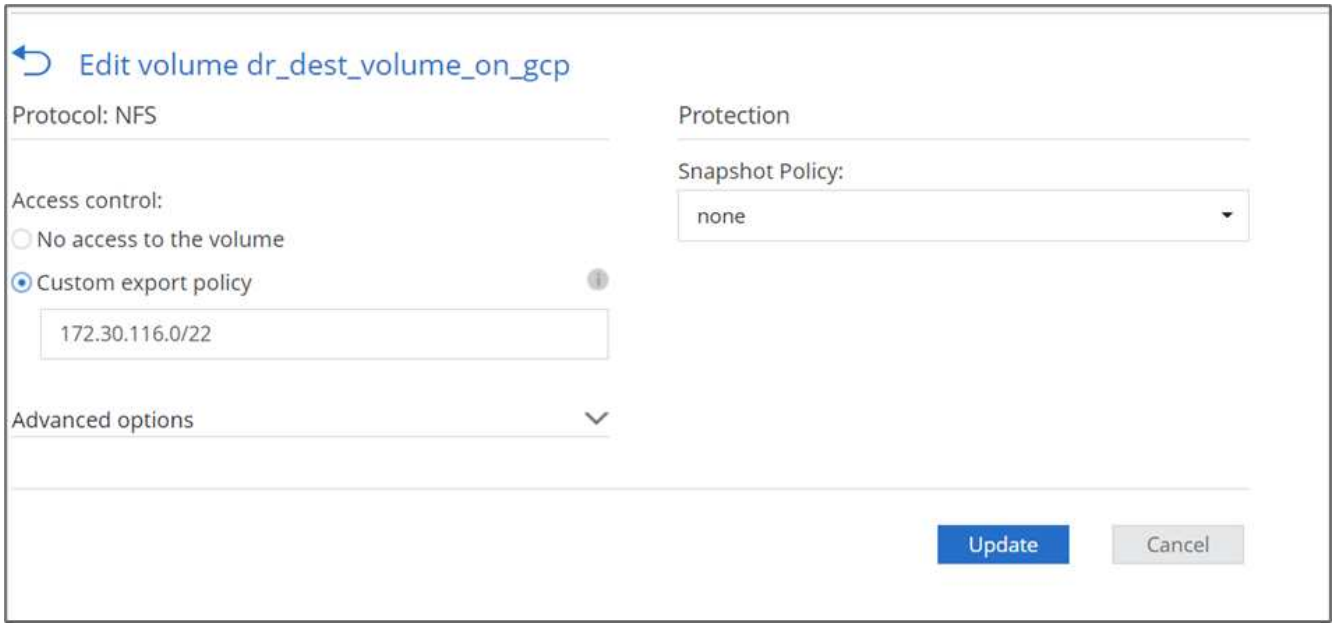


9. Replizierungsbeziehung wird zerbrechen und das Cloud Volumes ONTAP Ziel-Volume zur Produktion heraufstufen.

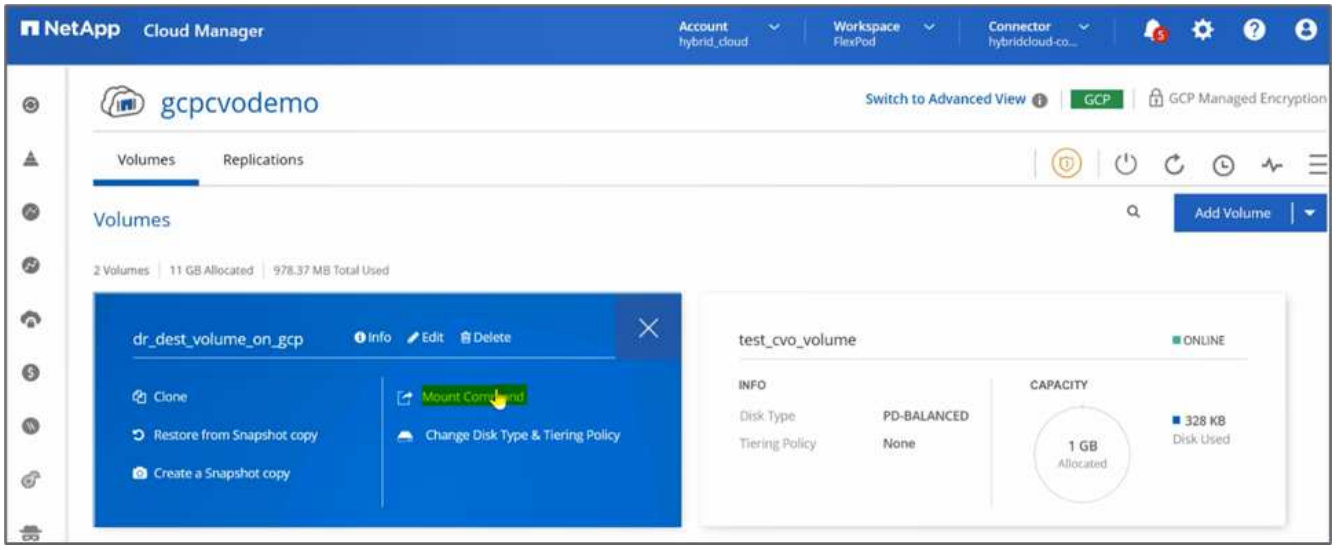




10. Bearbeiten Sie das Volume, und aktivieren Sie den Client-Zugriff, indem Sie es mit einer Exportrichtlinie verknüpfen.



11. Sie erhalten den Befehl Ready-to-Use Mount für das Volume.



12. Mounten Sie das Volume in eine Compute-Instanz, überprüfen Sie, ob die Daten im Ziel-Volume vorhanden sind, und generieren Sie die SHA256 Prüfsumme der `sample_dataset_2GB` Datei:

```
drwxr-xr-x 21 root   root            4096 Aug 24 10:20 ../
-rwxr-xr-x  1 nobody 4294967294 1015306240 Aug 24 09:59 test.zip*
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$ sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
```

13. Vergleichen Sie die Prüfsummenwerte sowohl an der Quelle (FlexPod) als auch am Ziel (Cloud Volumes ONTAP).
14. Die Prüfsummen werden mit Quelle und Ziel übereinstimmen.

Sie können bestätigen, dass die Datenreplizierung von der Quelle zum Ziel erfolgreich abgeschlossen wurde und die Datenintegrität gewahrt wurde. Diese Daten können jetzt von den Applikationen zur Bereitstellung von Clients sicher genutzt werden, während der Quellstandort die Wiederherstellung durchläuft.

"Weiter: Fazit."

Schlussfolgerung

"Zurück: Lösungsvalidierung."

In dieser Lösung wurden der NetApp Cloud Data Service, die Cloud Volumes ONTAP und die FlexPod Datacenter Infrastruktur verwendet, um eine DR-Lösung mit einer Public Cloud zu erstellen, die auf Cisco Intersight Cloud Orchestrator basiert. Die FlexPod Lösung wurde ständig weiterentwickelt, um Kunden die Modernisierung ihrer Applikationen und Geschäftsprozesse zu ermöglichen. Mit dieser Lösung können Sie einen BCDR-Plan mit der Public Cloud als Einsatzort für einen transienten oder Vollzeit-DR-Plan erstellen und gleichzeitig die Kosten der DR-Lösung gering halten.

Die Datenreplizierung zwischen On-Premises-FlexPod und NetApp Cloud Volumes ONTAP wird durch eine bewährte SnapMirror Technologie gehandhabt. Allerdings können Sie für Ihre Anforderungen an die Datenmobilität auch andere NetApp Übertragungs- und Synchronisierungstools wie Cloud Sync auswählen. Sicherheit der aktiven Daten durch integrierte Verschlüsselungstechnologien auf Basis von TLS/AES.

Unabhängig davon, ob Sie über einen temporären DR-Plan für eine Applikation oder einen VollzeitDR-Plan für ein Unternehmen verfügen – das in dieser Lösung verwendete Produktportfolio kann beide Anforderungen nach Maß erfüllen. Dank Cisco Intersight Workflow Orchestrator lässt sich dies auch in vordefinierten Workflows automatisieren, durch die nicht nur die Wiederherstellung von Prozessen überflüssig wird, sondern auch die Implementierung eines BCDR-Plans beschleunigt wird.

Diese Lösung ermöglicht das einfache und komfortable Management von FlexPod On-Premises und Datenreplizierung in einer Hybrid Cloud dank Automatisierung und Orchestrierung durch Cisco Intersight Cloud Orchestrator.

Wo Sie weitere Informationen finden

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

GitHub

- Alle Terraform-Konfigurationen werden verwendet

  "https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO"

- JSON-Dateien für den Import von Workflows

  "https://github.com/ucs-compute-solutions/FlexPod_DR_Workflows"

Cisco Intersight

- Cisco Intersight Help Center

  "https://intersight.com/help/saas/home"

- Dokumentation Von Cisco Intersight Cloud Orchestrator:

  "https://intersight.com/help/saas/features/orchestration/configure#intersight_cloud_orchestrator"

- Cisco Intersight Service for HashiCorp Terraform Documentation

"https://intersight.com/help/saas/features/terraform_cloud/admin"

- Cisco Intersight – Datenblatt

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html"

- Cisco Intersight Cloud Orchestrator – Datenblatt

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-cloud-orch-aag-cte-en.html"

- Cisco Intersight Service for HashiCorp Terraform – Datenblatt

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-terraf-ser-aag-cte-en.html"

FlexPod

- FlexPod Startseite

  "https://www.flexpod.com"

- Cisco Validated Design und Implementierungsleitfäden für FlexPod

  "FlexPod Datacenter with Cisco UCS 4.2(1) im UCS Managed Mode, VMware vSphere 7.0 U2 und NetApp ONTAP 9.9 Design Guide"

- FlexPod Datacenter mit Cisco UCS X-Serie

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"

Interoperabilität

- NetApp Interoperabilitäts-Matrix-Tool

  "http://support.netapp.com/matrix/"

- Cisco UCS Hardware and Software Interoperability Tool

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- VMware Compatibility Guide

  "http://www.vmware.com/resources/compatibility/search.php"

Referenzdokumente zu NetApp Cloud Volumes ONTAP

- NetApp Cloud Manager

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- Cloud Volumes ONTAP

https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-gcp.html

- Cloud Volumes ONTAP TCO-Rechner

  https://cloud.netapp.com/google-cloud-calculator

- Cloud Volumes ONTAP Sizer

  "https://cloud.netapp.com/cvo-sizer"

- Cloud Assessment Tool

  https://cloud.netapp.com/assessments

- NetApp Hybrid Cloud

  https://cloud.netapp.com/hybrid-cloud

- Dokumentation der Cloud Manager-API

  "https://docs.netapp.com/us-en/occm/reference_infrastructure_as_code.html"

Fehlerbehebung

"https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Cloud_Volumes_ONTAP_(CVO)"

Terraform

- Terraform Cloud

  "https://www.terraform.io/cloud"

- Terraform-Dokumentation

  "https://www.terraform.io/docs/"

- NetApp Cloud Manager Registry

  "https://registry.terraform.io/providers/NetApp/netapp-cloudmanager/lates"

GCP

- ONTAP Hochverfügbarkeit für GCP

  "https://cloud.netapp.com/blog/gcp-cvo-blg-what-makes-cloud-volumes-ontap-high-availability-for-gcp-tick"

- GCP pereprofür

  https://netapp.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=f3d0368b-7165-4d43-a76e-ae01011853d6

FlexPod Hybrid Cloud mit NetApp Astra und Cisco Intersight für Red hat OpenShift

TR-4936: FlexPod Hybrid Cloud mit NetApp Astra und Cisco Intersight for Red hat OpenShift

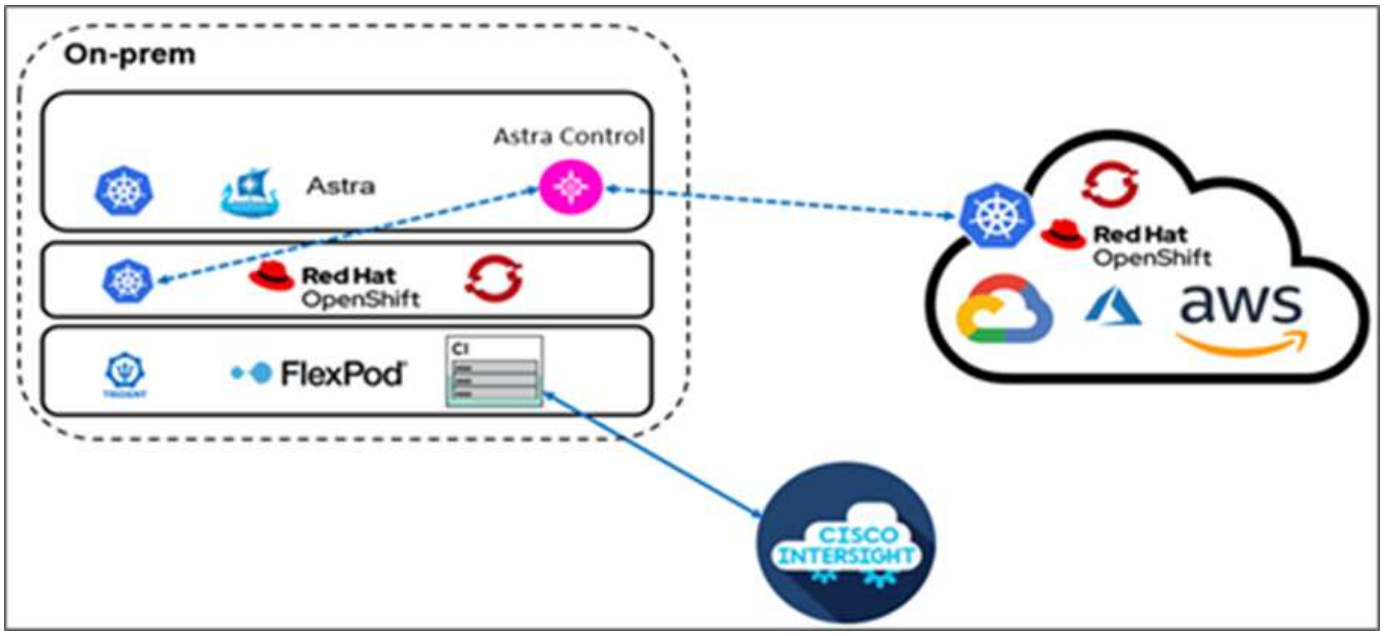
Abhinav Singh

Einführung

Da Container und Kubernetes sich zunehmend zur ersten Wahl für die Entwicklung, Implementierung, die Ausführung, das Management und die Skalierung von Container-Applikationen entwickeln, werden immer mehr Unternehmen auf ihren geschäftskritischen Applikationen ausgeführt. Geschäftskritische Applikationen sind stark von Staat abhängig. Eine zustandsorientierte Anwendung verfügt über zugeordnete Status-, Daten- und Konfigurationsinformationen und ist abhängig von früheren Datentransaktionen, um ihre Geschäftslogik auszuführen. Geschäftskritische Applikationen während der Ausführung auf Kubernetes bestehen weiterhin aus Anforderungen an Verfügbarkeit und Business Continuity wie herkömmliche Applikationen. Ein Service-Ausfall kann sich ernsthaft auf Umsatz-, Produktivitäts- und Reputationsverluste des Unternehmens auswirken. Daher ist es von großer Bedeutung, Kubernetes-Workloads schnell und einfach innerhalb von Clustern, On-Premises-Datacentern und Hybrid-Cloud-Umgebungen zu schützen, wiederherzustellen und zu verschieben. Unternehmen haben bereits erkannt, welche Vorteile sie haben, wenn sie ihr Unternehmen in ein Hybrid-Cloud-Modell verlagern und ihre Applikationen in einen Cloud-nativen Formfaktor modernisieren, steht ganz oben auf der Liste.

Dieser technische Bericht verbindet das NetApp Astra Control Center mit der Container-Plattform Red hat OpenShift auf einer konvergenten FlexPod-Infrastrukturlösung und kann mit Amazon Web Services (AWS) zu einem Hybrid-Cloud-Datacenter erweitert werden. Baut auf der Vertrautheit mit "FlexPod und Red hat OpenShift"In diesem Dokument geht es um das NetApp Astra Control Center: Von der Installation, Konfiguration, Workflows zur Applikationssicherung und der Applikationsmigration zwischen lokalen Ressourcen und der Cloud ausgehend. Außerdem werden die Vorteile applikationsgerechter Datenmanagementfunktionen (wie Backup und Recovery, Business Continuity) erläutert, die mit dem NetApp Astra Control Center für containerisierte Applikationen auf Red hat OpenShift ausgeführt werden.

Die folgende Abbildung zeigt den Lösungsüberblick.



Zielgruppe

Dieses Dokument richtet sich an Chief Technology Officers (CTOs), Applikationsentwickler, Cloud-Lösungsarchitekten, Site Reliability Engineers (SREs), DevOps Engineers, ITOps und Professional Services-Teams, die konzentriert sind auf die Entwicklung, das Hosting und das Management von Container-Applikationen.

NetApp Astra Control – wichtige Anwendungsfälle

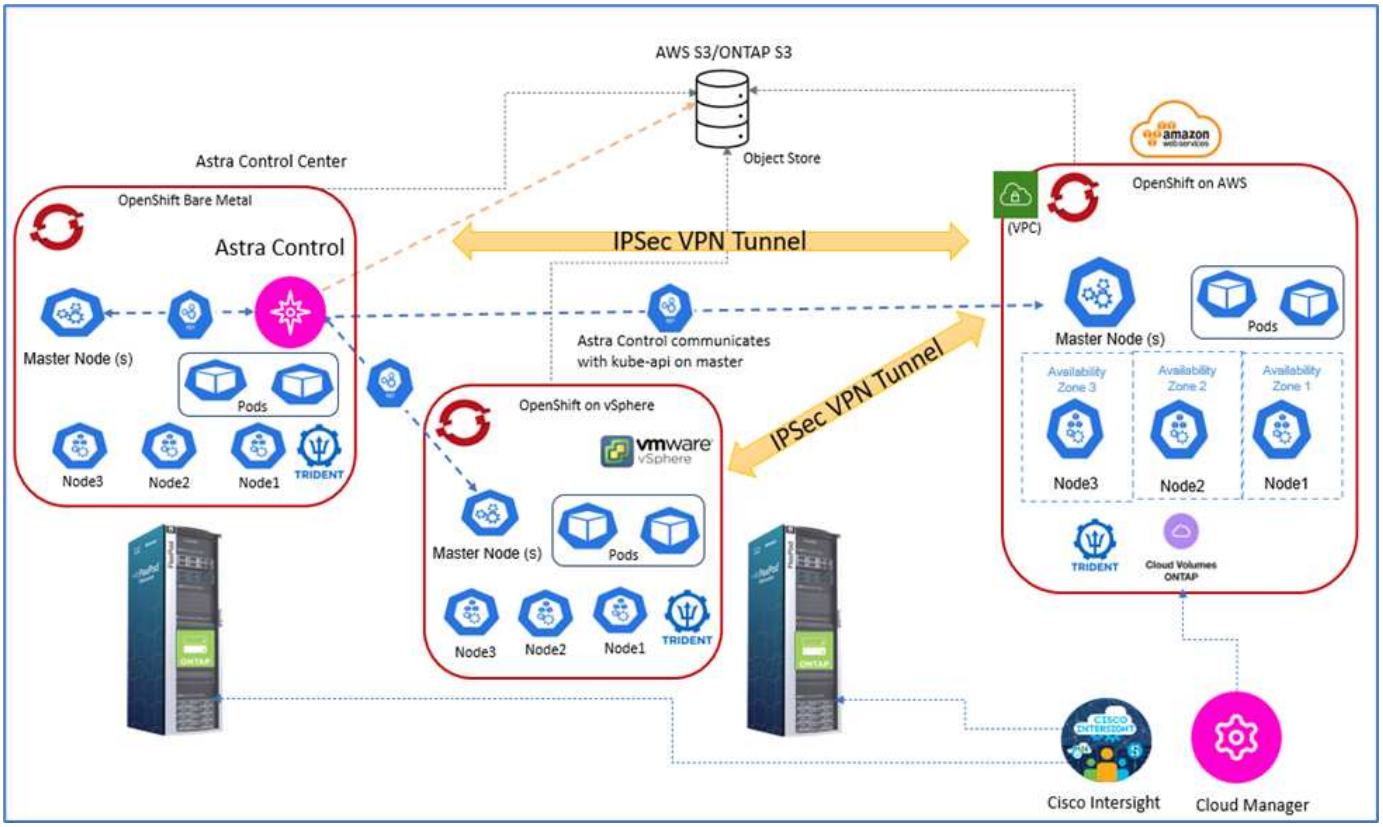
NetApp Astra Control möchte Kunden, die sich mit Cloud-nativen Microservices befassen, die Datensicherung vereinfachen:

- **Zeitpunktgenaue Applikationsperformationsdarstellung mit Snapshots.** mit Astra Control können Sie lückenlose Snapshots Ihrer Container-Applikationen erstellen, einschließlich der Konfigurationsdetails der auf Kubernetes ausgeführten Applikation und des zugehörigen persistenten Storage. Im Falle eines Vorfalls können Anwendungen in einem bekannten fehlerfreien Zustand in Button click wiederhergestellt werden.
- * Backup der Applikation in voller Kopie.* mit Astra Control können Sie ein komplettes Anwendungs-Backup auf einem vordefinierten Zeitplan erstellen, mit dem die Anwendung auf demselben K8s-Cluster oder auf einem anderen K8s-Cluster automatisiert bei Bedarf wiederhergestellt werden kann.
- **Applikationsportabilität und Migration mit Klonen.** mit Astra Control können Sie eine ganze Applikation mit den Daten von einem Kubernetes Cluster zum anderen oder innerhalb desselben K8s Clusters klonen. Diese Funktion unterstützt auch bei der Portierung oder Migration einer Applikation über K8s Cluster hinweg, unabhängig davon, wo sich die Cluster befinden (löschen Sie einfach die Quell-Applikationsinstanz nach dem Klonen).
- **Anpassung der Anwendungskonsistenz.** mit Astra Control können Sie die Festlegung von Stilllegungszuständen für Anwendungen unter Verwendung der Testsuiten steuern. Legen Sie die ‘pre’ und ‘post’ Execution Hooks auf die Snapshot-und Backup-Workflows, werden Ihre Anwendungen in Ihrer eigenen Weise stillgelegt, bevor ein Snapshot oder Backup erstellt wird.
- **Automatisieren Sie Disaster Recovery (DR) auf Applikationsebene.** mit Astra Control können Sie einen Business Continuity-Disaster-Recovery-Plan (BCDR) für Ihre Container-Applikationen konfigurieren. NetApp SnapMirror wird im Back-End eingesetzt und die vollständige Implementierung des DR-Workflows wird automatisiert.

Topologie der Lösung

In diesem Abschnitt wird die logische Topologie der Lösung beschrieben.

Die folgende Abbildung zeigt die Lösungstopologie, bestehend aus der On-Premises-FlexPod-Umgebung mit OpenShift-Container-Plattform-Clustern und einem selbst gemanagten OpenShift-Container-Plattform-Cluster auf AWS mit NetApp Cloud Volumes ONTAP, Cisco Intersight und der NetApp Cloud Manager SaaS-Plattform.



Das erste OpenShift-Container-Plattform-Cluster ist eine Bare-Metal-Installation auf FlexPod. Das zweite OpenShift-Container-Plattform-Cluster ist auf VMware vSphere unter FlexPod bereitgestellt. Das dritte OpenShift-Container-Plattform-Cluster wird als "Privater Cluster" In eine vorhandene virtuelle Private Cloud (VPC) von AWS als gemanagte Infrastruktur integrieren

In dieser Lösung ist FlexPod über ein Site-to-Site-VPN mit AWS verbunden. Kunden können die Implementierung der Direktverbindung zur Erweiterung auf eine Hybrid Cloud nutzen. Cisco Intersight wird für das Management der FlexPod Infrastrukturkomponenten eingesetzt.

Bei dieser Lösung managt Astra Control Center die Container-Applikation, die auf dem OpenShift Container Platform Cluster gehostet wird, das auf FlexPod und AWS ausgeführt wird. Astra Control Center ist auf der OpenShift Bare-Metal-Instanz auf FlexPod installiert. Astra Control kommuniziert mit der kube-API auf dem Master-Node und überwacht kontinuierlich den Kubernetes Cluster auf Änderungen. Alle neuen Anwendungen, die dem K8s-Cluster hinzugefügt wurden, werden automatisch erkannt und zur Verwaltung verfügbar gemacht.

Mithilfe des Astra Control Center können PIT-Darstellungen von containerisierten Applikationen als Snapshots erfasst werden. Applikations-Snapshots können entweder durch eine geplante Sicherungsrichtlinie oder bei Bedarf ausgelöst werden. Bei Anwendungen, die Astra unterstützt, ist der Snapshot Crash-konsistent. Ein Applikations-Snapshot besteht aus einem Snapshot der Applikationsdaten in den persistenten Volumes sowie den Applikationsmetadaten der verschiedenen Kubernetes-Ressourcen, die dieser Applikation zugeordnet sind.

Mithilfe von Astra Control kann ein Backup einer Applikation in voller Kopie erstellt werden. Dies ist mit einem vordefinierten Backup-Zeitplan oder nach Bedarf möglich. Zum Speichern des Backups der Applikationsdaten wird ein Objekt-Storage verwendet. NetApp ONTAP S3, NetApp StorageGRID und jede generische S3-Implementierung können als Objektspeicher verwendet werden.

"Als Nächstes: Lösungskomponenten."

Lösungskomponenten

"Zurück: Lösungsübersicht."

FlexPod

FlexPod ist eine definierte Gruppe von Hardware und Software und bildet eine integrierte Grundlage für virtualisierte und nicht virtualisierte Lösungen. FlexPod umfasst NetApp ONTAP Storage, Cisco Nexus Networking, Cisco MDS Storage Networking, Cisco Unified Computing System (Cisco UCS). Das Design ist flexibel genug, dass Netzwerk, Computing und Storage in ein Datacenter Rack passen oder nach dem Datacenter-Design des Kunden bereitgestellt werden können. Dank der Port-Dichte können die Netzwerkkomponenten mehrere Konfigurationen aufnehmen.

Astra Control

Astra Control bietet applikationsgerechte Datensicherungsservices für Cloud-native Applikationen, die sowohl in Public Clouds als auch in On-Premises-Umgebungen gehostet werden. Astra Control bietet Funktionen für Datensicherung, Disaster Recovery und Migration für Ihre auf Kubernetes laufende Container-Applikation.

Funktionen

Astra Control bietet entscheidende Funktionen für das Lifecycle Management von Kubernetes-Applikationsdaten:

- Automatisches Management von persistentem Storage
- Applikationskonsistente On-Demand Snapshots und Backups
- Automatisierte richtliniengesteuerte Snapshot- und Backup-Vorgänge
- Migrieren Sie Applikationen und zugehörige Daten in einer Hybrid-Cloud-Einrichtung von einem Kubernetes-Cluster zu einem anderen
- Eine Anwendung auf demselben K8s-Cluster oder einem anderen K8s-Cluster klonen
- Der Datensicherungsstatus der Applikation wird visualisiert
- Grafische Benutzeroberfläche und umfassende Rest-APIs zur Implementierung aller Sicherungs-Workflows über vorhandene interne Tools

Astra Control bietet Ihnen eine zentrale Konsole für die Visualisierung Ihrer Container-Applikationen und gewährt Ihnen einen Einblick in die damit verbundenen Ressourcen, die auf dem Kubernetes Cluster erstellt werden. Über ein Portal können alle Cluster, alle Applikationen in allen Clouds oder in allen Datacentern angezeigt werden. Mit den Astra Control APIs können Sie Ihre Datenmanagement-Workflows über alle Umgebungen hinweg (lokal oder in Public Clouds) implementieren.

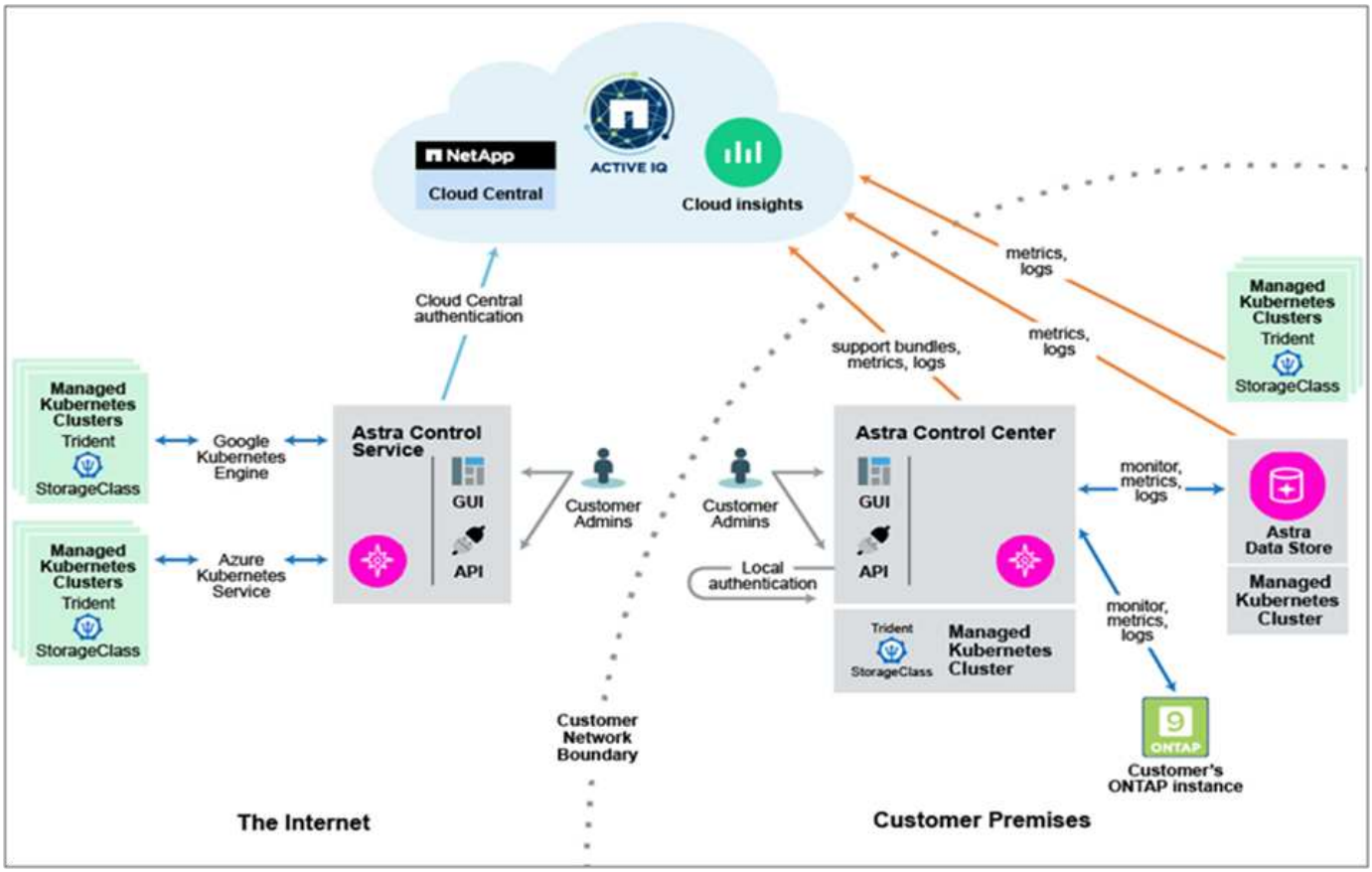
Astra Control Nutzungsmodelle

Astra Control ist in zwei Verbrauchsmodellen erhältlich:

- **Astra Control Service.** ein vollständig gemanagter Service, der von NetApp gehostet wird und applikationsgerechtes Datenmanagement für Kubernetes Cluster in der Google Kubernetes Engine (GKE), Azure Kubernetes Service (AKS) ermöglicht.
- **Astra Control Center.** selbst gemanagte Software für applikationsgerechtes Datenmanagement von Kubernetes Clustern, die in Ihrer lokalen und Hybrid-Cloud-Umgebung ausgeführt werden.

Dieser technische Bericht nutzt das Astra Control Center für das Management von Cloud-nativen Applikationen, die auf Kubernetes ausgeführt werden.

Das folgende Bild zeigt die Astra Control Architektur.



Astra Trident

Astra Trident ist ein vollständig unterstützter Open-Source-Orchestrator für Container und Kubernetes-Distributionen. Es wurde von Anfang an entwickelt, um Ihnen zu helfen, die Persistenzanforderungen Ihrer containerisierten Anwendungen mit Industriestandard-Schnittstellen wie die zu erfüllen "Container-Speicherschnittstelle (CSI)". Mit Astra Trident können Microservices und containerisierte Applikationen von Storage-Services der Enterprise-Klasse profitieren, die über das NetApp Portfolio an Storage-Systemen bereitgestellt werden.

Astra Trident wird auf Kubernetes-Clustern als Pods bereitgestellt und bietet dynamische Speicherorchestrierungsdienste für Ihre Kubernetes-Workloads. Es ermöglicht Ihren containerisierten Anwendungen, persistenten Speicher aus dem breiten Portfolio von NetApp schnell und einfach zu nutzen, darunter NetApp ONTAP (NetApp AFF, NetApp FAS, NetApp ONTAP Select, Cloud und Amazon FSx for NetApp ONTAP), die NetApp Element Software (NetApp SolidFire) sowie der Azure NetApp Files Service. In einer FlexPod Umgebung wird Astra Trident verwendet, um persistente Volumes für Container dynamisch bereitzustellen und zu verwalten, die von NetApp FlexVol Volumes und LUNs unterstützt werden, die auf einer ONTAP Speicherplattform wie NetApp AFF und FAS -Systemen und Cloud Volumes ONTAP gehostet werden. Trident spielt auch eine Schlüsselrolle bei der Implementierung von Anwendungsschutzsystemen, die von Astra Control bereitgestellt werden. Weitere Informationen zu Astra Trident finden Sie unter "Astra Trident-Dokumentation:"

Storage-Back-End

Zur Verwendung von Astra Trident benötigen Sie ein unterstütztes Storage-Backend. Ein Trident Back-End definiert die Beziehung zwischen Trident und einem Storage-System. Er erzählt Trident, wie man mit diesem Storage-System kommuniziert und wie Trident Volumes daraus bereitstellen sollte. Trident bietet automatisch

Storage-Pools aus Back-Ends an, die zusammen mit den von einer Storage-Klasse definierten Anforderungen übereinstimmen.

- ONTAP AFF und FAS Storage Back-End ONTAP ist eine Storage-Software- und Hardware-Plattform und bietet wichtige Storage-Services, Unterstützung für mehrere Storage-Zugriffsprotokolle und Storage-Managementfunktionen, wie beispielsweise NetApp Snapshot Kopien und Spiegelung.
- Cloud Volumes ONTAP Storage Back-End
- "Astra Data Store" Storage-Back-End

NetApp Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP ist ein softwaredefiniertes Storage-Angebot, das erweitertes Datenmanagement für Datei- und Block-Workloads bietet. 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:

- Nutzen Sie integrierte Datendeduplizierung, Datenkomprimierung, Thin Provisioning und Klonen und minimieren Sie so die Storage-Kosten.
- Zuverlässigkeit der Enterprise-Klasse und unterbrechungsfreien Betrieb bei Ausfällen in der Cloud-Umgebung sicherstellen.
- Cloud Volumes ONTAP nutzt SnapMirror, die branchenführende NetApp Replizierungstechnologie, um Daten vor Ort in der Cloud zu replizieren und so sekundäre Kopien für unterschiedliche Anwendungsfälle verfügbar zu machen.
- Die Integration von Cloud Volumes ONTAP in Cloud Backup Service bietet zudem Backup- und Restore-Funktionen zur Sicherung und zur Langzeitarchivierung Ihrer Cloud-Daten.
- Wechseln Sie nach Bedarf zwischen hochperformanten Storage Pools, ohne Applikationen offline zu schalten.
- Konsistenz von Snapshot-Kopien mit NetApp SnapCenter sicherstellen.
- Cloud Volumes ONTAP unterstützt die Datenverschlüsselung und bietet Schutz vor Viren und Ransomware.
- Integration in Cloud Data Sense unterstützt Sie dabei, den Datenkontext zu verstehen und sensible Daten zu identifizieren.

Cloud Central

Cloud Central bietet einen zentralen Standort zum Zugriff auf NetApp Cloud-Datenservices und -Management. Mit diesen Services können Sie kritische Applikationen in der Cloud ausführen, automatisierte DR-Standorte erstellen, Ihre Daten sichern und Daten effektiv zwischen diversen Clouds migrieren und kontrollieren. Weitere Informationen finden Sie unter "Cloud Central:"

Cloud Manager

Cloud Manager ist eine SaaS-basierte Managementplattform der Enterprise-Klasse, mit der IT-Experten und Cloud-Architekten ihre Hybrid-Multi-Cloud-Infrastruktur mithilfe der Cloud-Lösungen von NetApp 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 "Cloud Manager".

Stecker

Dieser Connector ermöglicht Cloud Manager das Management von Ressourcen und Prozessen in einer Public Cloud-Umgebung. Um viele Funktionen von Cloud Manager nutzen zu können, ist ein Connector erforderlich. Ein Connector kann in der Cloud oder im On-Premises-Netzwerk bereitgestellt werden.

Der Anschluss wird an folgenden Orten unterstützt:

- AWS
- Microsoft Azure
- Google Cloud
- Vor Ort

Weitere Informationen zu Connector finden Sie unter "Dieser Link."

NetApp Cloud Insights

Cloud Insights ist ein Cloud-Infrastruktur-Monitoring-Tool von NetApp und ermöglicht Ihnen, die Performance und Auslastung Ihrer Kubernetes Cluster zu überwachen und von Astra Control Center zu verwalten. Cloud Insights korreliert die Storage-Auslastung mit Workloads. Wenn Sie die Cloud Insights-Verbindung im Astra Control Center aktivieren, werden Telemetriedaten auf den UI-Seiten des Astra Control Center angezeigt.

NetApp Active IQ Unified Manager

Mit NetApp Active IQ Unified Manager können Sie Ihre ONTAP Storage-Cluster über eine neu konzipierte und intuitive Benutzeroberfläche überwachen, die Ihnen wertvolle Informationen aus Community-Wissen und KI-Analysen bietet. Er ermöglicht einen umfassenden Einblick in den Betrieb, die Performance und den proaktiven Einblick in die Storage-Umgebung und die darauf ausgeführten Virtual Machines (VMs). Wenn bei der Storage-Infrastruktur ein Problem auftritt, gibt Ihnen Unified Manager Informationen über das Problem und hilft Ihnen bei der Ermittlung der Ursache des Problems. Das VM Dashboard gibt Ihnen einen Überblick über die Performance-Statistiken für die VM, sodass Sie den gesamten I/O-Pfad vom VMware vSphere Host über das Netzwerk und schließlich den Storage erfassen können. Einige Ereignisse bieten auch Abhilfemaßnahmen, die zur Behebung des Problems ergriffen werden können. Sie können benutzerdefinierte Alarme für Ereignisse konfigurieren, sodass bei Problemen per E-Mail und SNMP-Traps benachrichtigt werden. Mit Active IQ Unified Manager lassen sich die Storage-Anforderungen Ihrer Benutzer planen, indem Kapazität und Nutzungstrends proaktiv vor Problemen vorhergesagt werden. Reaktive, kurzfristige Entscheidungen, die langfristig zu weiteren Problemen führen können, werden vermieden.

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 Veränderungen mit IT-Teams und bietet ein Betriebsmodell für Hybrid Clouds.

Cisco Intersight bietet folgende Vorteile:

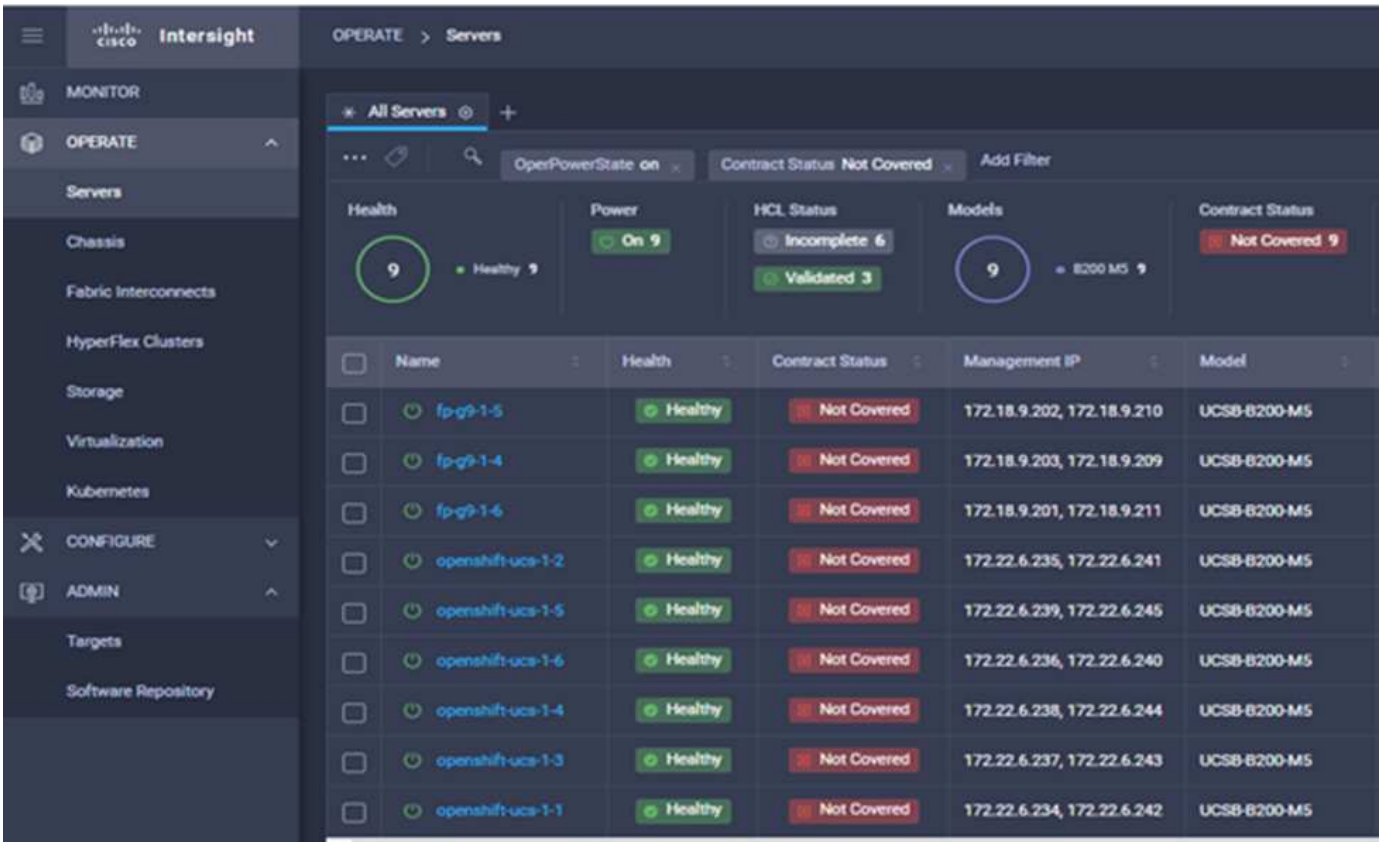
- **Schnellere Lieferung.** als Service aus der Cloud oder im Rechenzentrum des Kunden mit häufigen Updates und fortgesetzten Innovationen durch ein agiles, auf Software basierendes Entwicklungsmodell geliefert. So kann sich der Kunde ganz einfach darauf konzentrieren, die Bereitstellung für den Geschäftsbereich zu beschleunigen.
- **Vereinfachter Betrieb.** vereinfachter Betrieb durch den Einsatz eines einzigen sicheren SaaS-bereitgestellten Tools mit gemeinsamem Inventar, Authentifizierung und APIs für den gesamten Stack und alle Standorte. Silos in allen Teams sind damit nicht mehr erforderlich. Vom Management physischer

Server und Hypervisoren vor Ort, zu VMs, K8s, serverlos, Automatisierung, Die Optimierung und Kostenkontrolle über On-Premises- und Public Clouds hinweg.

- **Kontinuierliche Optimierung.** Optimieren Sie Ihre Umgebung mithilfe von Informationen, die von Cisco Intersight in allen Schichten bereitgestellt werden, sowie von Cisco TAC. Diese Informationen werden in empfohlene und automatisierbare Aktionen umgewandelt, mit denen Sie Echtzeit an jede Änderung anpassen können: Von der Verschiebung von Workloads und der Überwachung des Zustands von physischen Servern über die automatische Größenanpassung von K8s Clustern bis hin zu Kostenreduzierungsempfehlungen für die Public Clouds, mit denen Sie arbeiten.

Cisco Intersight ermöglicht zwei verschiedene Managementmodi: UCSM Managed Mode (UMM) und Intersight Managed Mode (IMM). Sie können das native UMM- oder IMM-System für die Fabric-Attached Cisco UCS-Systeme während der ersten Einrichtung der Fabric Interconnects auswählen. In dieser Lösung wird die native UMM verwendet.

Das folgende Bild zeigt das Cisco Intersight Dashboard.



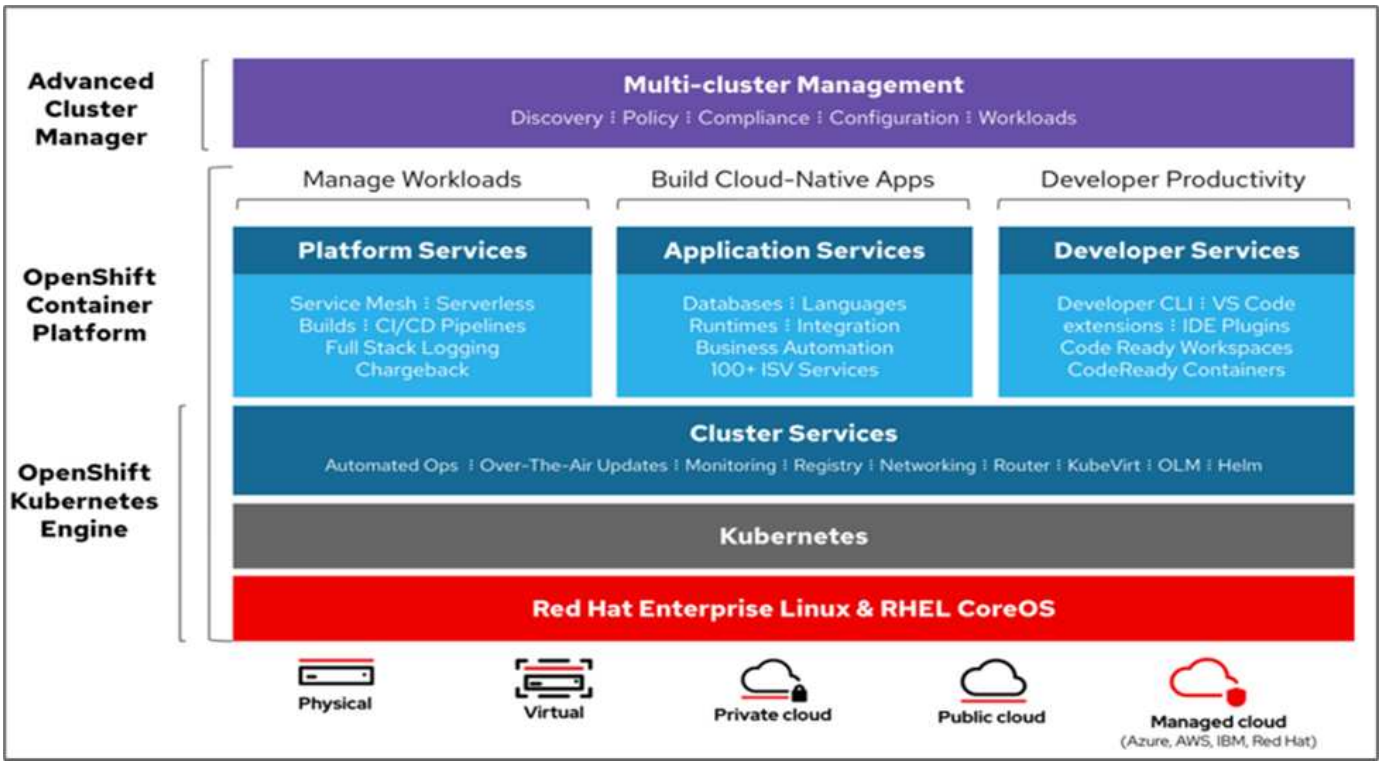
Red hat OpenShift Container Platform

Die Container-Applikationsplattform Red hat OpenShift ist eine Container-Applikationsplattform, die CRI-O und Kubernetes zusammenführt und eine API sowie eine Webschnittstelle zum Managen dieser Services bietet. CRI-O ist eine Implementierung der Kubernetes Container Runtime Interface (CRI), die die Verwendung von Offene Container Initiative (OCI)-kompatiblen Laufzeiten ermöglicht. Dabei handelt es sich um eine leichtgewichtige Alternative zur Verwendung von Docker als Laufzeit für Kubernetes.

Mit OpenShift Container Platform können Kunden Container erstellen und managen. Container sind eigenständige Prozesse, die innerhalb der eigenen Umgebung ausgeführt werden können – unabhängig vom Betriebssystem und der zugrunde liegenden Infrastruktur. OpenShift Container Platform unterstützt die Entwicklung, Bereitstellung und das Management Container-basierter Applikationen. Es stellt eine Self-Service-Plattform zum bedarfsgerechten Erstellen, Ändern und Implementieren von Applikationen bereit, die

eine schnellere Entwicklung und Verkürzung der Lebenszyklen ermöglicht. Die OpenShift Container Platform verfügt über eine auf Microservices basierende Architektur mit kleineren, entkoppelten Einheiten, die zusammen arbeiten. Es wird auf einem Kubernetes-Cluster ausgeführt, wobei Daten zu den in etc. Gespeicherten Objekten ein zuverlässiger Cluster-Schlüsselwertspeicher sind.

Das folgende Bild bietet einen Überblick über die Container-Plattform Red hat OpenShift.



Kubernetes-Infrastruktur

Innerhalb der OpenShift Container Platform managt Kubernetes containerisierte Applikationen über eine Reihe von CRI-O-Laufzeithosts hinweg und bietet Mechanismen für die Implementierung, Wartung und Applikationsskalierung. Die CRI-O-Servicepakete, instantiates und führen containerisierte Applikationen aus.

Ein Kubernetes-Cluster besteht aus einem oder mehreren Master und einem Satz Worker-Nodes. Das Lösungsdesign umfasst Hochverfügbarkeit (HA) in der Hardware und dem Software Stack. Ein Kubernetes Cluster wurde zur Ausführung im HA-Modus mit drei Master Nodes und mindestens zwei Worker Nodes entwickelt, um sicherzustellen, dass keine Single Point of Failure für das Cluster vorhanden sind.

Red hat Core OS

OpenShift Container Platform nutzt Red hat Enterprise Linux CoreOS (RHCOS), ein containerorientiertes Betriebssystem, das einige der besten Funktionen von CoreOS und Red hat Atomic Host-Betriebssystemen vereint. RHCOS ist speziell für die Ausführung von Container-Anwendungen über die OpenShift Container Platform konzipiert und arbeitet mit neuen Tools zusammen, um eine schnelle Installation, eine rasche Verwaltung und vereinfachte Upgrades zu ermöglichen.

RHCOS bietet die folgenden Funktionen:

- Zündung, die OpenShift Container Platform als erste Bootsystemkonfiguration zum ersten Einschalten und Konfigurieren von Maschinen verwendet.
- CRI-O, eine native Kubernetes-Laufzeitimplementierung für Container, die sich eng in das Betriebssystem

integriert und so eine effiziente und optimierte Kubernetes-Erfahrung ermöglicht. CRI-O bietet Funktionen zum Ausführen, Stoppen und Neustarten von Containern. Es ersetzt vollständig die Docker Container Engine, die in OpenShift Container Platform 3 eingesetzt wurde.

- Kubelet, der primäre Node-Agent für Kubernetes, ist für die Einführung und Überwachung von Containern verantwortlich.

VMware vSphere 7.0

VMware vSphere ist eine Virtualisierungsplattform, mit der sich umfangreiche Sammlung von Infrastrukturen (Ressourcen wie CPUs, Storage und Netzwerk) vollständig als nahtlose, vielseitige und dynamische Betriebsumgebung managen lassen. Im Gegensatz zu herkömmlichen Betriebssystemen, die eine einzelne Machine managen, sammelt VMware vSphere die Infrastruktur eines gesamten Datacenters und erstellt so ein einzelnes Kraftpaket, mit Ressourcen, die den jeweiligen Applikationen schnell und dynamisch zugewiesen werden können.

Weitere Informationen finden Sie unter "VMware vSphere".

VMware vSphere vCenter

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.

Hardware- und Software-Versionen

Diese Lösung kann auf jede FlexPod Umgebung erweitert werden, in der unterstützte Versionen von Software, Firmware und Hardware ausgeführt werden, wie in definiert "NetApp Interoperabilitäts-Matrix-Tool" Und "Cisco UCS Hardware Compatibility List:" Das OpenShift-Cluster ist sowohl auf FlexPod Bare Metal-Weise als auch auf VMware vSphere installiert.

Für das Management mehrerer OpenShift-Cluster ist nur eine einzige Instanz von Astra Control Center erforderlich, während Trident CSI auf jedem OpenShift-Cluster installiert ist. Astra Control Center kann auf jedem dieser OpenShift-Cluster installiert werden. In dieser Lösung ist Astra Control Center auf dem Bare-Metal-Cluster OpenShift installiert.

In der folgenden Tabelle sind die Versionen der Hardware und Software von FlexPod für OpenShift aufgeführt.

Komponente	Produkt	Version
Computing	Cisco UCS Fabric Interconnects 6454	4.1(3c)
	Cisco UCS B200 M5 Server	4.1(3c)
Netzwerk	Cisco Nexus 9336C-FX2 NX-OS	9.3 (8)
Storage	NetApp AFF A700	9.11.1
	NetApp Astra Control Center	22.04.0
	NetApp Astra Trident CSI-Plug-in	22.04.0
	NetApp Active IQ Unified Manager	9.11

Komponente	Produkt	Version
Software	VMware ESXi Nenic Ethernet-Treiber	1.0.35.0
	VSphere ESXi	7.0 (U2)
	VMware vCenter Appliance	7.0 U2b
	Cisco Intersight Assist Virtual Appliance	1.0.9-342
	OpenShift Container Platform	4.9
	OpenShift Container Platform Master Node	RHCOS 4.9
	OpenShift Container Platform Worker-Node	RHCOS 4.9

In der folgenden Tabelle sind die Softwareversionen für OpenShift auf AWS aufgeführt.

Komponente	Produkt	Version
Computing	Master Instance Typ: m5.xlarge	k. A.
	Worker-Instanz Typ: m5.large	k. A.
Netzwerk	Virtual Private Cloud Transit Gateway	k. A.
Storage	NetApp Cloud Volumes ONTAP	9.11.1
	NetApp Astra Trident CSI-Plug-in	22.04.0
Software	OpenShift Container Platform	4.9
	OpenShift Container Platform Master Node	RHCOS 4.9
	OpenShift Container Platform Worker-Node	RHCOS 4.9

"Weiter: FlexPod für OpenShift Container Platform 4 Bare-Metal-Installation."

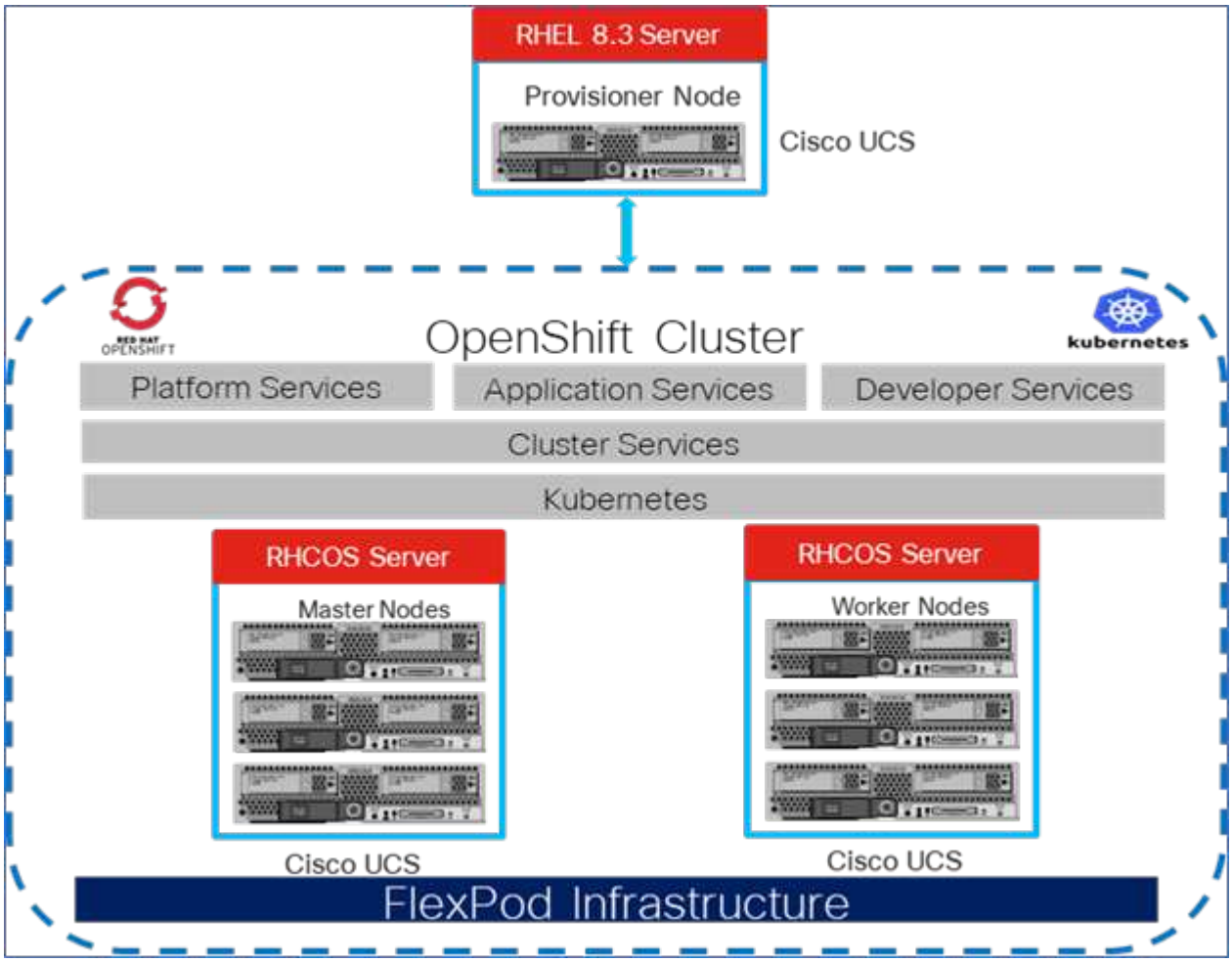
Installation und Konfiguration

FlexPod für OpenShift Container Platform 4 Bare-Metal-Installation

"Früher: Lösungskomponenten."

Weitere Informationen zum Bare-Metal-Design, den Implementierungsdetails und der Installation und Konfiguration von NetApp Astra Trident finden Sie unter FlexPod for OpenShift Container Platform 4 "FlexPod mit OpenShift Cisco Validated Design and Deployment Guide (CVD)". Dieses CVD deckt die Implementierung der FlexPod- und OpenShift-Container-Plattform mit Ansible ab. Das CVD bietet auch detaillierte Informationen zum Vorbereiten von Worker-Nodes, zur Astra Trident-Installation, zum Storage-Backend und zu Storage-Klassenkonfigurationen. Diese sind die wenigen

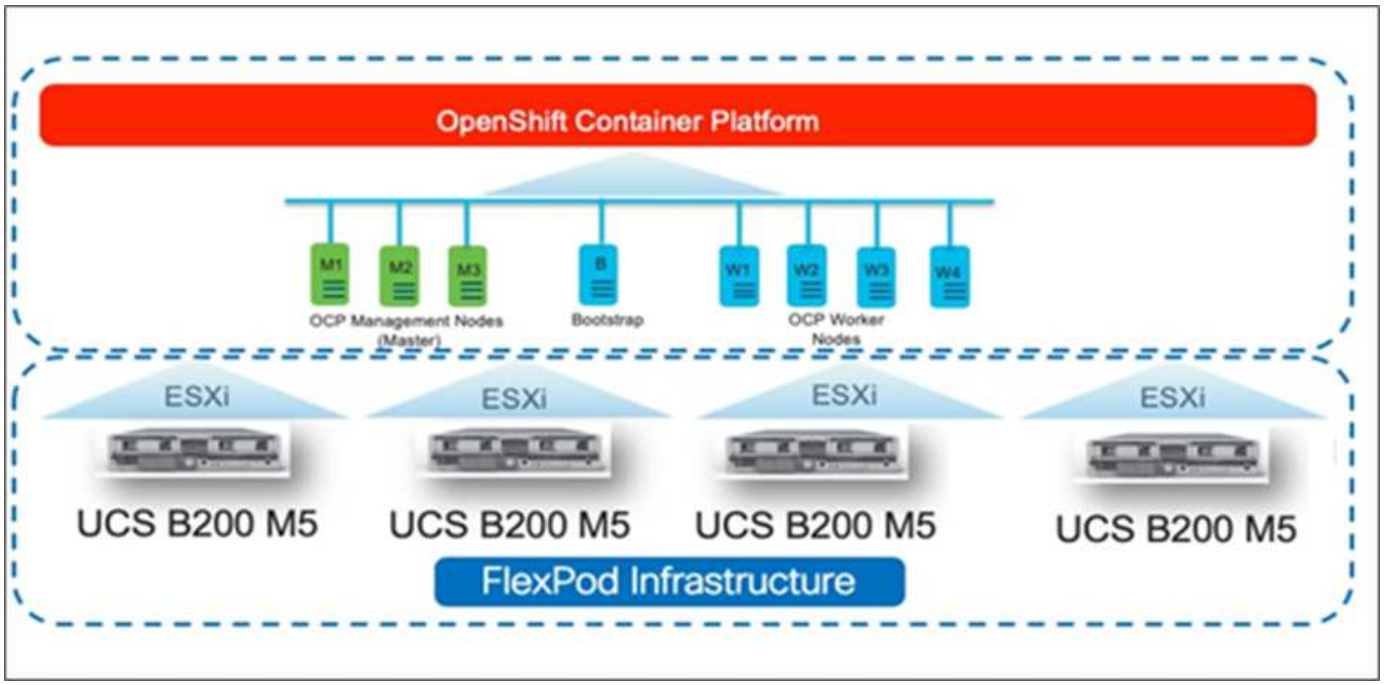
Die folgende Abbildung zeigt OpenShift Container Platform 4 Bare Metal auf FlexPod.



FlexPod for OpenShift Container Platform 4 auf VMware-Installation

Weitere Informationen zur Bereitstellung der Red hat OpenShift-Container-Plattform 4 auf FlexPod mit VMware vSphere finden Sie unter "FlexPod-Datacenter für OpenShift-Container-Plattform 4".

Die folgende Abbildung zeigt FlexPod für OpenShift Container Platform 4 auf vSphere.

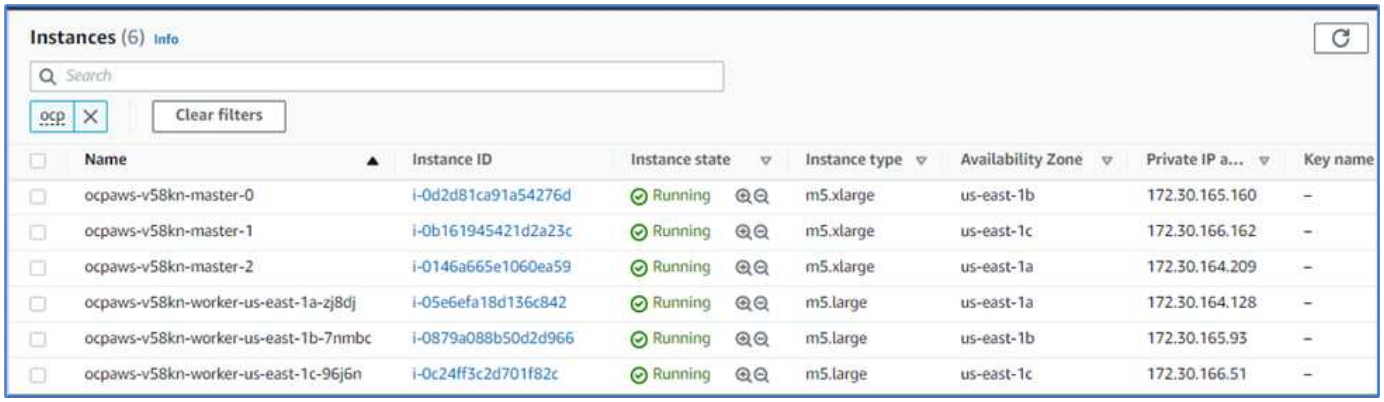


"Nächste Frage: Red hat OpenShift auf AWS"

Red hat OpenShift auf AWS

"Früher: FlexPod für OpenShift Container Platform 4 Bare-Metal-Installation."

Ein separater selbst verwalteter OpenShift-Container-Plattform-4-Cluster wird auf AWS als DR-Standort bereitgestellt. Die Master- und Worker-Nodes erstrecken sich auf drei Verfügbarkeitszonen, um Hochverfügbarkeit zu gewährleisten.



```
[ec2-user@ip-172-30-164-92 ~]$ oc get nodes
NAME                                STATUS   ROLES    AGE   VERSION
ip-172-30-164-128.ec2.internal   Ready    worker   29m   v1.22.8+f34b40c
ip-172-30-164-209.ec2.internal   Ready    master   36m   v1.22.8+f34b40c
ip-172-30-165-160.ec2.internal   Ready    master   33m   v1.22.8+f34b40c
ip-172-30-165-93.ec2.internal    Ready    worker   30m   v1.22.8+f34b40c
ip-172-30-166-162.ec2.internal   Ready    master   36m   v1.22.8+f34b40c
ip-172-30-166-51.ec2.internal    Ready    worker   28m   v1.22.8+f34b40c
```

OpenShift ist als bereitgestellter Einsatz "Privater Cluster" Zu einer vorhandenen VPC auf AWS. Ein privates Cluster der OpenShift Container Platform weist keine externen Endpunkte auf und ist nur über ein internes Netzwerk zugänglich und nicht für das Internet sichtbar. Mit NetApp Cloud Manager wird eine NetApp Single-Node Cloud Volumes ONTAP implementiert, die ein Storage-Back-End für Astra Trident bietet.

Weitere Informationen zur Installation von OpenShift auf AWS finden Sie unter "OpenShift-Dokumentation".

"Weiter: NetApp Cloud Volumes ONTAP."

NetApp Cloud Volumes ONTAP

"Früher: Red hat OpenShift auf AWS."

Die NetApp Cloud Volumes ONTAP Instanz ist auf AWS implementiert und dient als Backend-Storage für Astra Trident. Bevor Sie eine Cloud Volumes ONTAP Arbeitsumgebung hinzufügen, muss ein Connector bereitgestellt werden. Der Cloud-Manager fordert Sie auf, wenn Sie versuchen, die erste Cloud Volumes ONTAP-Arbeitsumgebung ohne entsprechenden Connector zu erstellen. Informationen zur Implementierung eines Connectors in AWS finden Sie unter "Einen Konnektor erstellen".

Informationen zur Implementierung von Cloud Volumes ONTAP auf AWS finden Sie unter "Schnellstart für AWS".

Nach der Implementierung von Cloud Volumes ONTAP können Sie Astra Trident installieren und das Storage-Back-End und die Snapshot-Klasse auf dem OpenShift Container Platform Cluster konfigurieren.

"Als Nächstes: Astra Control Center-Installation auf OpenShift Container Platform."

Astra Control Center-Installation auf OpenShift Container Platform

"Früher NetApp Cloud Volumes ONTAP."

Sie können Astra Control Center entweder auf OpenShift-Cluster auf FlexPod oder auf AWS mit einem Cloud Volumes ONTAP-Storage-Backend installieren. In dieser Lösung wird Astra Control Center auf dem Bare-Metal-Cluster OpenShift implementiert.

Astra Control Center kann mit dem beschriebenen Standardprozess installiert werden "Hier" Oder über den Red hat OpenShift OperatorHub. Astra Control Operator ist ein Red hat zertifizierter Operator. In dieser Lösung wird Astra Control Center mit dem Red hat OperatorHub installiert.

Umgebungsanforderungen

- Astra Control Center unterstützt mehrere Kubernetes-Distributionen. Für Red hat OpenShift sind die unterstützten Versionen die Red hat OpenShift Container Platform 4.8 oder 4.9.
- Astra Control Center benötigt zusätzlich zu den Anforderungen der Anwendungsressourcen der Umgebung und des Endbenutzers folgende Ressourcen:

Komponenten	Anforderungen
Storage-Back-End-Kapazität	Mindestens 500 GB verfügbar
Worker-Nodes	Mindestens 3 Worker-Nodes mit 4 CPU-Kernen und 12 GB RAM
Vollständig qualifizierte Domänenname (FQDN)-Adresse	Eine FQDN-Adresse für Astra Control Center
Astra Trident	Astra Trident 21.04 oder höher ist installiert und konfiguriert
Eingangs-Controller oder Load-Balancer	Konfigurieren Sie den Ingress-Controller so, dass Astra Control Center mit einer URL oder einem Load-Balancer zur Bereitstellung von IP-Adressen bereitgestellt wird, die sich auf den FQDN beziehen

- Sie benötigen eine bereits vorhandene private Bildregistrierung, in die Sie die Astra Control Center-Bilder übertragen können. Sie müssen die URL der Bildregistrierung angeben, in der Sie die Bilder hochladen.

Einige Images werden bei der Ausführung bestimmter Workflows entfernt und Container werden bei Bedarf erstellt und zerstört.

- Astra Control Center erfordert, dass eine Storage-Klasse erstellt und als Standard-Storage-Klasse eingestellt wird. Astra Control Center unterstützt die folgenden ONTAP-Treiber von Astra Trident:
  - ontap-nas
  - ontap-nas-Flexgroup
  - ontap-san
  - ontap-san-Ökonomie

Astra Trident ist in den implementierten OpenShift-Clustern mit einem ONTAP-Back-End installiert und konfiguriert. Außerdem wird eine Standard-Storage-Klasse definiert.

- Zum Klonen von Applikationen in OpenShift-Umgebungen muss das Astra Control Center OpenShift erlauben, Volumes anzuhängen und die Eigentümerschaft von Dateien zu ändern. Um die ONTAP Exportrichtlinie zu ändern, um diese Vorgänge zu ermöglichen, führen Sie die folgenden Befehle aus:

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

Wenn Sie eine zweite OpenShift-Betriebsumgebung als gemanagte Computing-Ressource hinzufügen möchten, stellen Sie sicher, dass die Astra Trident Volume Snapshot-Funktion aktiviert ist. Lesen Sie den offiziellen Abschnitt zum Aktivieren und Testen von Volume-Snapshots mit Astra Trident "Astra Trident Anweisungen".

- A "VolumeSnapClass" Sollte auf allen Kubernetes-Clustern konfiguriert werden, von denen die Applikationen gemanagt werden. Dazu könnte auch der K8s-Cluster gehören, auf dem Astra Control Center installiert ist. Astra Control Center kann Anwendungen auf dem K8s-Cluster verwalten, auf dem es ausgeführt wird.

Anforderungen für das Applikationsmanagement

- **Lizenzierung.** um Anwendungen mit Astra Control Center zu verwalten, benötigen Sie eine Astra Control Center-Lizenz.
- **Namesaces.** Ein Namespace ist die größte Instanz, die von Astra Control Center als Anwendung verwaltet werden kann. Sie können Komponenten anhand der Anwendungsbezeichnungen und benutzerdefinierten Beschriftungen in einem bestehenden Namespace herausfiltern und als Anwendung eine Untermenge von Ressourcen verwalten.
- **StorageClass.** Wenn Sie eine Anwendung mit einem explizit eingestellten StorageClass installieren und die Anwendung klonen müssen, muss das Zielcluster für den Klonvorgang die ursprünglich angegebene StorageClass haben. Klonen einer Applikation, deren StorageClass explizit auf Cluster festgelegt ist, die nicht dieselbe StorageClass aufweisen, schlägt fehl.
- **Kubernetes-Ressourcen.** Applikationen, die Kubernetes-Ressourcen nutzen, die nicht von Astra Control erfasst sind, verfügen möglicherweise nicht über umfassende Datenmanagementfunktionen für Applikationen. Astra Control kann die folgenden Kubernetes-Ressourcen erfassen:

Kubernetes-Ressourcen		
ClusterCole	ClusterrollenBding	Konfigmap
KundenressourcenDefinition	Benutzerressource	Kronjob
DemonSet	Horizon PodAutoscaler	Eindringen
BereitstellungConfig	MutatingWebhook	PersistentVolumeClaim
Pod	PodDisruptionBudget	PodTemplate
Netzwerkrichtlinie	ReplicaSet	Rolle
Rollenverschwarten	Route	Geheim
ValidierenWebhook		

Installieren Sie Astra Control Center mit OpenShift OperatorHub

Das folgende Verfahren installiert Astra Control Center mithilfe des Red hat OperatorHub. In dieser Lösung ist Astra Control Center auf einem Bare-Metal OpenShift Cluster installiert, das unter FlexPod ausgeführt wird.

1. Laden Sie das Astra Control Center Bundle herunter (`astra-control-center-[version].tar.gz`) Vom "NetApp Support Website".
2. Laden Sie die .zip-Datei für die Astra Control Center-Zertifikate und -Schlüssel aus dem herunter "NetApp Support Website".
3. Überprüfen Sie die Signatur des Bundles.

```
openssl dgst -sha256 -verify astra-control-center[version].pub
-signature <astra-control-center[version].sig astra-control-
center[version].tar.gz
```

4. Extrahieren Sie die Astra-Bilder.

```
tar -vxzf astra-control-center-[version].tar.gz
```

5. Wechseln Sie in das Astra-Verzeichnis.

```
cd astra-control-center-[version]
```

6. Fügen Sie die Bilder Ihrer lokalen Registrierung hinzu.

```
For Docker:
docker login [your_registry_path]OR
For Podman:
podman login [your_registry_path]
```

7. Verwenden Sie das entsprechende Skript, um die Bilder zu laden, die Bilder zu kennzeichnen und sie in Ihre lokale Registrierung zu übertragen.

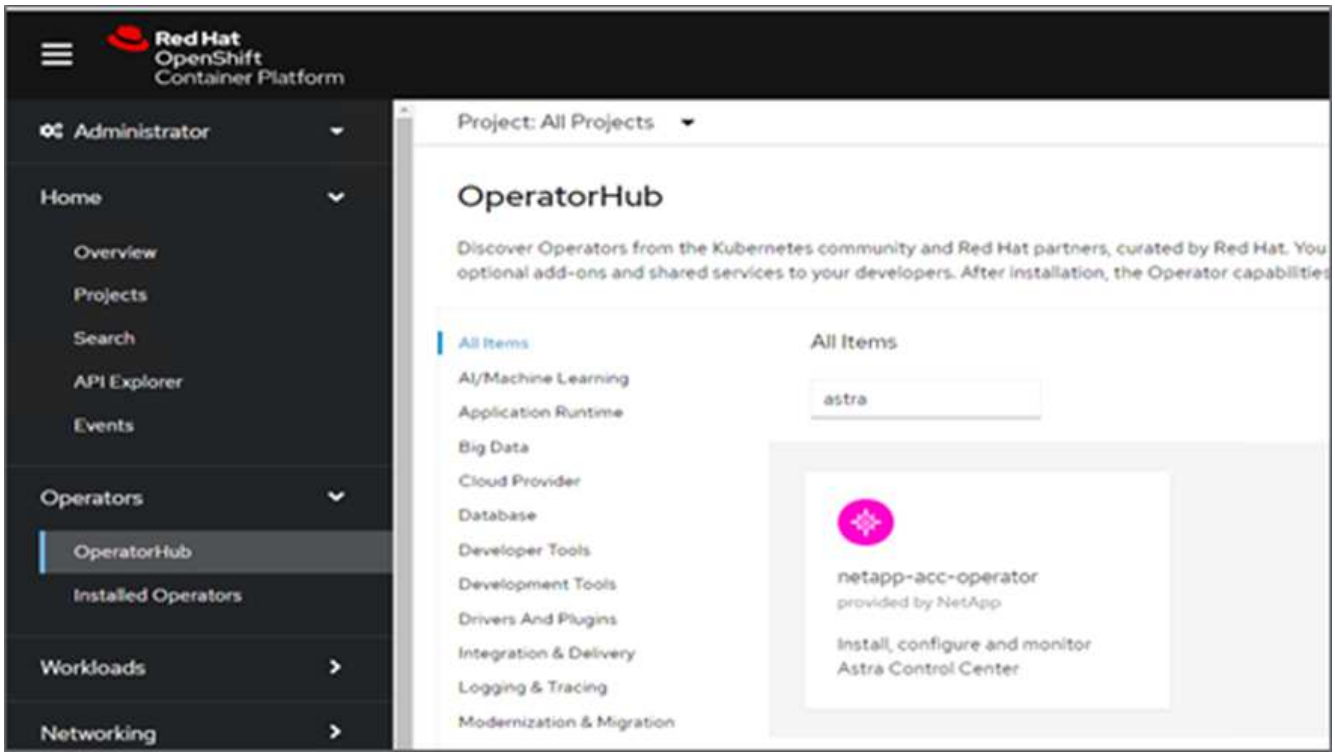
   Für Docker:

```
export REGISTRY=[Docker_registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded
image: //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done
```

   Für Podman:

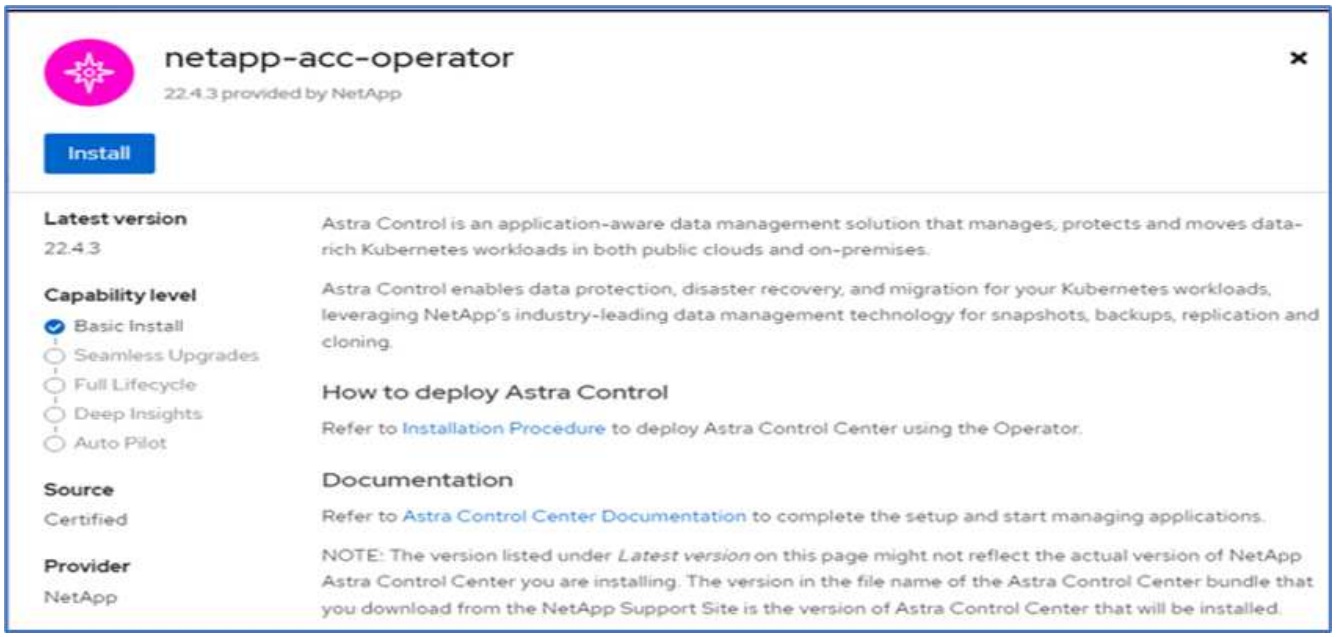
```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  podman push ${REGISTRY}/${astraImage}
done
```

8. Melden Sie sich bei der Bare-Metal OpenShift Cluster Webkonsole an. Wählen Sie im Menü „Seite“ die Option „Operatoren“ > „OperatorHub“. Eingabe `astra` Um die aufzulisten `netapp-acc-operator`.

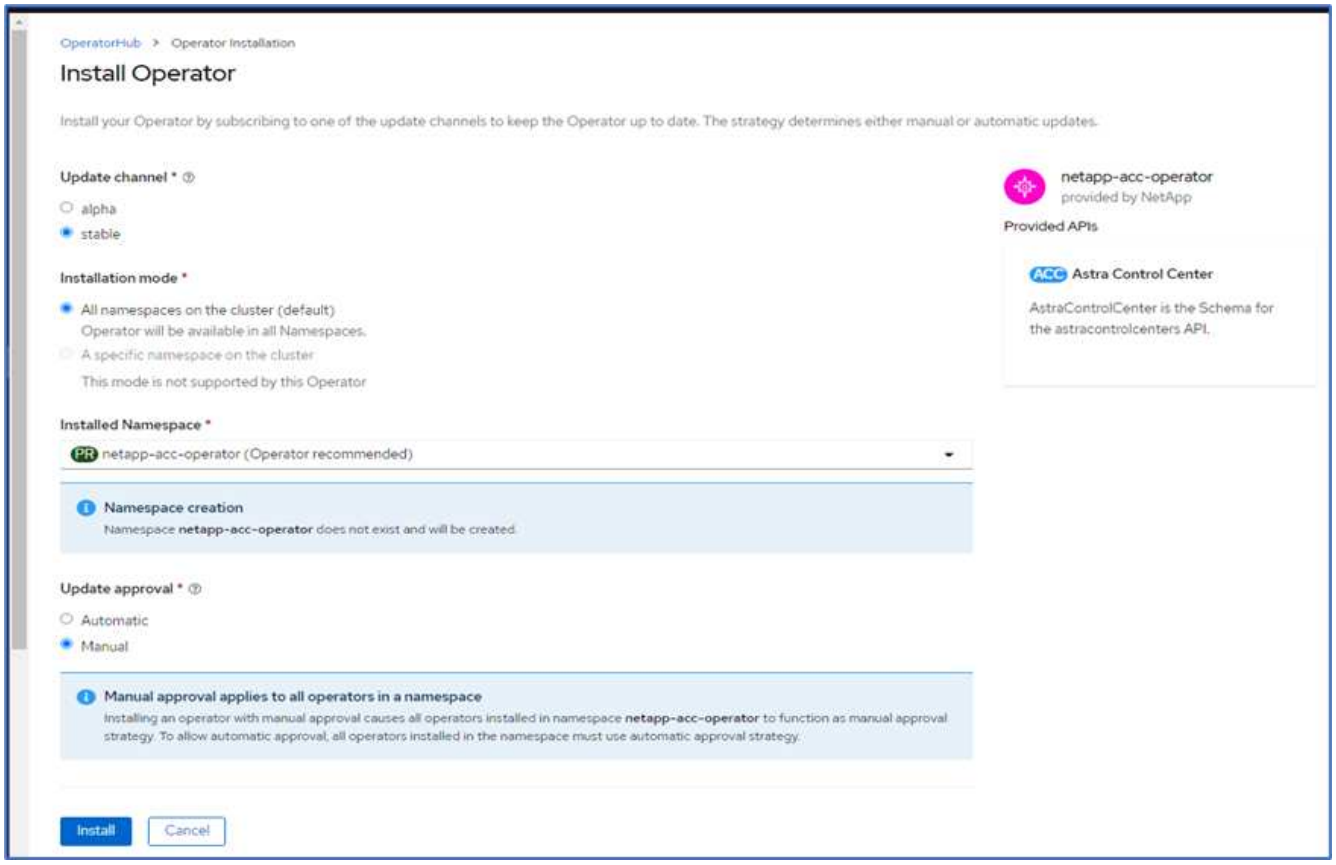


`netapp-acc-operator` Ist ein zertifizierter Red hat OpenShift Operator und ist im OperatorHub-Katalog aufgeführt.

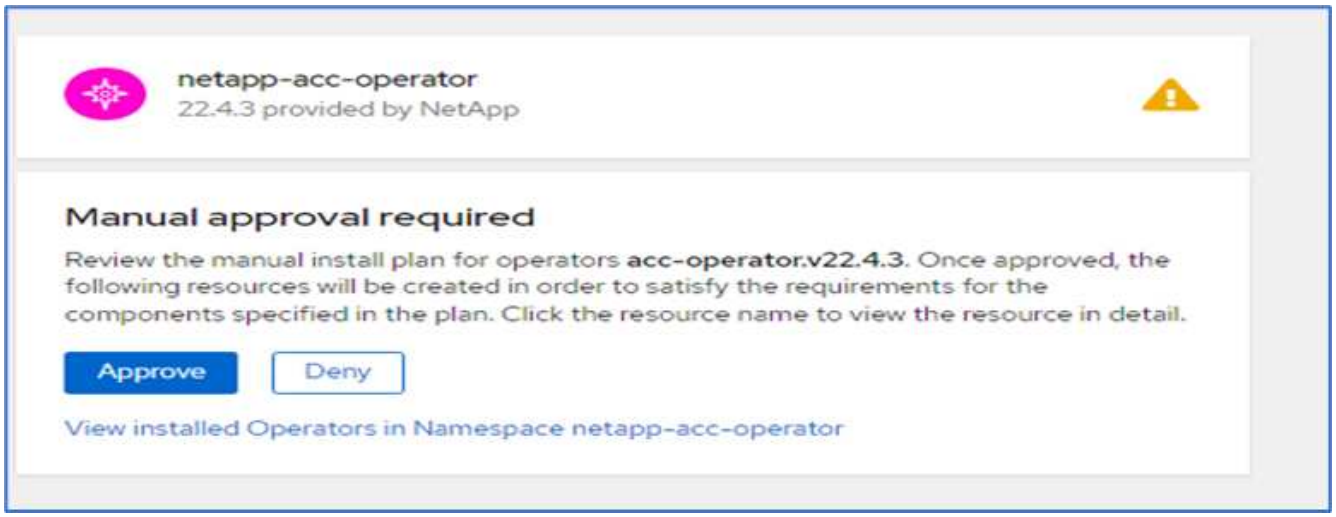
9. Wählen Sie `netapp-acc-operator` Und klicken Sie auf Installieren.



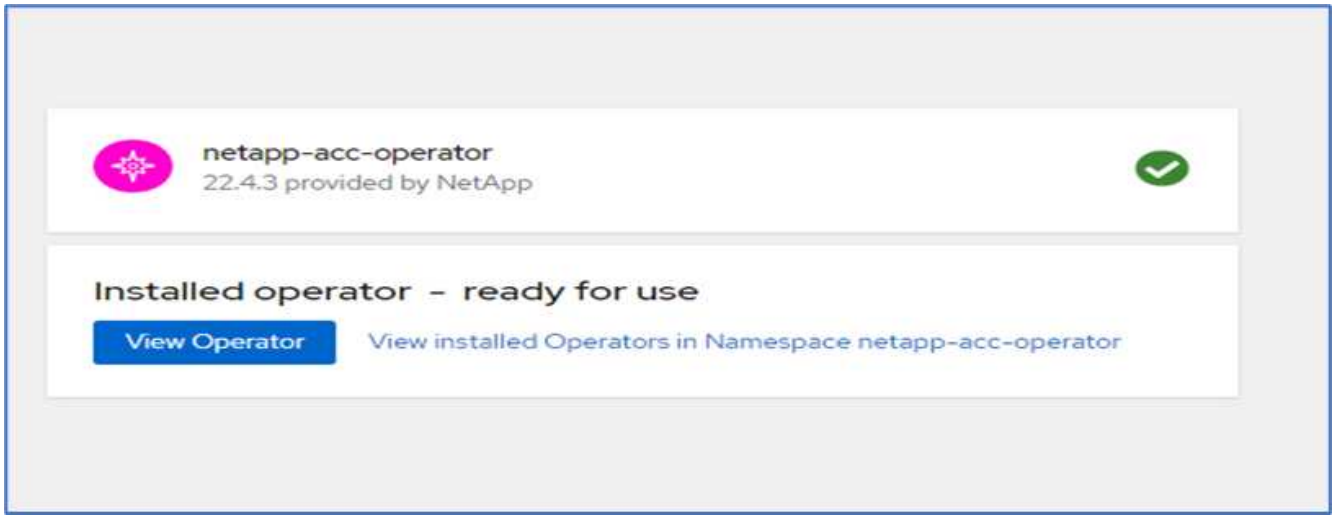
10. Wählen Sie die entsprechenden Optionen aus, und klicken Sie auf Installieren.



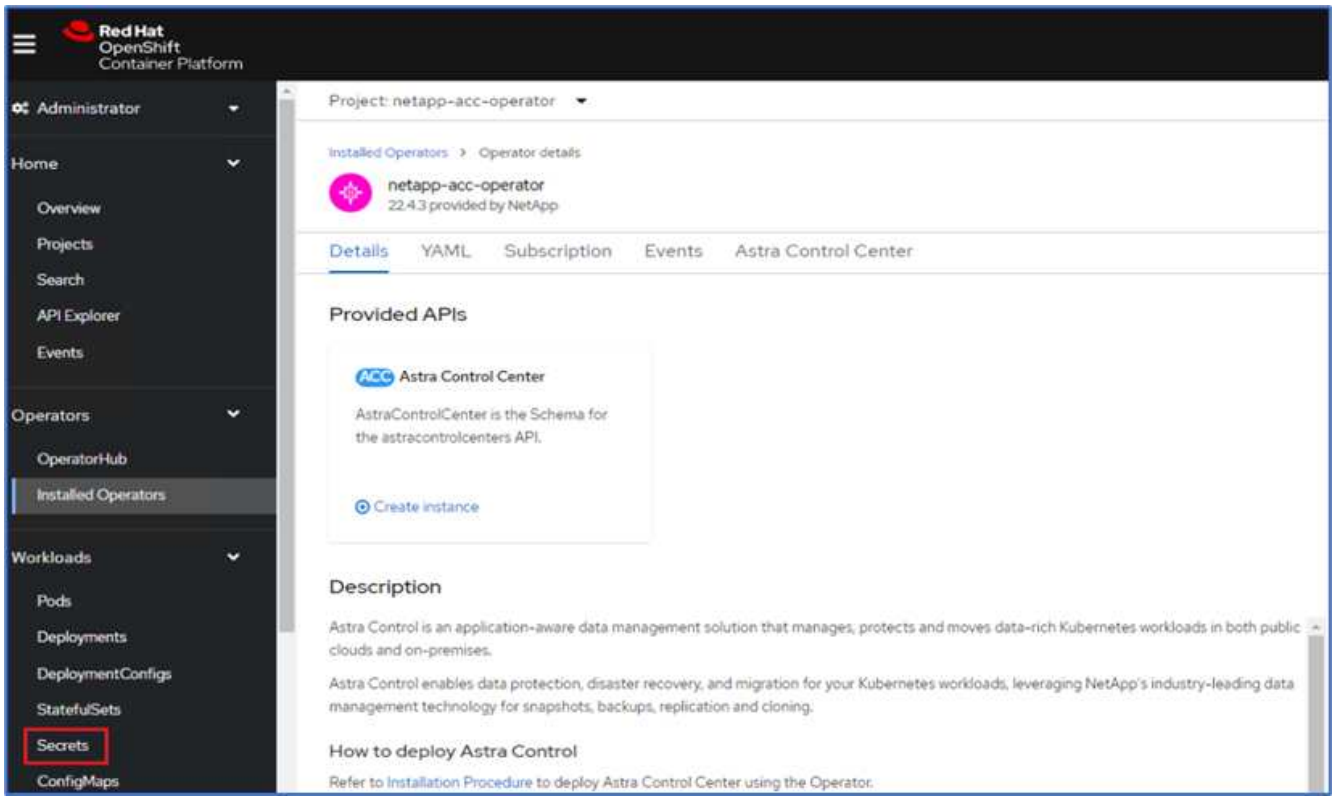
11. Genehmigen Sie die Installation, und warten Sie, bis der Bediener installiert ist.



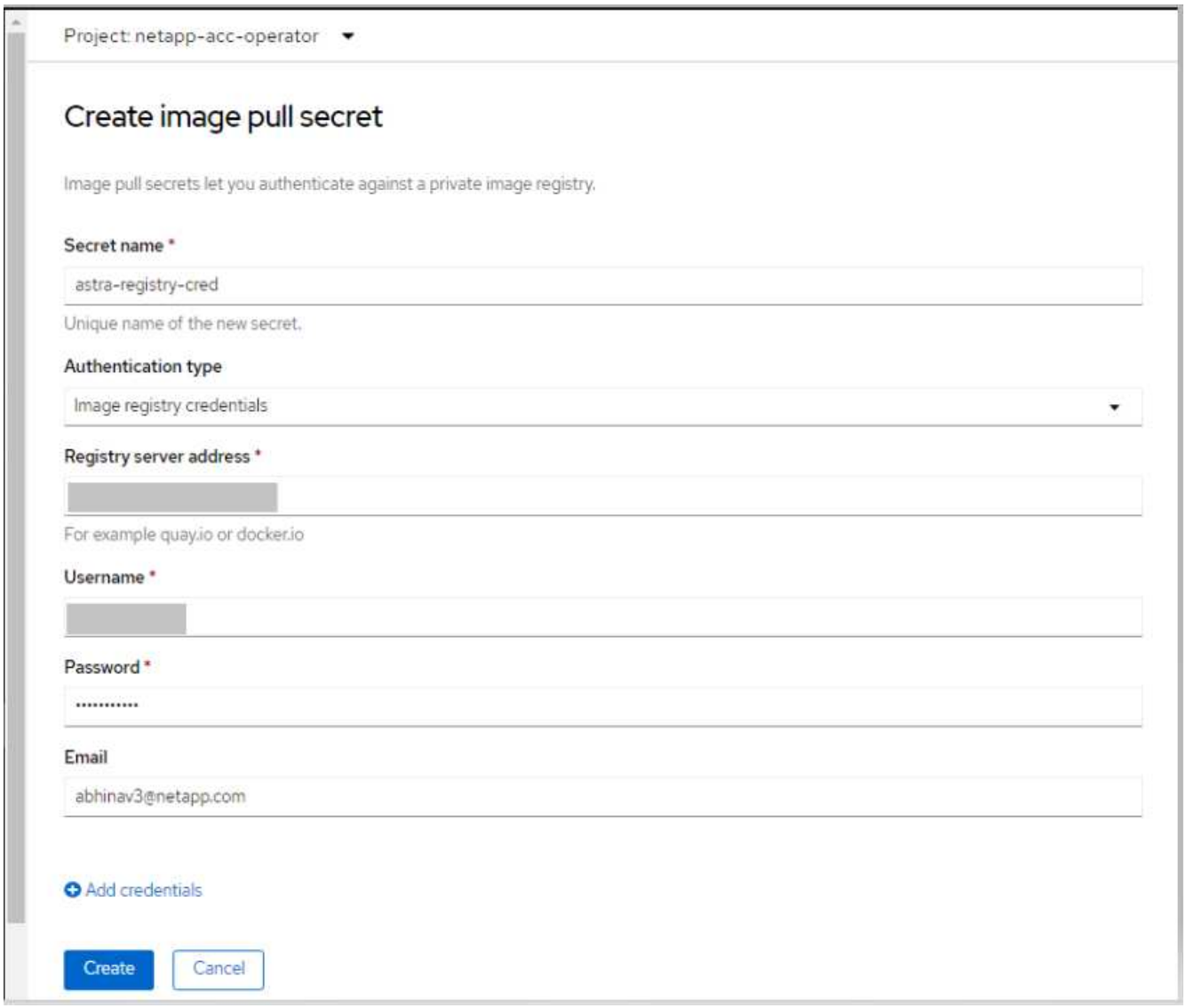
12. In dieser Phase ist der Bediener erfolgreich installiert und betriebsbereit. Klicken Sie auf Ansichtsverwalter, um die Installation des Astra Control Centers zu starten.



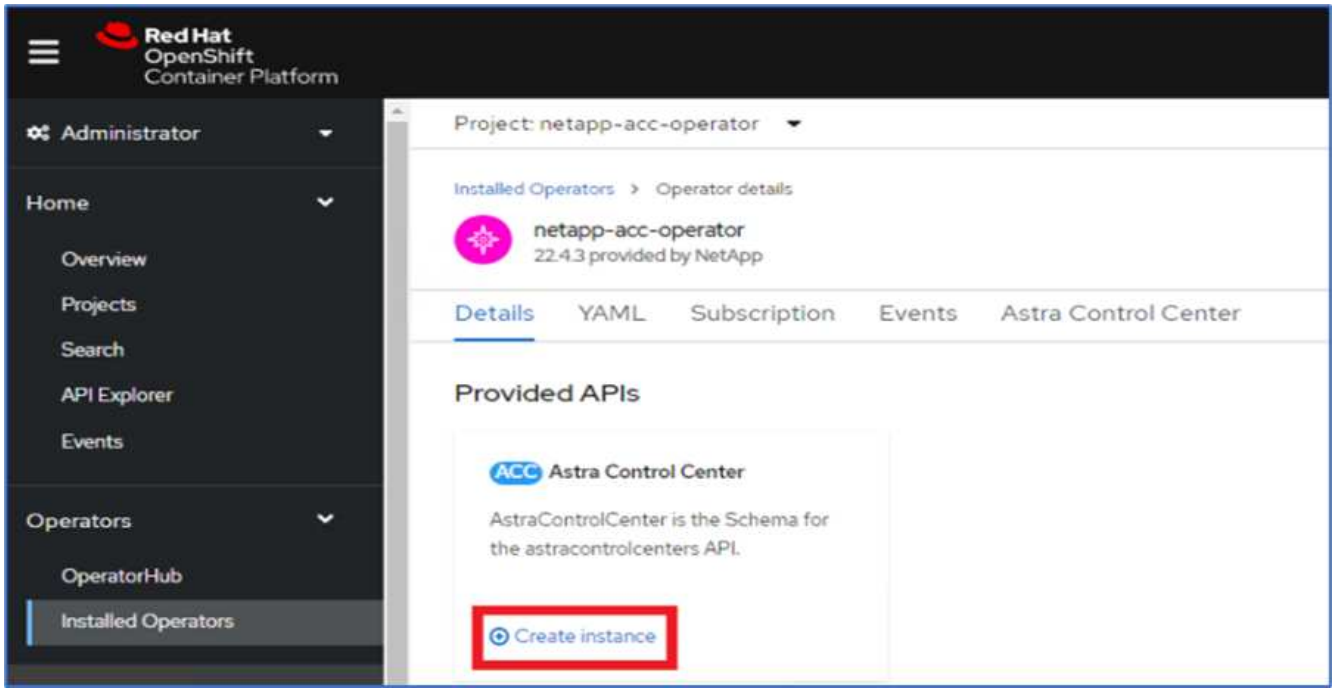
13. Erstellen Sie vor der Installation von Astra Control Center das Pull Secret, um Astra-Bilder aus der Docker-Registry, die Sie früher verschoben haben, herunterzuladen.



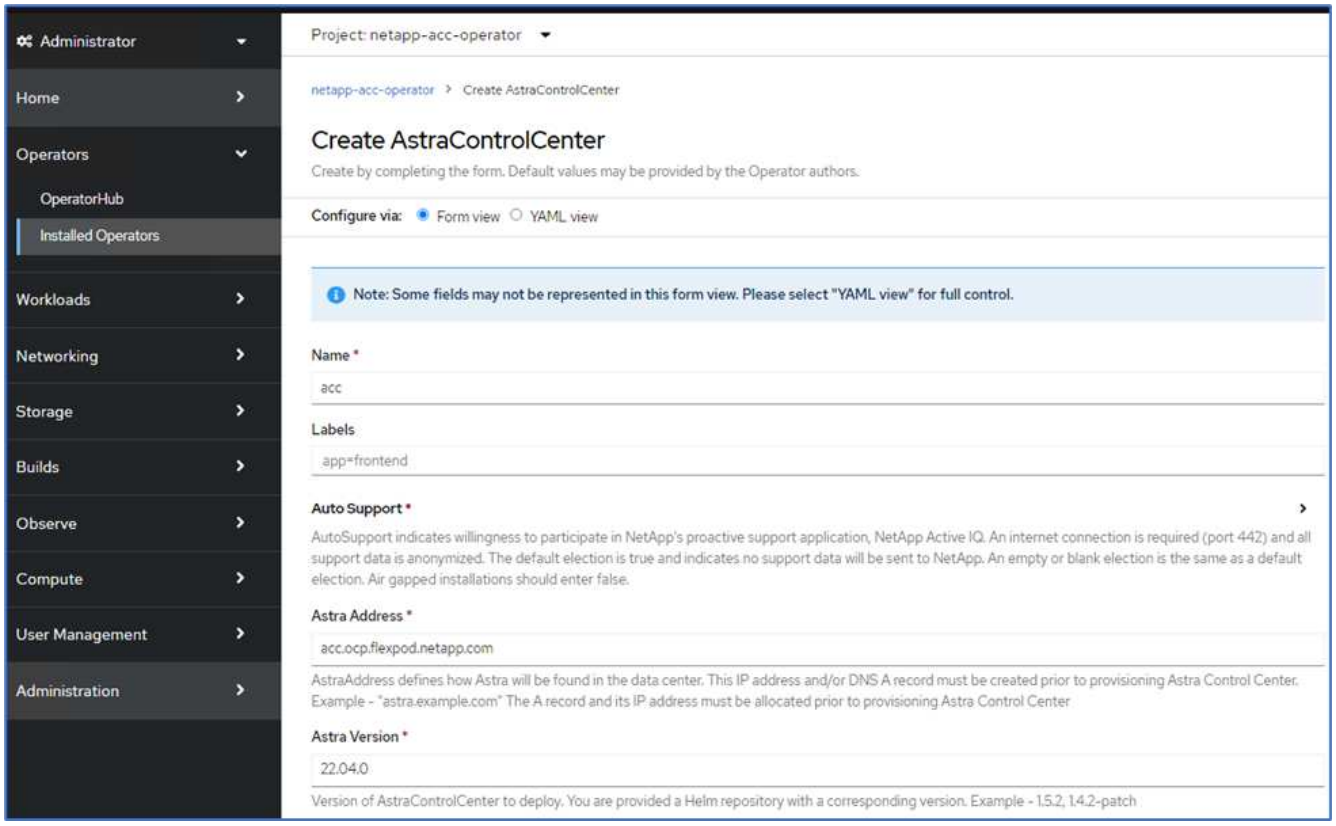
14. Damit Sie die Astra Control Center-Bilder von Ihrer privaten Docker-Repo abrufen können, sollten Sie im ein Geheimnis schaffen `netapp-acc-operator` Namespace. Dieser geheime Name wird in einem späteren Schritt im Astra Control Center YAML-Manifest angegeben.



15. Wählen Sie im Seitenmenü Operatoren > Installed Operators aus, und klicken Sie im Abschnitt bereitgestellte APIs auf Create Instance.



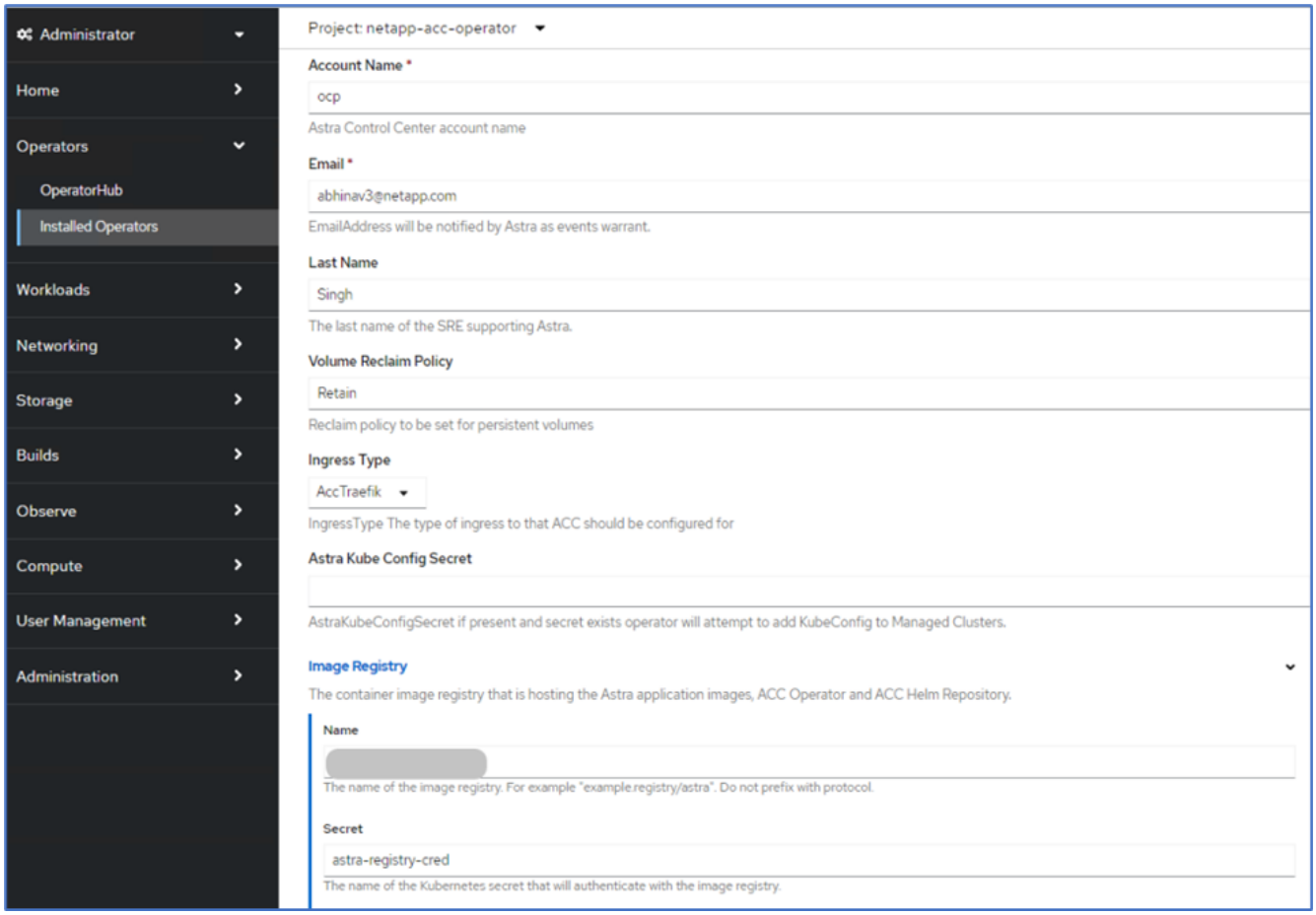
16. Füllen Sie das Formular AstraControlCenter erstellen aus. Geben Sie den Namen, die Astra-Adresse und die Astra-Version an.



Geben Sie unter Astra Address die FQDN-Adresse für Astra Control Center an. Diese Adresse wird für den Zugriff auf die Astra Control Center Webkonsole verwendet. Der FQDN sollte auch in einem erreichbaren IP-Netzwerk auflösen und im DNS konfiguriert werden.

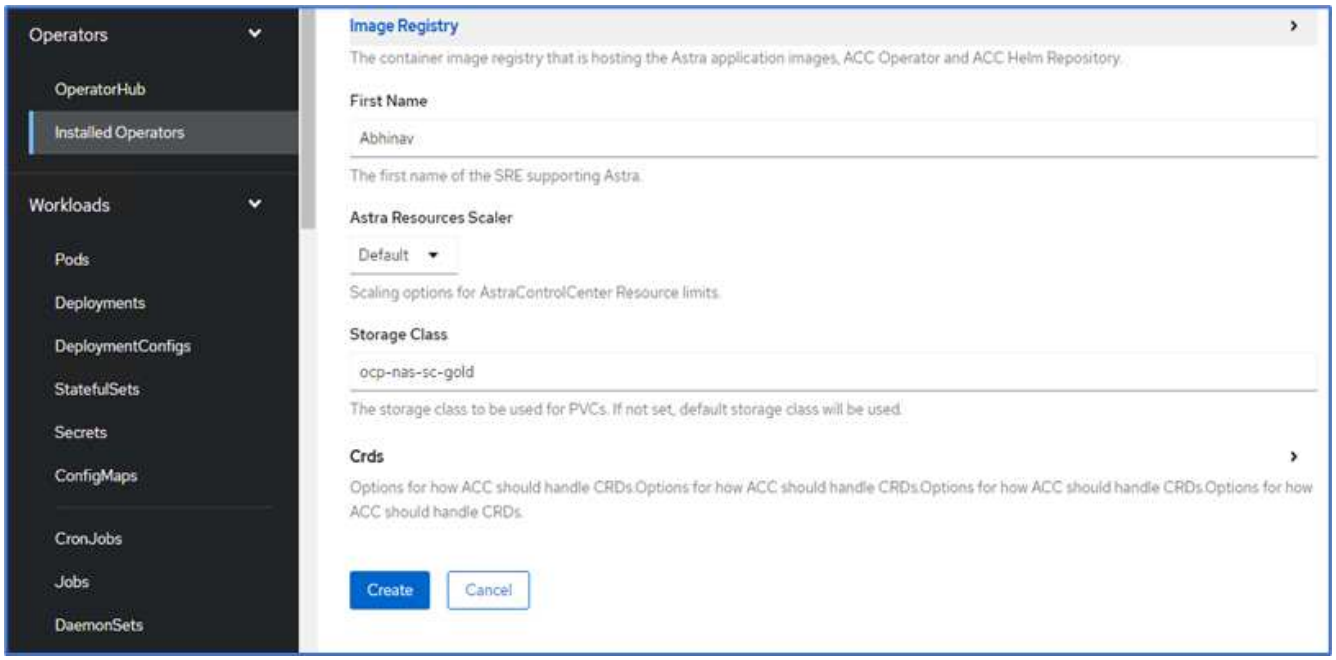
17. Geben Sie einen Kontonamen, eine E-Mail-Adresse, einen Administrator-Nachnamen ein, und behalten

Sie die standardmäßige Richtlinie zur Rückgewinnung von Volumes bei. Wenn Sie einen Load Balancer verwenden, setzen Sie den Ingress-Typ auf `AccTraefik`. Wählen Sie andernfalls Generic für aus `Ingress.Controller`. Geben Sie unter Image Registry den Registry-Pfad für das Container-Image und den geheimen Schlüssel ein.

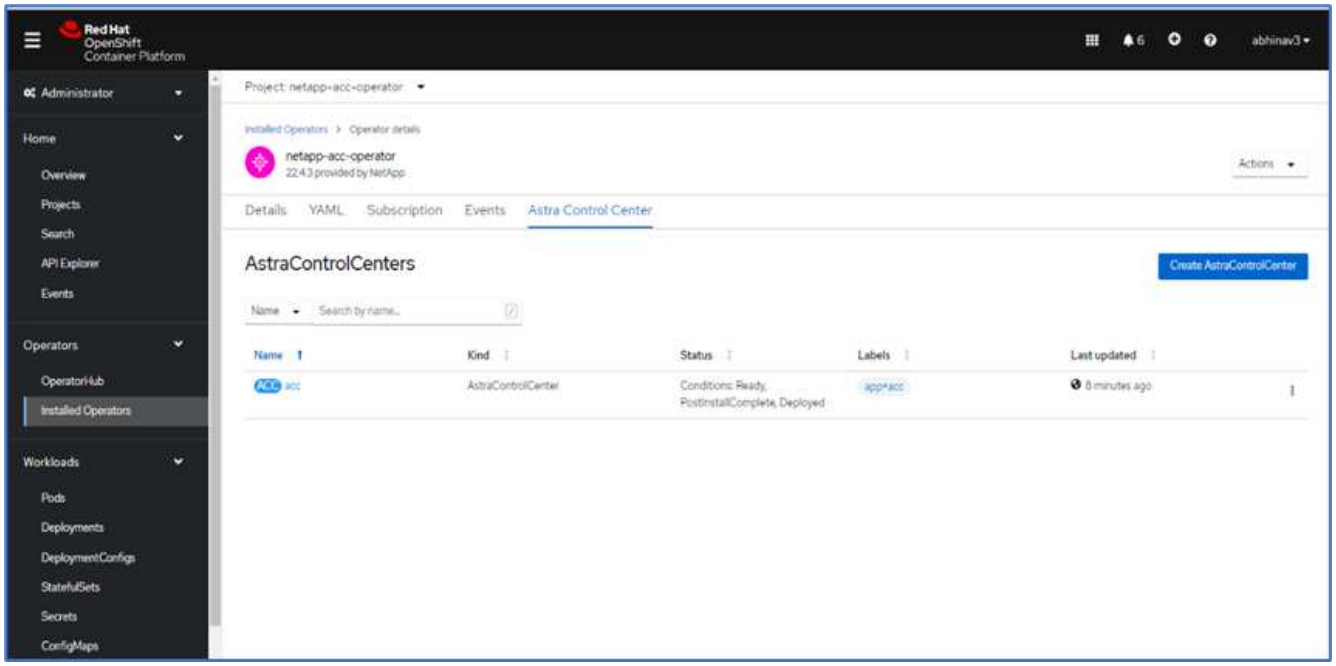


In dieser Lösung wird der Metallb Load Balancer eingesetzt. Daher ist der Eingangstyp AccTraefik. Das Astra Control Center Trafik Gateway wird damit als Kubernetes Service des Typ Load Balancer bereitgestellt.

18. Geben Sie den Vornamen des Administrators ein, konfigurieren Sie die Skalierung von Ressourcen und stellen Sie die Storage-Klasse bereit. Klicken Sie auf Erstellen .



Der Status der Astra Control Center-Instanz sollte von „Bereitstellen“ auf „bereit“ geändert werden.



19. Überprüfen Sie, ob alle Systemkomponenten erfolgreich installiert wurden und alle Pods ausgeführt werden.

```
root@abhinav-ansible# oc get pods -n netapp-acc-operator
NAME                                          READY   STATUS
RESTARTS   AGE
acc-helm-repo-77745b49b5-7zg2v                1/1     Running   0
10m
acc-operator-controller-manager-5c656c44c6-tqnmn   2/2     Running   0
13m
```

```
activity-589c6d59f4-x2sfs                          1/1     Running   0
6m4s
api-token-authentication-4q5lj                     1/1     Running   0
5m26s
api-token-authentication-pzptd                     1/1     Running   0
5m27s
api-token-authentication-tbtg6                     1/1     Running   0
5m27s
asup-669df8d49-qps54                               1/1     Running   0
5m26s
authentication-5867c5f56f-dnpp2                    1/1     Running   0
3m54s
bucketservice-85495bc475-5zcc5                     1/1     Running   0
5m55s
cert-manager-67f486bbc6-txhh6                      1/1     Running   0
9m5s
cert-manager-cainjector-75959db744-4l5p5           1/1     Running   0
9m6s
cert-manager-webhook-765556b869-g6wdf              1/1     Running   0
9m6s
cloud-extension-5d595f85f-txrfl                    1/1     Running   0
5m27s
cloud-insights-service-674649567b-5s4wd            1/1     Running   0
5m49s
composite-compute-6b58d48c69-46vhc                 1/1     Running   0
6m11s
composite-volume-6d447fd959-chnrt                  1/1     Running   0
5m27s
credentials-66668f8ddd-8qc5b                       1/1     Running   0
7m20s
entitlement-fd6fc5c58-wxnmh                        1/1     Running   0
6m20s
features-756bbb7c7c-rgcrm                          1/1     Running   0
5m26s
fluent-bit-ds-278pg                                1/1     Running   0
3m35s
fluent-bit-ds-5pqc6                                1/1     Running   0
3m35s
fluent-bit-ds-8l7cq                                1/1     Running   0
3m35s
fluent-bit-ds-9qbft                                1/1     Running   0
3m35s
fluent-bit-ds-nj475                                1/1     Running   0
3m35s
fluent-bit-ds-x9pd8                                1/1     Running   0
3m35s
```

```
graphql-server-698d6f4bf-kftwc                    1/1     Running   0
3m20s
identity-5d4f4c87c9-wjz6c                         1/1     Running   0
6m27s
influxdb2-0                                       1/1     Running   0
9m33s
krakend-657d44bf54-8cb56                          1/1     Running   0
3m21s
license-594bbdc-rghdg                             1/1     Running   0
6m28s
login-ui-6c65fbbbd4-jg8wz                         1/1     Running   0
3m17s
loki-0                                            1/1     Running   0
9m30s
metrics-facade-75575f69d7-hnlk6                   1/1     Running   0
6m10s
monitoring-operator-65dff79cfb-z78vk              2/2     Running   0
3m47s
nats-0                                            1/1     Running   0
10m
nats-1                                            1/1     Running   0
9m43s
nats-2                                            1/1     Running   0
9m23s
nautilus-7bb469f857-4hlc6                         1/1     Running   0
6m3s
nautilus-7bb469f857-vz94m                         1/1     Running   0
4m42s
openapi-8586db4bcd-gwwvf                          1/1     Running   0
5m41s
packages-6bdb949cfb-nrq8l                         1/1     Running   0
6m35s
polaris-consul-consul-server-0                    1/1     Running   0
9m22s
polaris-consul-consul-server-1                    1/1     Running   0
9m22s
polaris-consul-consul-server-2                    1/1     Running   0
9m22s
polaris-mongodb-0                                 2/2     Running   0
9m22s
polaris-mongodb-1                                 2/2     Running   0
8m58s
polaris-mongodb-2                                 2/2     Running   0
8m34s
polaris-ui-5df7687dbd-trcnf                       1/1     Running   0
3m18s
```

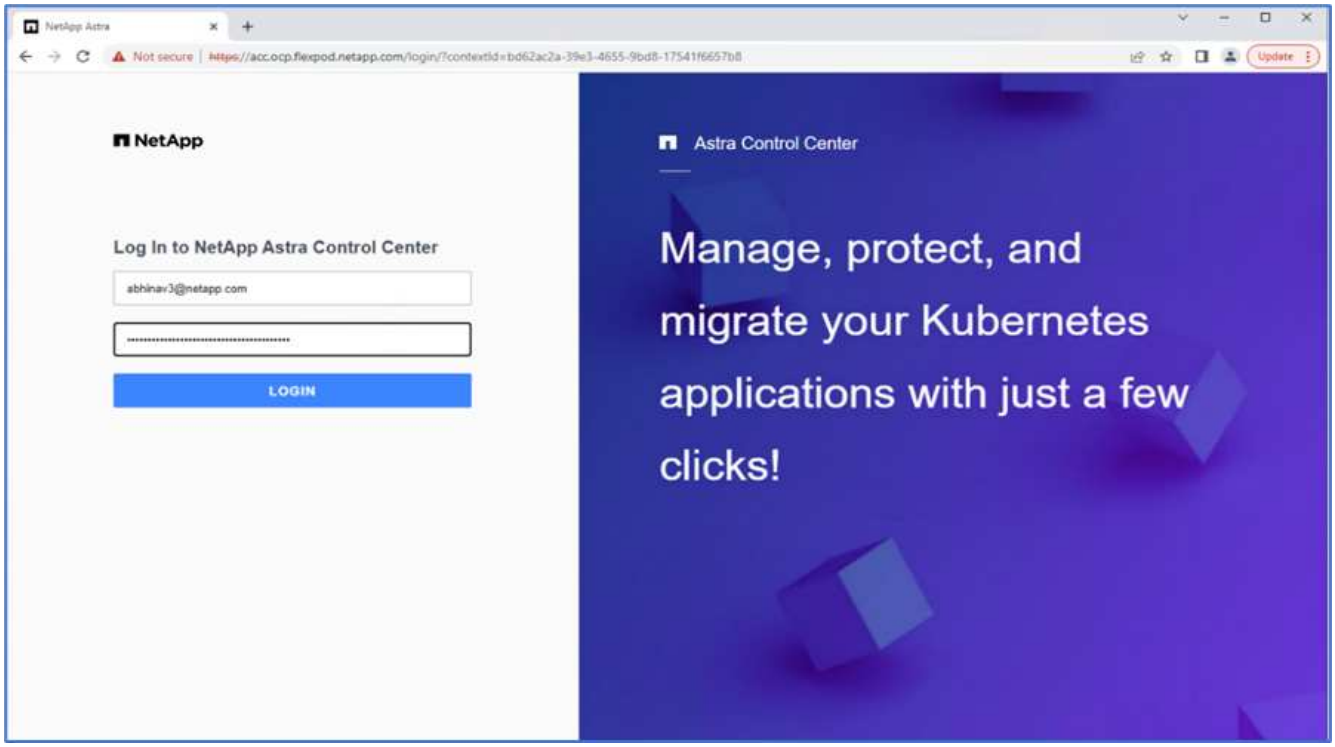
```
polaris-vault-0                                   1/1     Running   0
9m18s
polaris-vault-1                                   1/1     Running   0
9m18s
polaris-vault-2                                   1/1     Running   0
9m18s
public-metrics-7b96476f64-j88bw                   1/1     Running   0
5m48s
storage-backend-metrics-5fd6d7cd9c-vcb4j          1/1     Running   0
5m59s
storage-provider-bb85ff965-m7qrq                  1/1     Running   0
5m25s
telegraf-ds-4zqgz                                 1/1     Running   0
3m36s
telegraf-ds-cp9x4                                 1/1     Running   0
3m36s
telegraf-ds-h4n59                                 1/1     Running   0
3m36s
telegraf-ds-jnp2q                                 1/1     Running   0
3m36s
telegraf-ds-pdz5j                                 1/1     Running   0
3m36s
telegraf-ds-znqtp                                 1/1     Running   0
3m36s
telegraf-rs-rt64j                                 1/1     Running   0
3m36s
telemetry-service-7dd9c74bfc-sfkzt                1/1     Running   0
6m19s
tenancy-d878b7fb6-wf8x9                           1/1     Running   0
6m37s
traefik-6548496576-5v2g6                          1/1     Running   0
98s
traefik-6548496576-g82pq                          1/1     Running   0
3m8s
traefik-6548496576-psn49                          1/1     Running   0
38s
traefik-6548496576-qrkfd                          1/1     Running   0
2m53s
traefik-6548496576-srs6r                          1/1     Running   0
98s
trident-svc-679856c67-78kbt                       1/1     Running   0
5m27s
vault-controller-747d664964-xmn6c                 1/1     Running   0
7m37s
```

Jeder Pod sollte den Status „laufen“ aufweisen. Es kann mehrere Minuten dauern, bevor die System-Pods implementiert sind.

20. Wenn alle Pods ausgeführt werden, führen Sie den folgenden Befehl aus, um das einmalige Passwort abzurufen. Prüfen Sie in der YAML-Version der Ausgabe das `status.deploymentState` Feld für den bereitgestellten Wert, und kopieren Sie anschließend die `status.uuid` Wert: Das Passwort lautet `ACC-` Anschließend der UUID-Wert. (ACC-[UUID]).

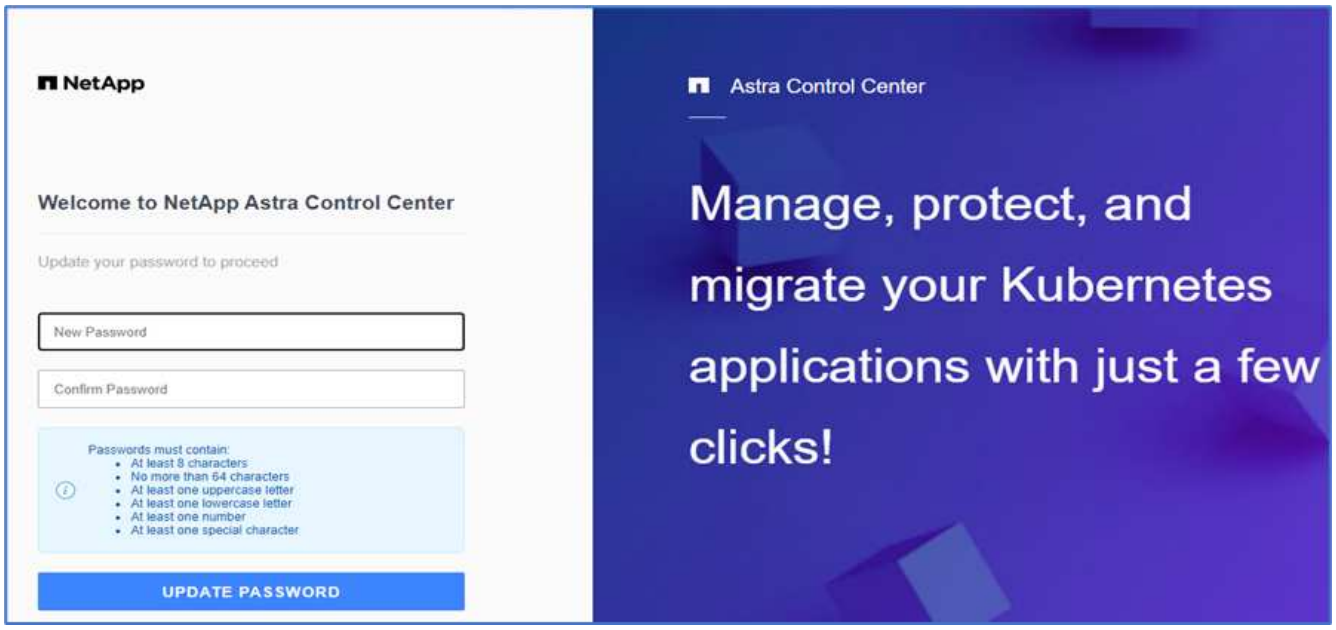
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

21. Navigieren Sie in einem Browser zur URL mithilfe des FQDN, den Sie bereitgestellt haben.
22. Melden Sie sich mit dem Standardbenutzernamen an. Dies ist die E-Mail-Adresse, die während der Installation angegeben wurde, und das einmalige Passwort ACC-[UUID].



Wenn Sie dreimal ein falsches Kennwort eingeben, ist das Administratorkonto 15 Minuten lang gesperrt.

23. Ändern Sie das Passwort, und fahren Sie fort.

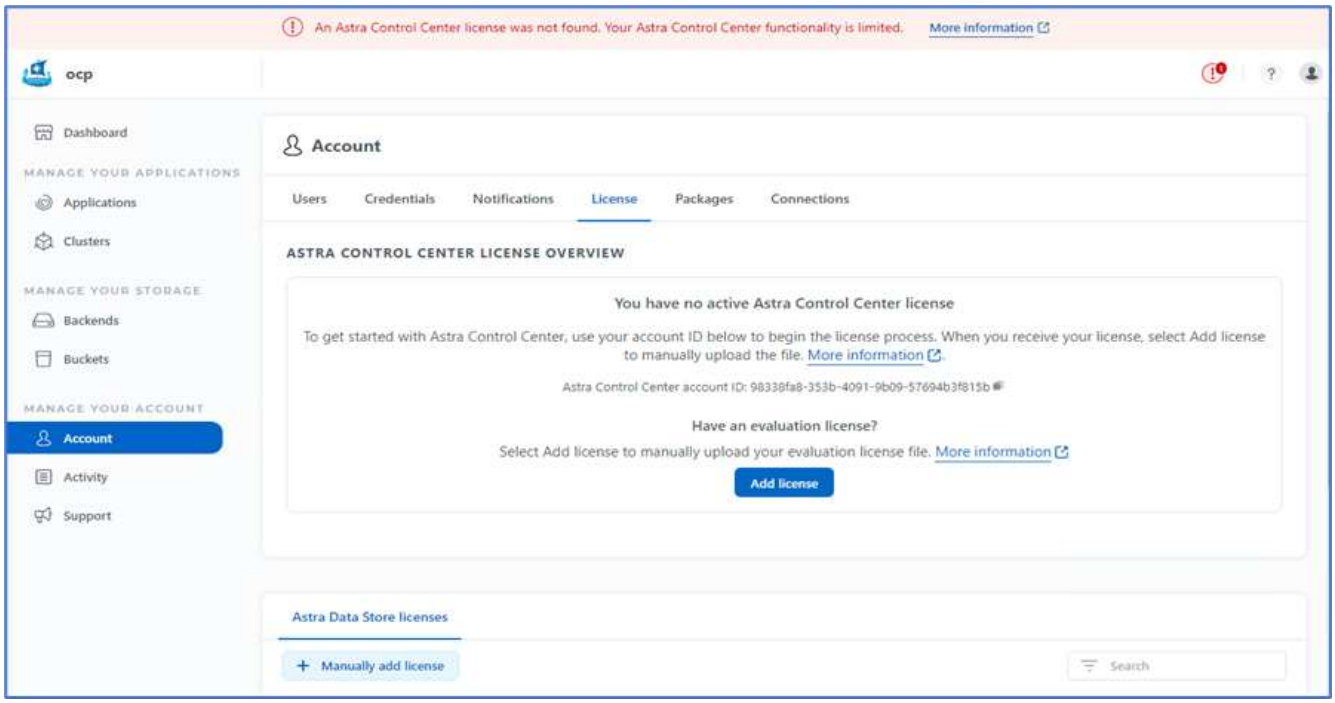


Weitere Informationen zur Installation des Astra Control Center finden Sie im "Astra Control Center – Übersicht über die Installation" Seite.

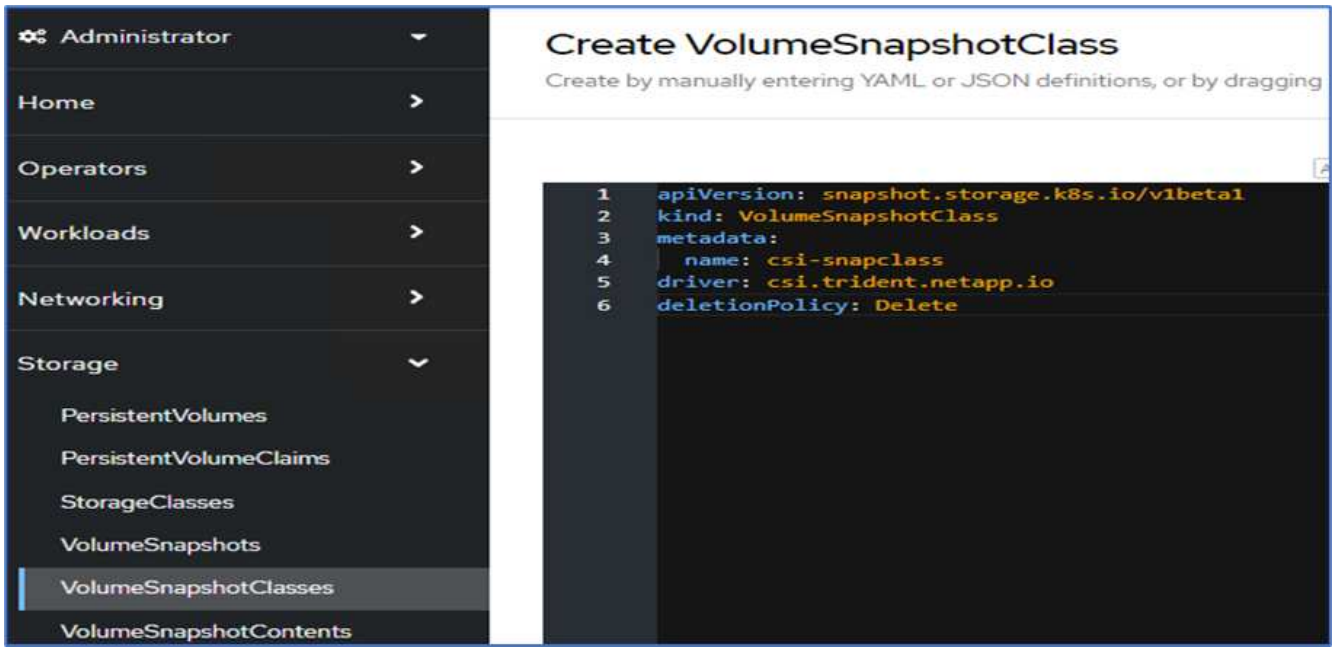
Einrichten des Astra Control Center

Melden Sie sich nach der Installation von Astra Control Center in der UI an, laden Sie die Lizenz hoch, fügen Sie Cluster hinzu, managen Sie den Storage und fügen Sie Buckets hinzu.

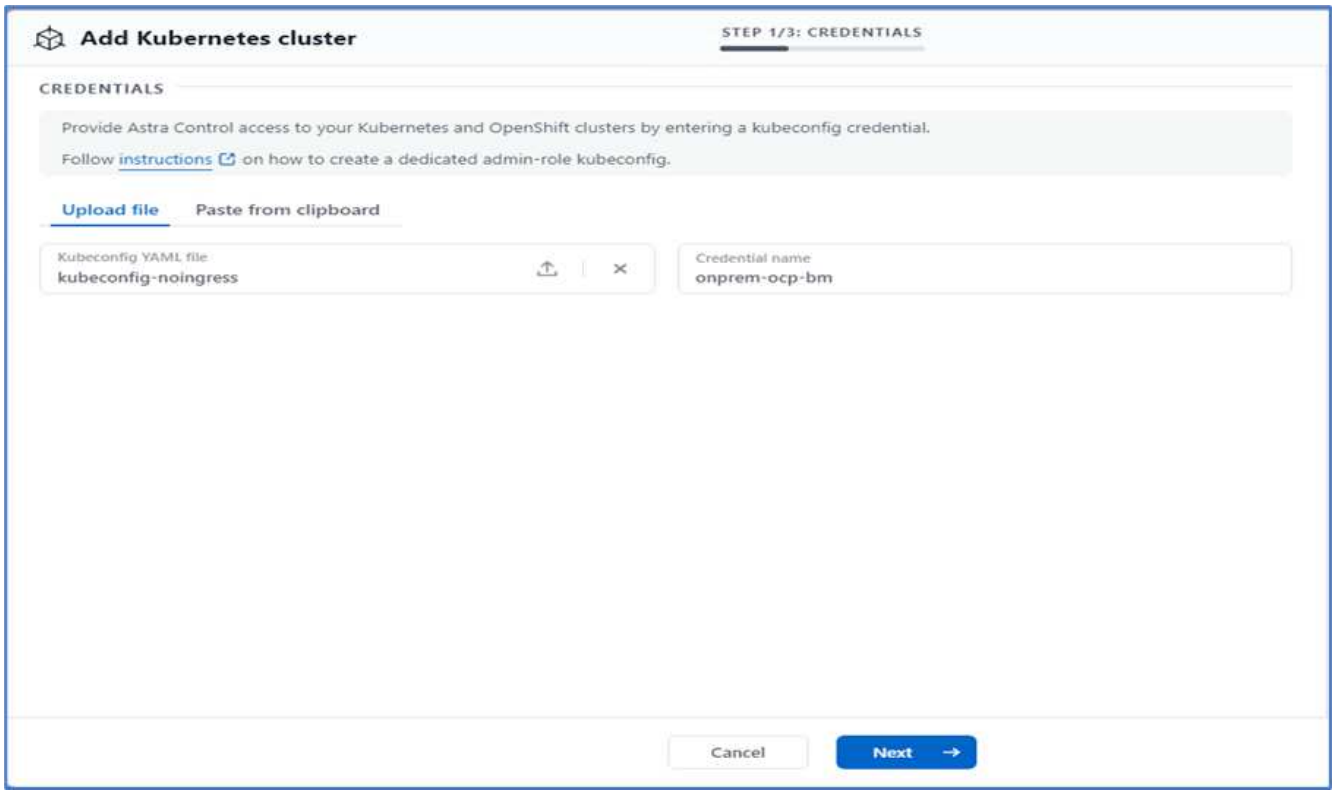
1. Gehen Sie auf der Homepage unter Konto auf die Registerkarte Lizenz und wählen Sie Lizenz hinzufügen, um die Astra-Lizenz hochzuladen.



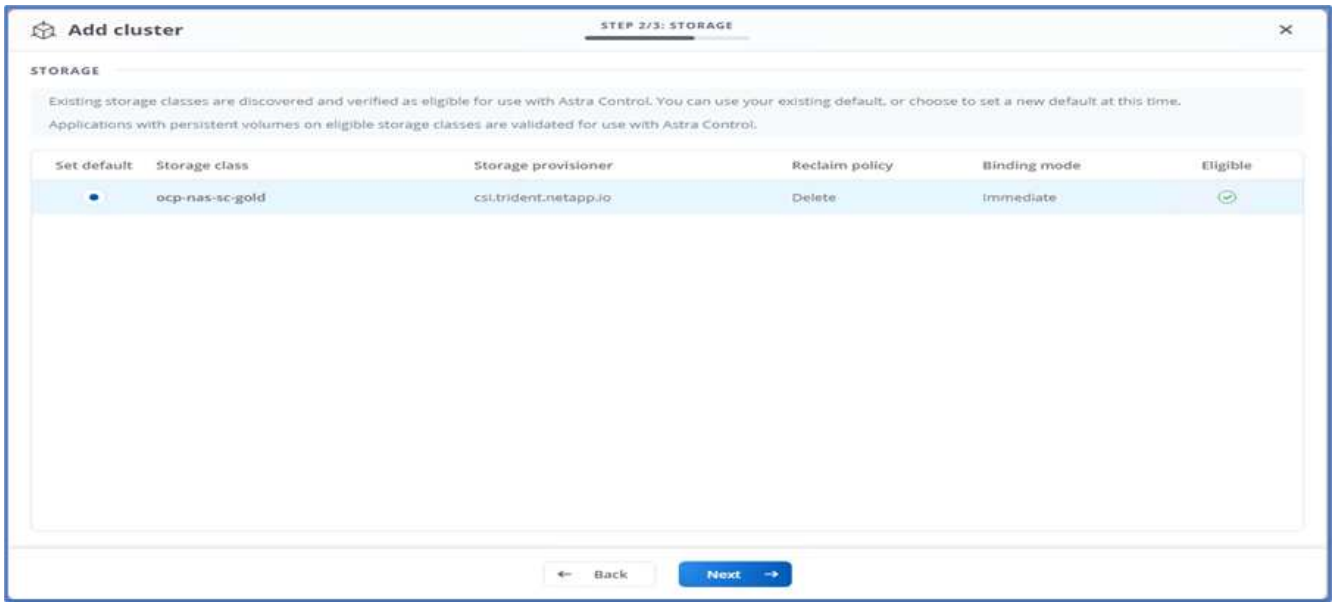
2. Erstellen Sie vor dem Hinzufügen des OpenShift-Clusters über die OpenShift-Webkonsole einen Astra Trident Volume Snapshot. Die Klasse Volume Snapshot wird mit dem konfiguriert `csi.trident.netapp.io` Treiber.



3. Zum Hinzufügen des Kubernetes-Clusters wechseln Sie auf der Startseite zu Clusters und klicken auf Kubernetes-Cluster hinzufügen. Laden Sie anschließend die hoch `kubeconfig` Datei für den Cluster und geben einen Namen für die Anmeldeinformationen an. Klicken Sie Auf Weiter.



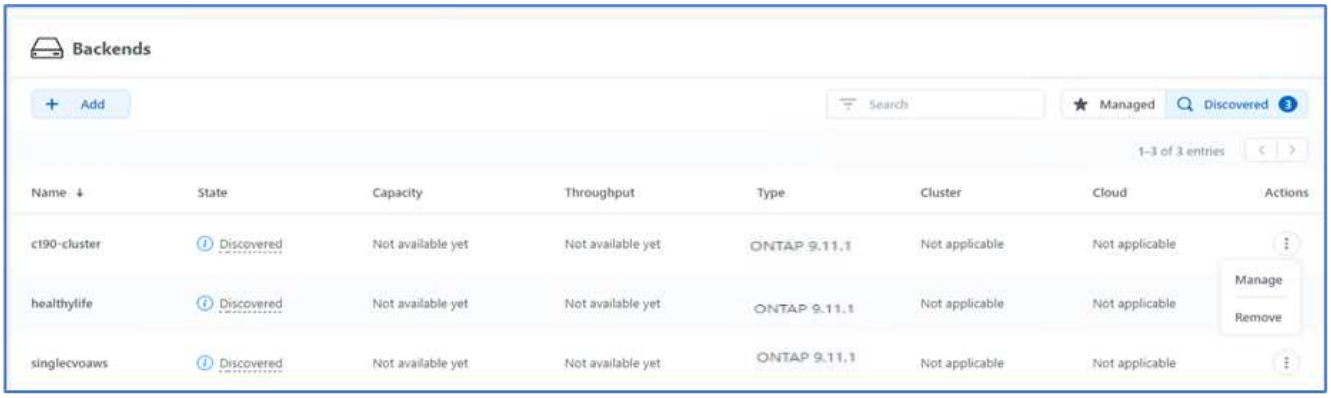
4. Die vorhandenen Speicherklassen werden automatisch erkannt. Wählen Sie die Standard-Storage-Klasse aus, klicken Sie auf Weiter und klicken Sie dann auf Cluster hinzufügen.



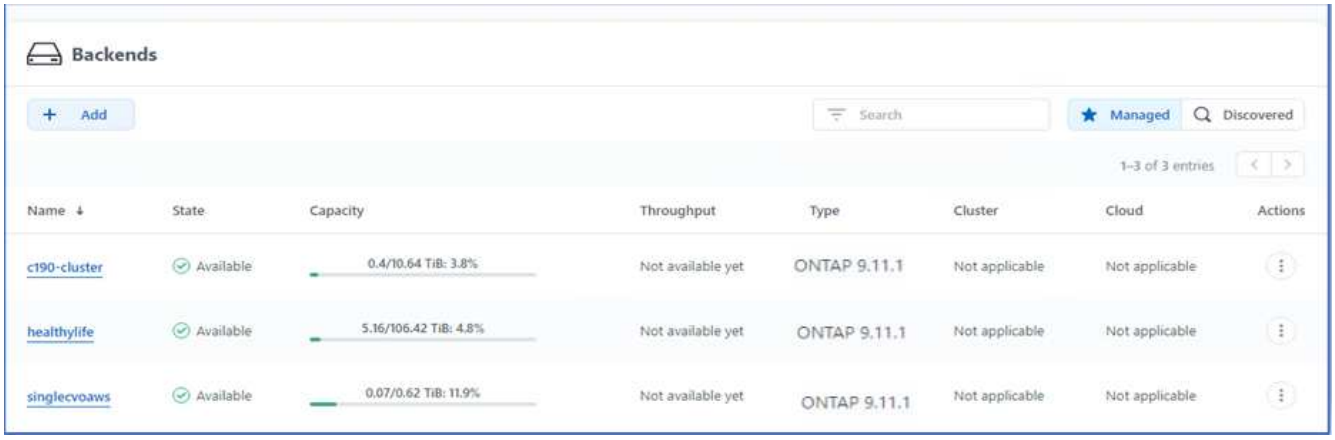
5. Der Cluster wird in wenigen Minuten hinzugefügt. Um weitere Cluster der OpenShift Container Platform hinzuzufügen, wiederholen Sie die Schritte 1 bis 4.

> Wenn Sie eine zusätzliche OpenShift-Betriebsumgebung als verwaltete Computing-Ressource hinzufügen möchten, sollten Sie den Astra Trident in die Umgebung einbinden "VolumeSnapshotClass-Objekte" Werden definiert.

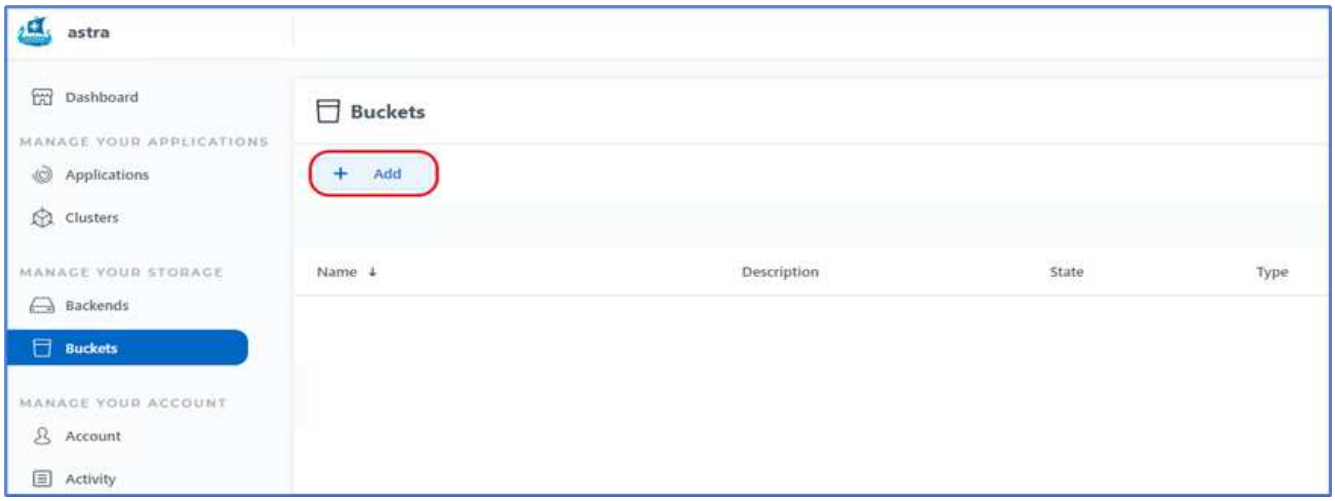
6. Um den Speicher zu verwalten, gehen Sie zu Backend, klicken Sie auf die drei Punkte unter Aktionen gegen das Backend, das Sie verwalten möchten. Klicken Sie Auf Verwalten.



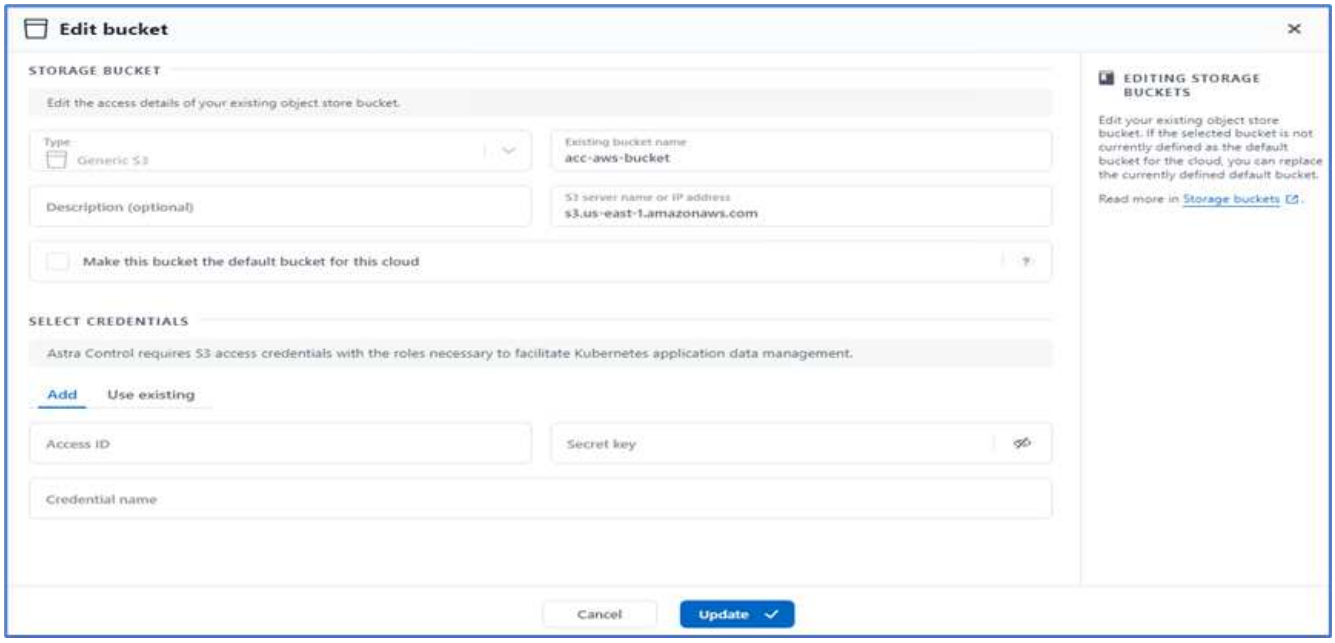
7. Geben Sie die ONTAP Zugangsdaten ein und klicken Sie auf Weiter. Überprüfen Sie die Informationen, und klicken Sie auf verwaltet. Die Back-Ends sollten wie im folgenden Beispiel aussehen.



8. Um Astra Control einen Bucket hinzuzufügen, wählen Sie Eimer aus, und klicken Sie auf Hinzufügen.

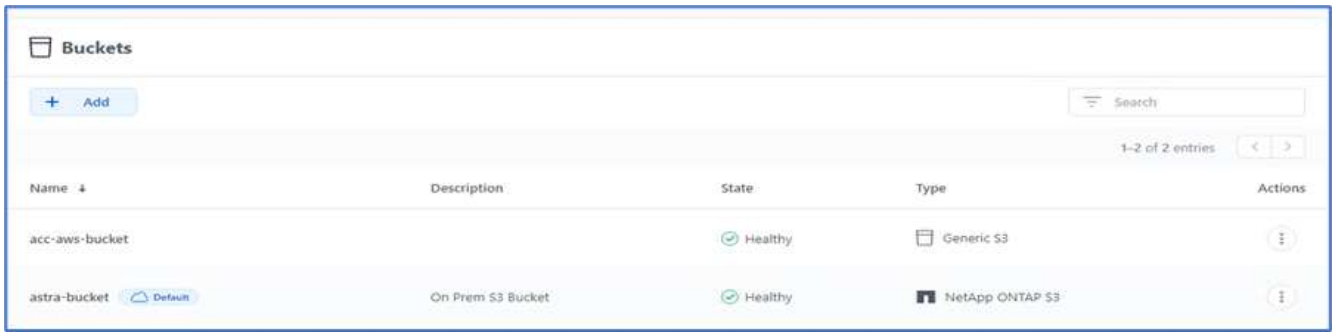


9. Wählen Sie den Bucket-Typ aus und geben Sie den Bucket-Namen, den S3-Servernamen oder die IP-Adresse und S3-Zugangsdaten an. Klicken Sie Auf Aktualisieren.



In dieser Lösung werden AWS S3 und ONTAP S3 Buckets verwendet. Sie können auch StorageGRID verwenden.

Der Bucket-Status sollte sich in einem ordnungsgemäßen Zustand befinden.



Im Rahmen der Kubernetes-Cluster-Registrierung mit Astra Control Center für applikationskonsistentes Datenmanagement erstellt Astra Control automatisch Rollenbindungen und einen NetApp Monitoring Namespace, mit dem Kennzahlen und Protokolle von den Applikations-Pods und den Worker-Nodes erfasst werden. Nutzen Sie als Standard eine der unterstützten ONTAP-basierten Storage-Klassen.

Nach Ihnen "Fügen Sie dem Astra Control Management einen Cluster hinzu", Sie können Apps auf dem Cluster installieren (außerhalb von Astra Control) und dann auf der Seite Apps in Astra Control die Apps und ihre Ressourcen verwalten. Weitere Informationen zum Verwalten von Apps mit Astra finden Sie im "Anforderungen für das Applikationsmanagement".

"Weiter: Übersicht zur Lösungsvalidierung"

Lösungsvalidierung

Überblick

"Früher: Astra Control Center Installation auf OpenShift Container Platform."

In diesem Abschnitt kommen wir nochmals auf die Lösung zurück. Einige Anwendungsfälle:

- Wiederherstellung einer statusorientierten Anwendung aus einem Remote-Backup in ein anderes OpenShift-Cluster, das in der Cloud ausgeführt wird.
- Eine zustandsorientierte Anwendung wird in demselben Namespace im OpenShift-Cluster wiederhergestellt.
- Applikationsmobilität durch Klonen von einem FlexPod System (OpenShift Container Platform Bare Metal) auf ein anderes FlexPod-System (OpenShift Container Platform auf VMware)

Insbesondere sind in dieser Lösung nur einige Anwendungsfälle validiert. Diese Validierung stellt in keiner Weise die gesamte Funktionalität des Astra Control Centers dar.

"Im nächsten Schritt: Applikations-Recovery mit Remote-Backups."

Applikations-Recovery mit Remote-Backups

"Zurück: Übersicht zur Lösungsvalidierung"

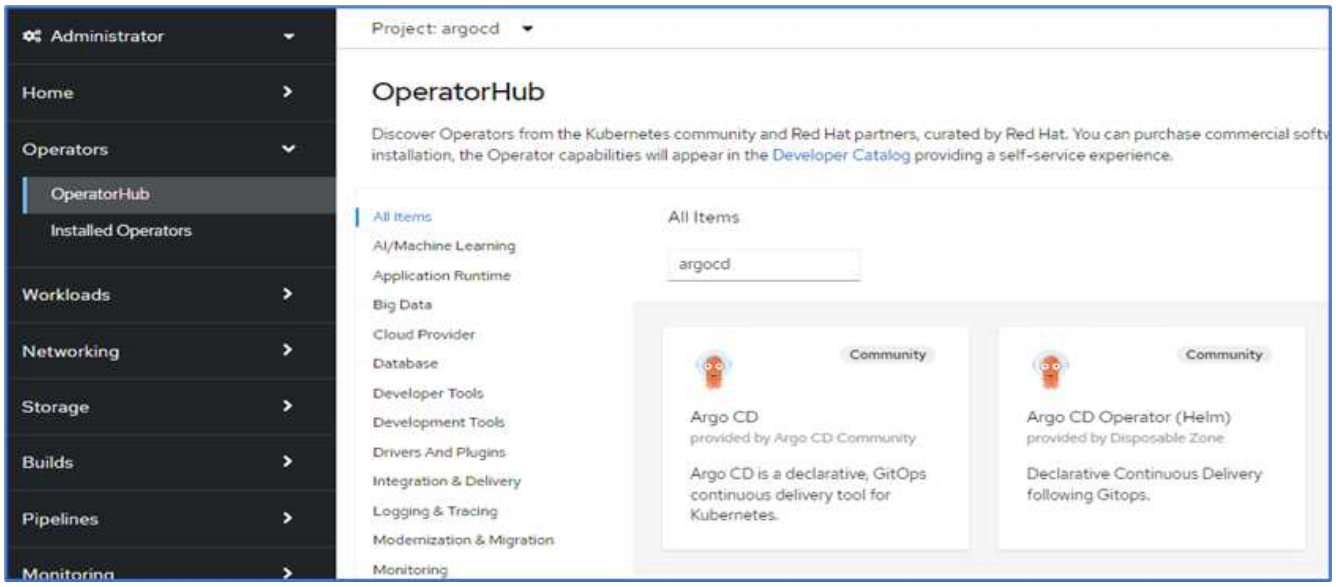
Mit Astra können Sie ein vollständiges und applikationskonsistentes Backup erstellen, mit dem Ihre Applikation ihre Daten auf einem anderen Kubernetes-Cluster wiederherstellen kann, der in einem On-Premises-Datacenter oder in einer Public Cloud ausgeführt wird.

Um die erfolgreiche Wiederherstellung von Applikationen zu validieren, simulieren Sie einen lokalen Ausfall einer Applikation, die im FlexPod System ausgeführt wird, und stellen Sie die Applikation mithilfe eines Remote-Backups in einem K8s Cluster in der Cloud wieder her.

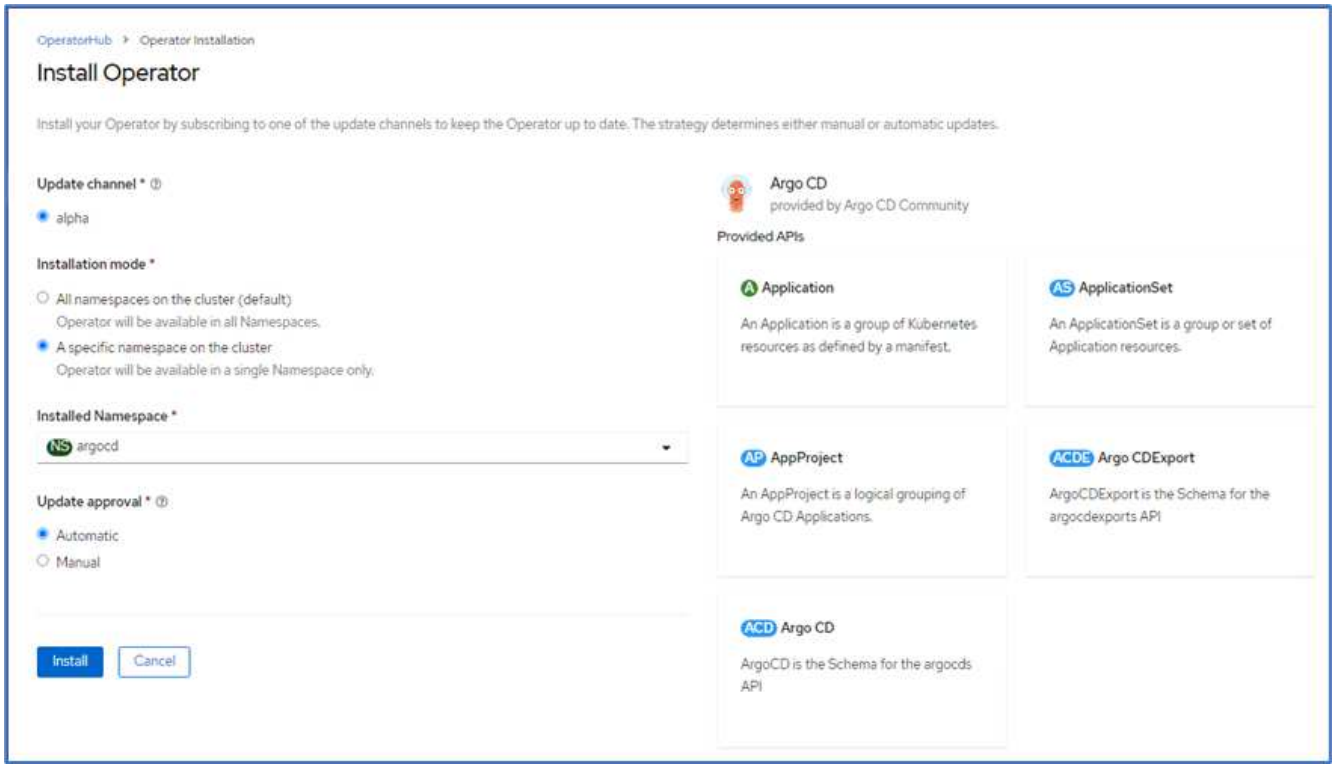
Die Beispielanwendung ist eine Anwendung der Preisliste, die MySQL für die Datenbank verwendet. Zur Automatisierung der Implementierung verwendeten wir das "Argo-CD" Werkzeug. Argo CD ist ein deklaratives GitOps, Continuous Delivery Tool für Kubernetes.

1. Melden Sie sich beim lokalen OpenShift-Cluster an, und erstellen Sie ein neues Projekt mit dem Namen `argocd`.

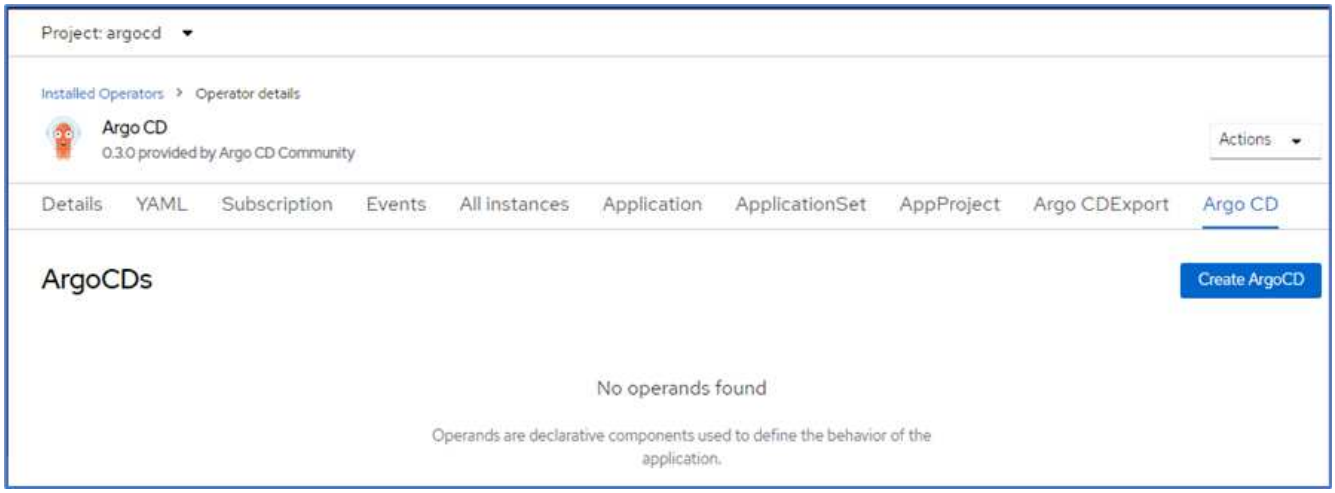
2. Suchen Sie im OperatorHub nach `argocd` Und wählen Sie Argo CD Operator.



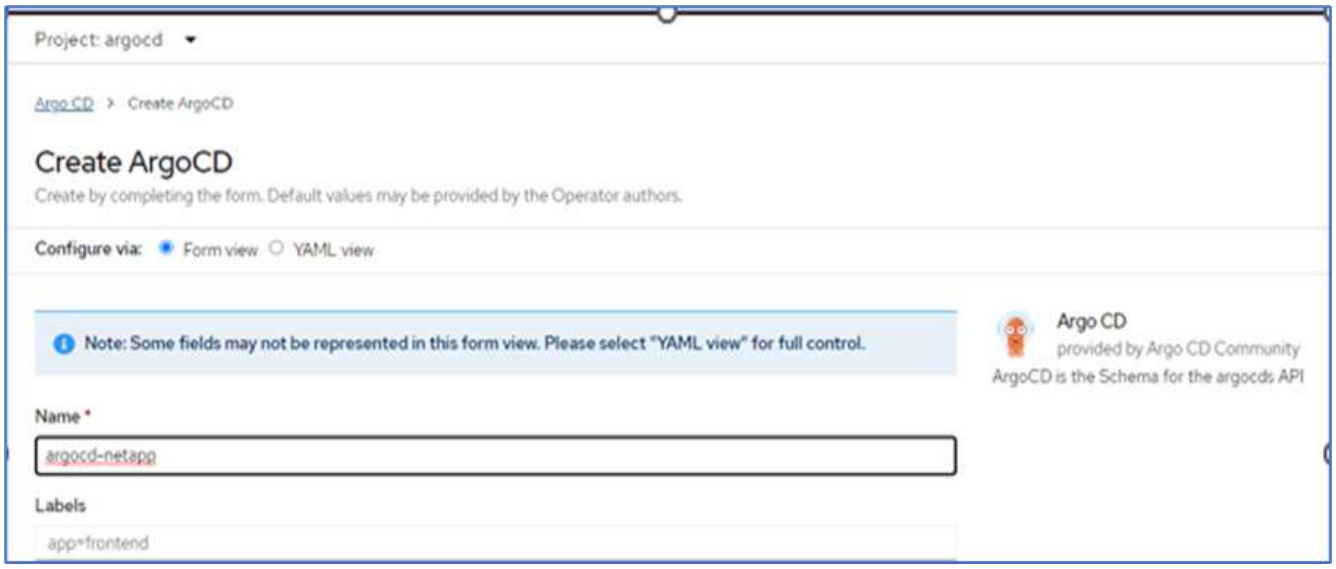
3. Installieren Sie den Operator in das `argocd` Namespace.



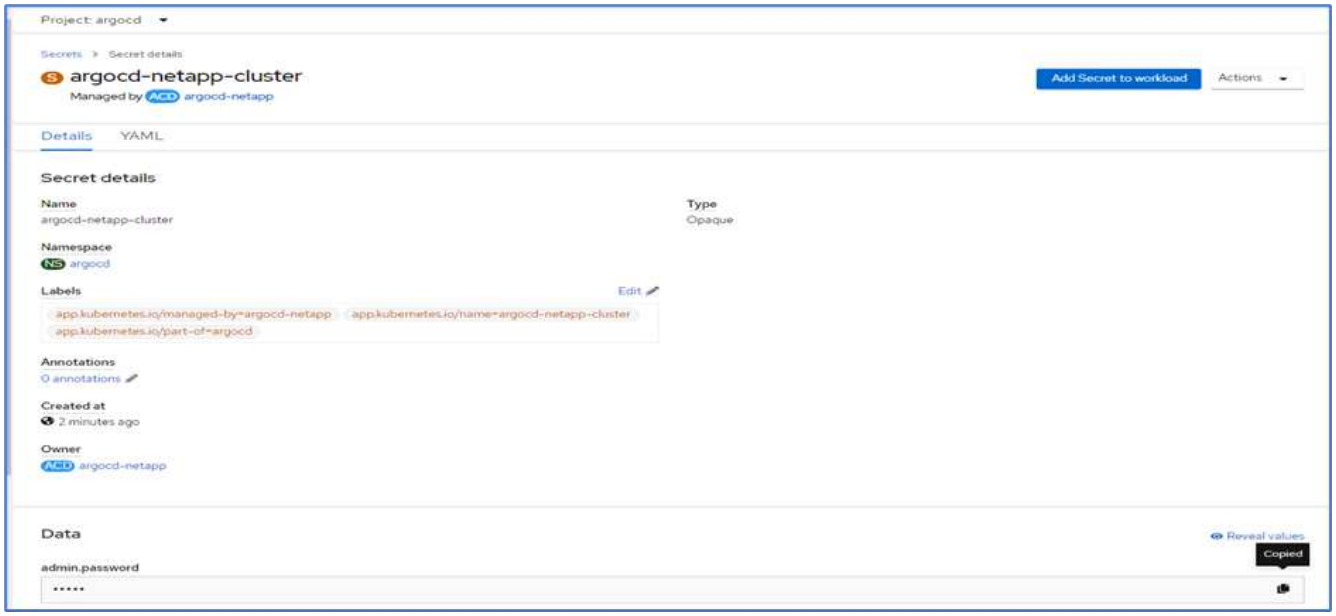
4. Gehen Sie zum Operator und klicken Sie auf ArgoCD erstellen.



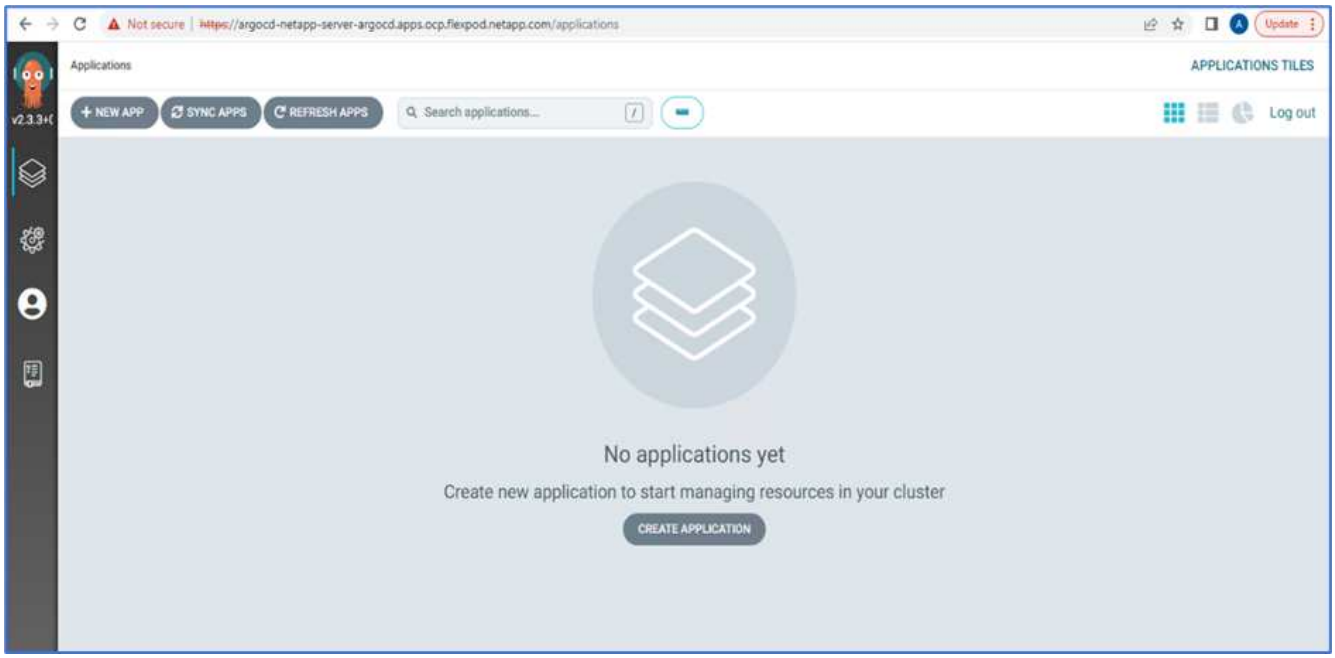
5. So stellen Sie die Argo-CD-Instanz im bereit `argocd` Geben Sie einen Namen ein, und klicken Sie auf Erstellen.



6. Um sich bei Argo CD anzumelden, ist der Standardbenutzer admin und das Passwort befindet sich in einer geheimen Datei mit dem Namen `argocd-netapp-cluster`.



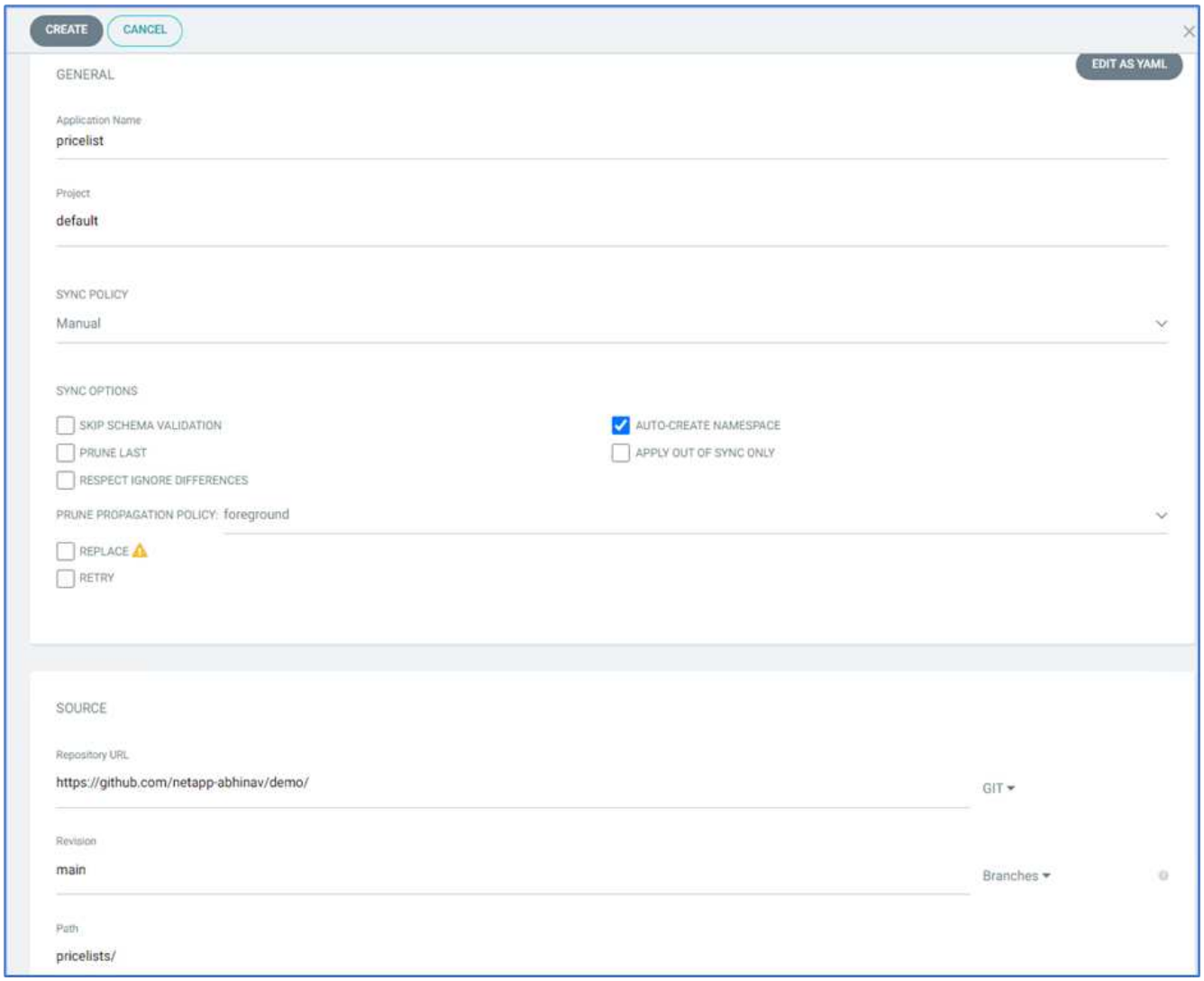
7. Wählen Sie im Seitenmenü Routen > Standort aus, und klicken Sie auf die URL für das `argocd` Routen. Geben Sie den Benutzernamen und das Kennwort ein.



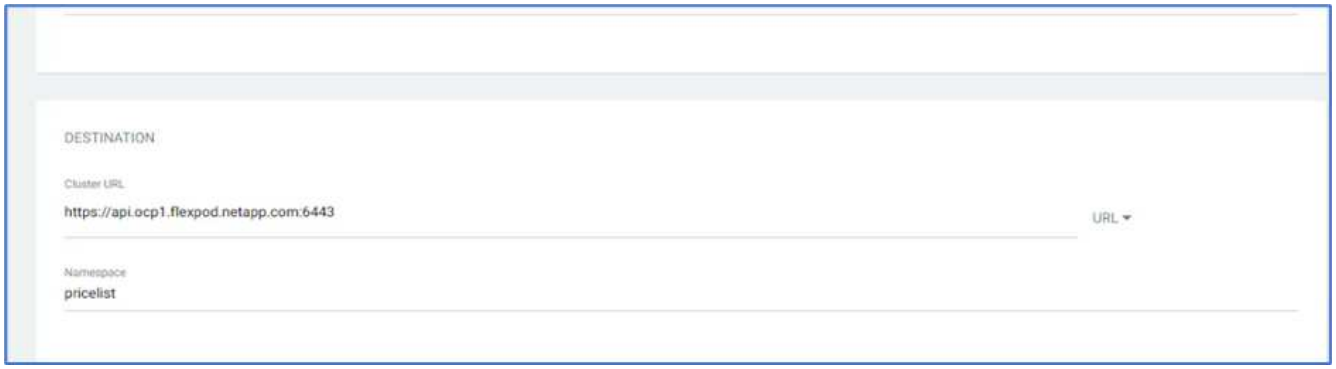
8. Fügen Sie den lokalen OpenShift-Cluster über die CLI zur Argo-CD hinzu.

```
####Login to Argo CD####
abhinav3@abhinav-ansible$ argocd-linux-amd64 login argocd-netapp-server-
argocd.apps.ocp.flexpod.netapp.com --insecure
Username: admin
Password:
'admin:login' logged in successfully
Context'argocd-netapp-server-argocd.apps.ocp.flexpod.netapp.com' updated
####List the On-Premises OpenShift cluster####
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add
ERRO[0000] Choose a context name from:
CURRENT  NAME
CLUSTER              SERVER
*        default/api-ocp-flexpod-netapp-com:6443/abhinav3
api-ocp-flexpod-netapp-com:6443
https://api.ocp.flexpod.netapp.com:6443
         default/api-ocp1-flexpod-netapp-com:6443/abhinav3
api-ocp1-flexpod-netapp-com:6443
https://api.ocp1.flexpod.netapp.com:6443
####Add On-Premises OpenShift cluster###
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add default/api-
ocp1-flexpod-netapp-com:6443/abhinav3
WARNING: This will create a service account `argocd-manager` on the
cluster referenced by context `default/api-ocp1-flexpod-netapp-
com:6443/abhinav3` with full cluster level admin privileges. Do you want
to continue [y/N]? y
INFO[0002] ServiceAccount "argocd-manager" already exists in namespace
"kube-system"
INFO[0002] ClusterRole "argocd-manager-role" updated
INFO[0002] ClusterRoleBinding "argocd-manager-role-binding" updated
Cluster 'https://api.ocp1.flexpod.netapp.com:6443' added
```

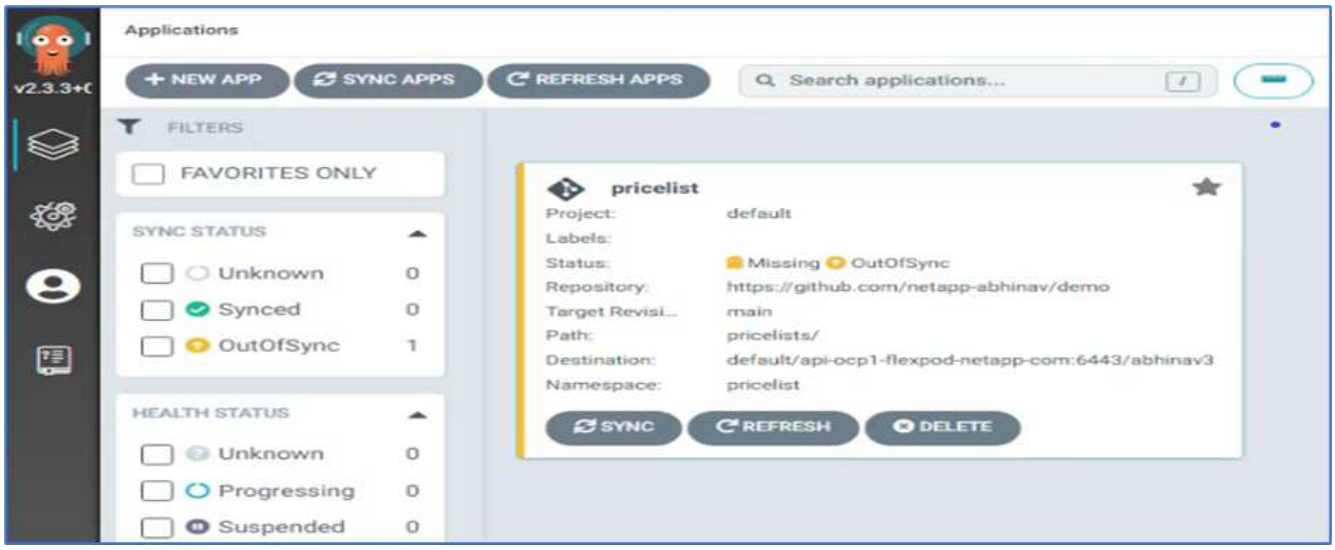
9. Klicken Sie in der ArgoCD-Benutzeroberfläche AUF DIE NEUE APP, und geben Sie die Details zum App-Namen und Code-Repository ein.



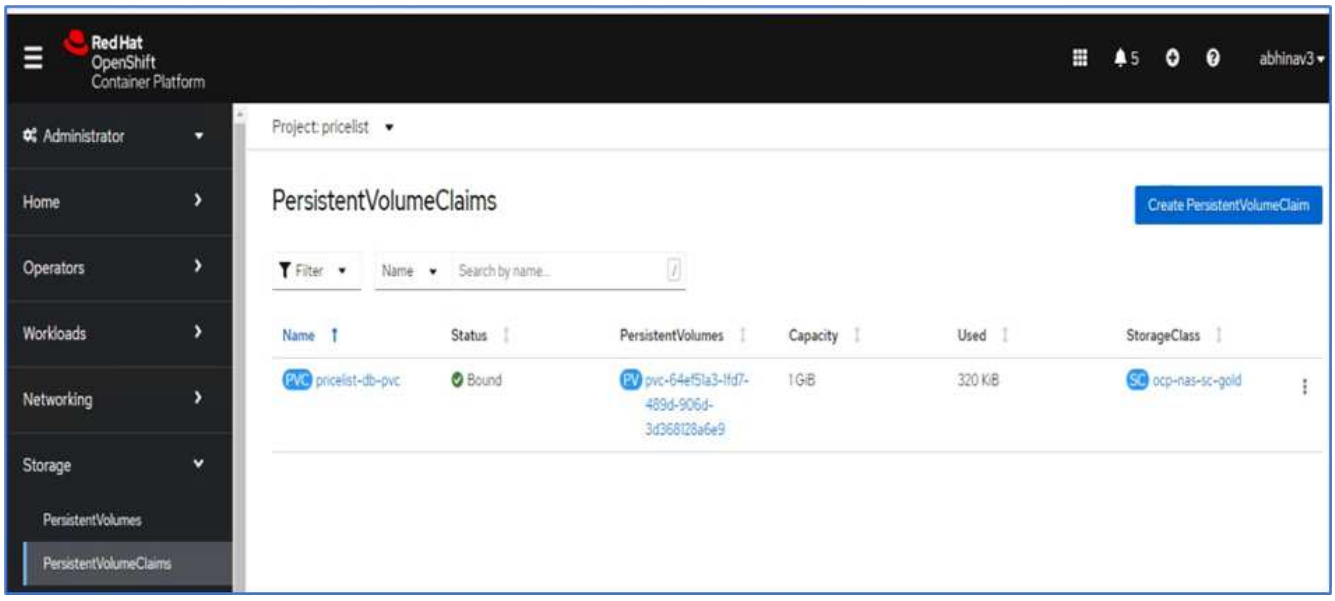
10. Geben Sie den OpenShift-Cluster ein, in dem die App zusammen mit dem Namespace bereitgestellt wird.



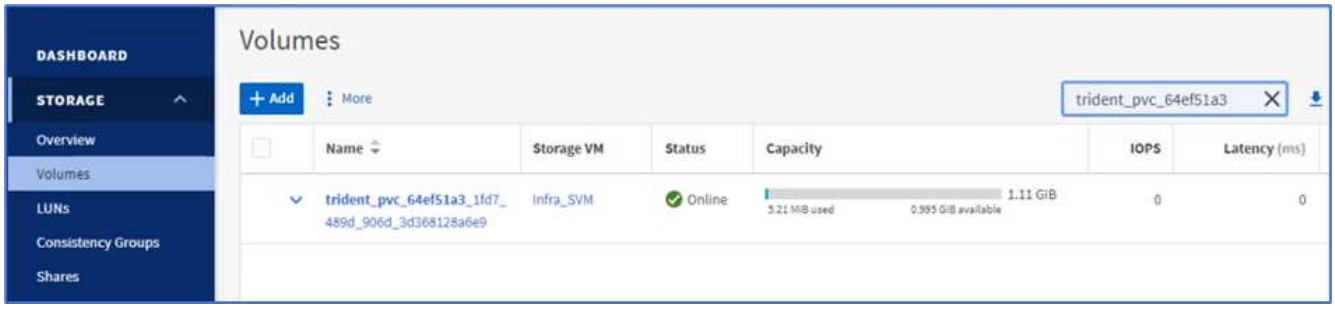
11. Klicken SIE ZUM Bereitstellen der App auf dem lokalen OpenShift-Cluster auf „SYNC“.



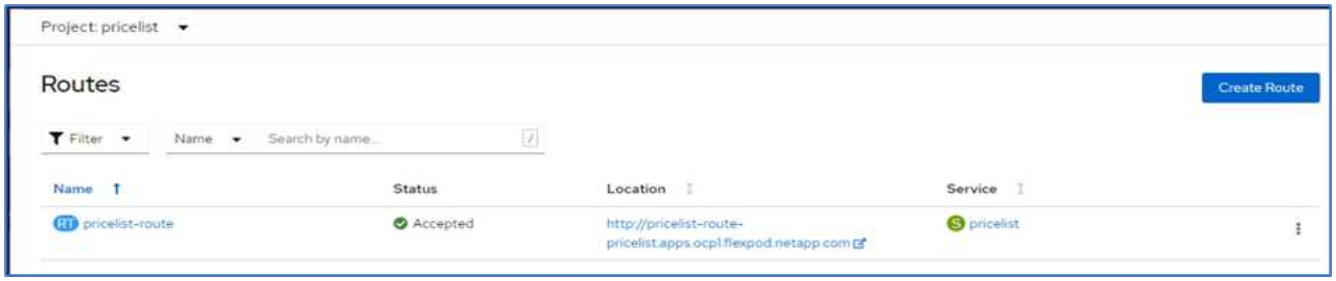
12. Wechseln Sie in der Konsole der OpenShift Container Platform zur Project Pricliste, und überprüfen Sie unter Storage den Namen und die Größe des PVC.



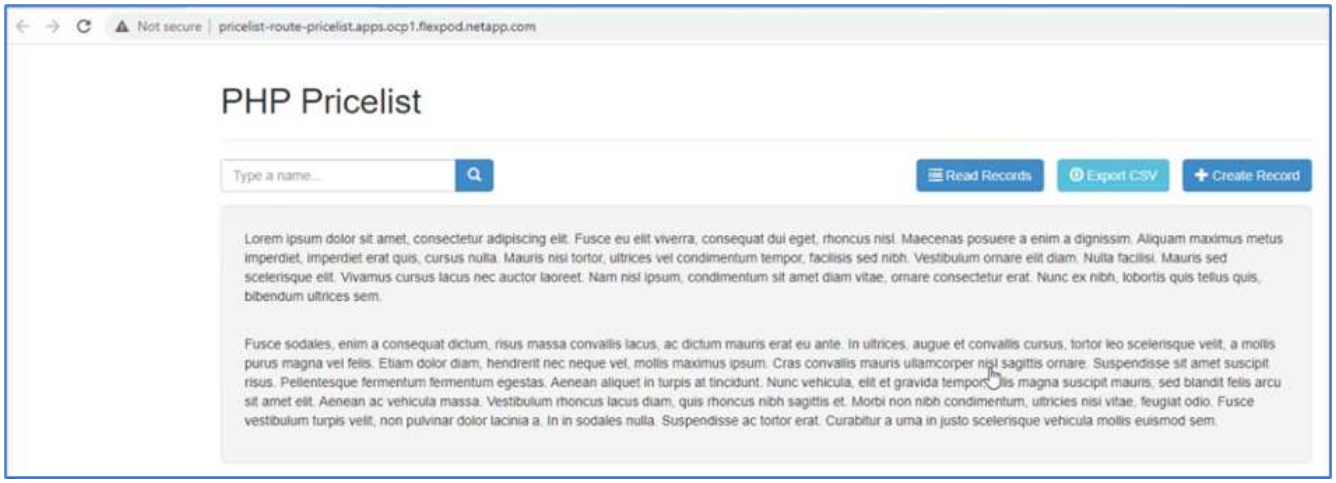
13. Melden Sie sich bei System Manager an und überprüfen Sie die PVC.



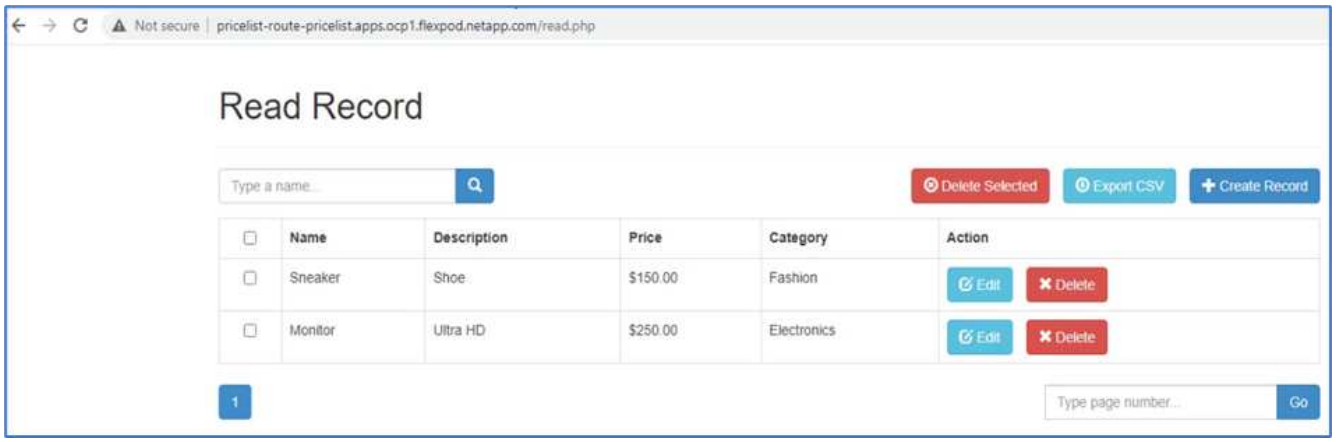
14. Wählen Sie nach dem Ausführen der Pods im Seitenmenü Netzwerk > Routen aus, und klicken Sie unter Speicherort auf die URL.



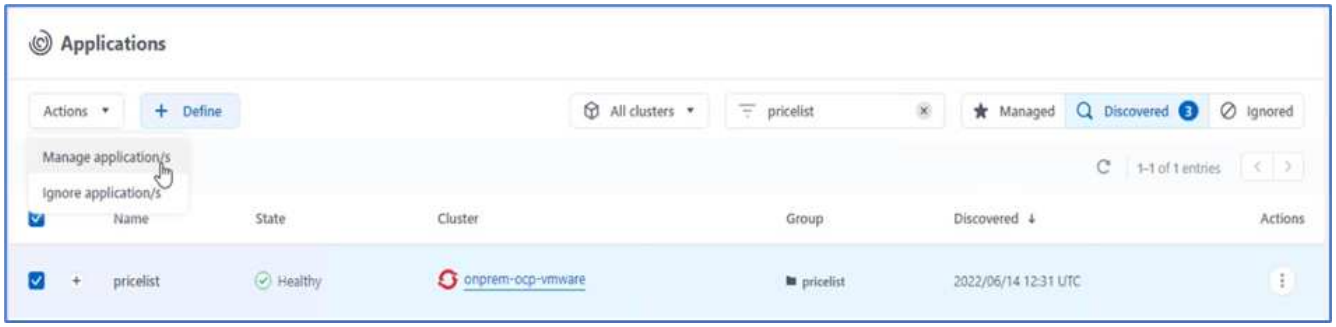
15. Die Homepage der Preisliste wird angezeigt.



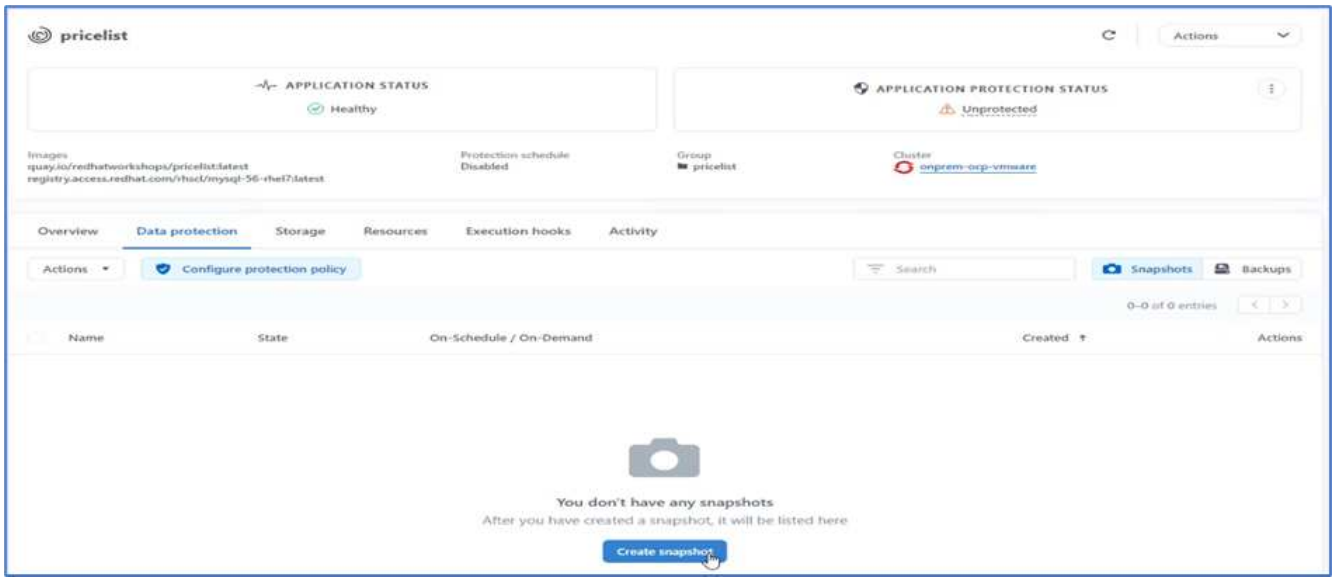
16. Erstellen Sie ein paar Datensätze auf der Webseite.



17. Die App wird im Astra Control Center entdeckt. Um die App zu verwalten, gehen Sie zu Anwendungen > entdeckt, wählen Sie die App Preisliste aus, und klicken Sie unter Aktionen auf Anwendungen verwalten.

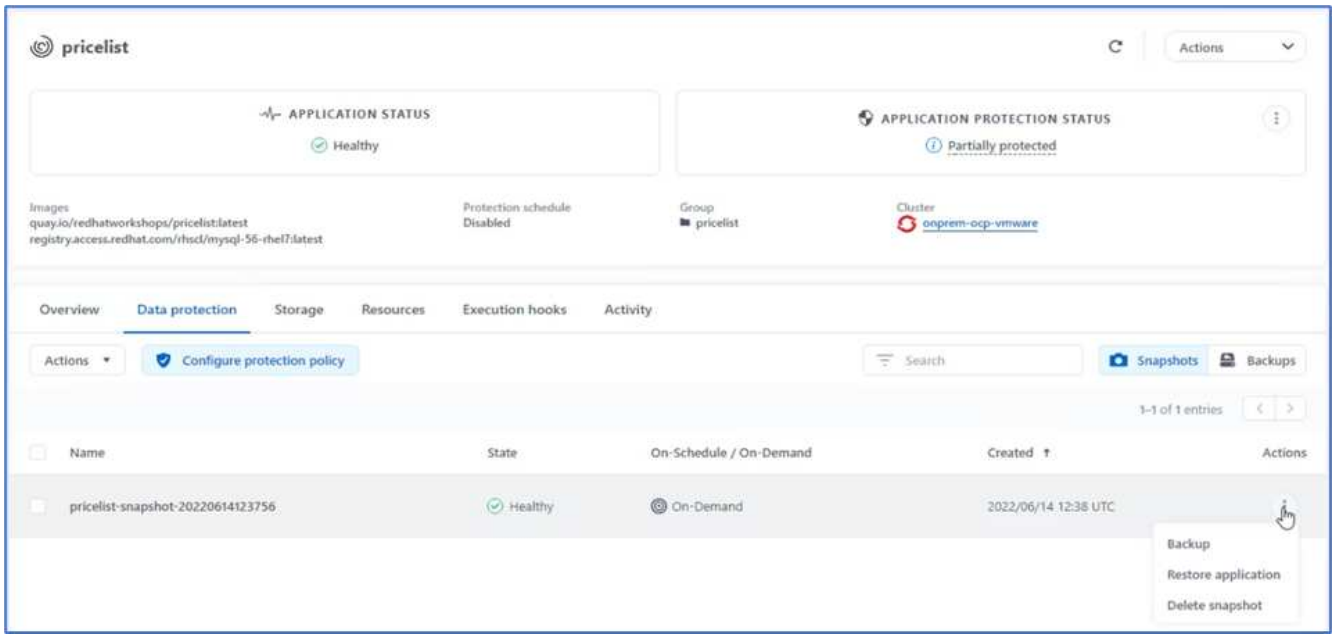


18. Klicken Sie auf die Preisliste-App und wählen Sie Datenschutz aus. Zu diesem Zeitpunkt sollten keine Snapshots oder Backups vorhanden sein. Klicken Sie auf Snapshot erstellen, um einen On-Demand-Snapshot zu erstellen.

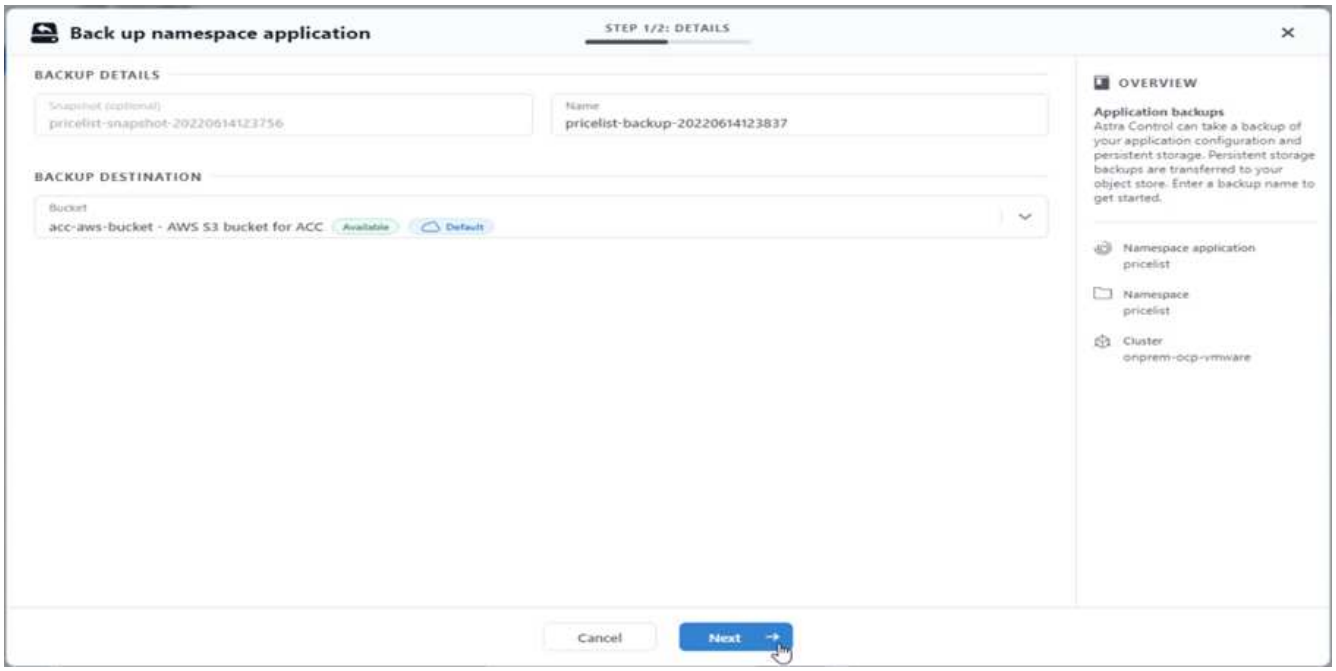


Das NetApp Astra Control Center unterstützt sowohl On-Demand als auch geplante Snapshots und Backups.

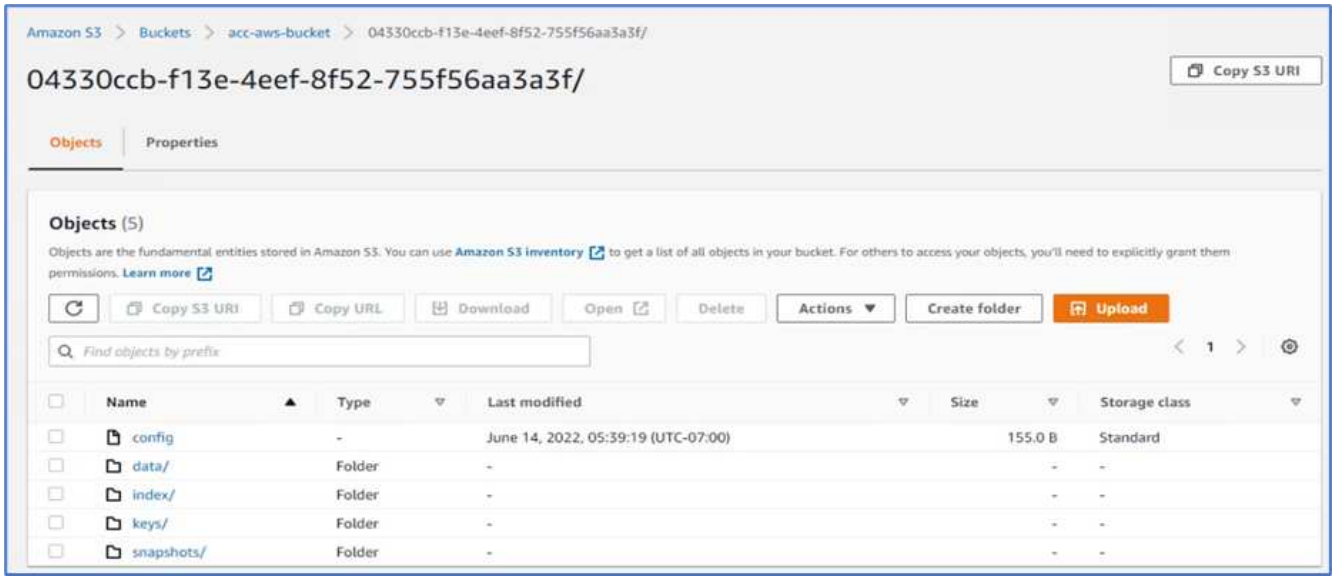
19. Nachdem der Snapshot erstellt wurde und der Status sich in einem ordnungsgemäßen Zustand befindet, erstellen Sie mithilfe dieses Snapshots eine Remote-Sicherung. Dieses Backup wird im S3-Bucket gespeichert.



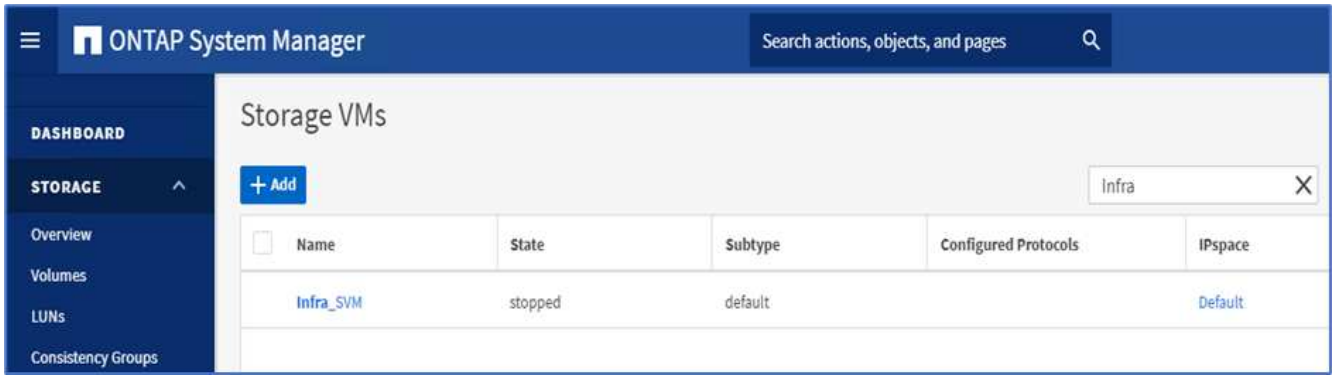
20. Wählen Sie den AWS S3-Bucket aus und initiieren Sie den Backup-Vorgang.



21. Der Backup-Vorgang sollte einen Ordner mit mehreren Objekten im AWS S3-Bucket erstellen.



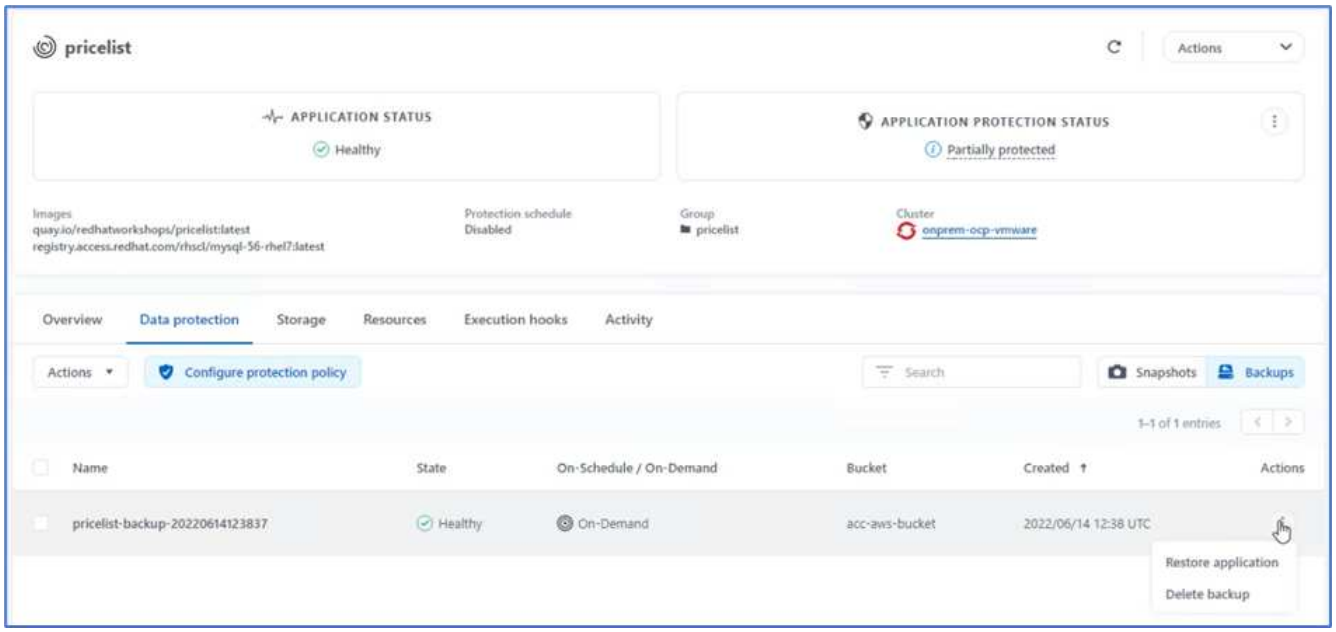
22. Nach Abschluss des Remote Backups simulieren Sie eine Katastrophe im lokalen Datacenter, indem Sie die Storage Virtual Machine (SVM) stoppen, die das zugrunde liegende Volume für das PV hostet.



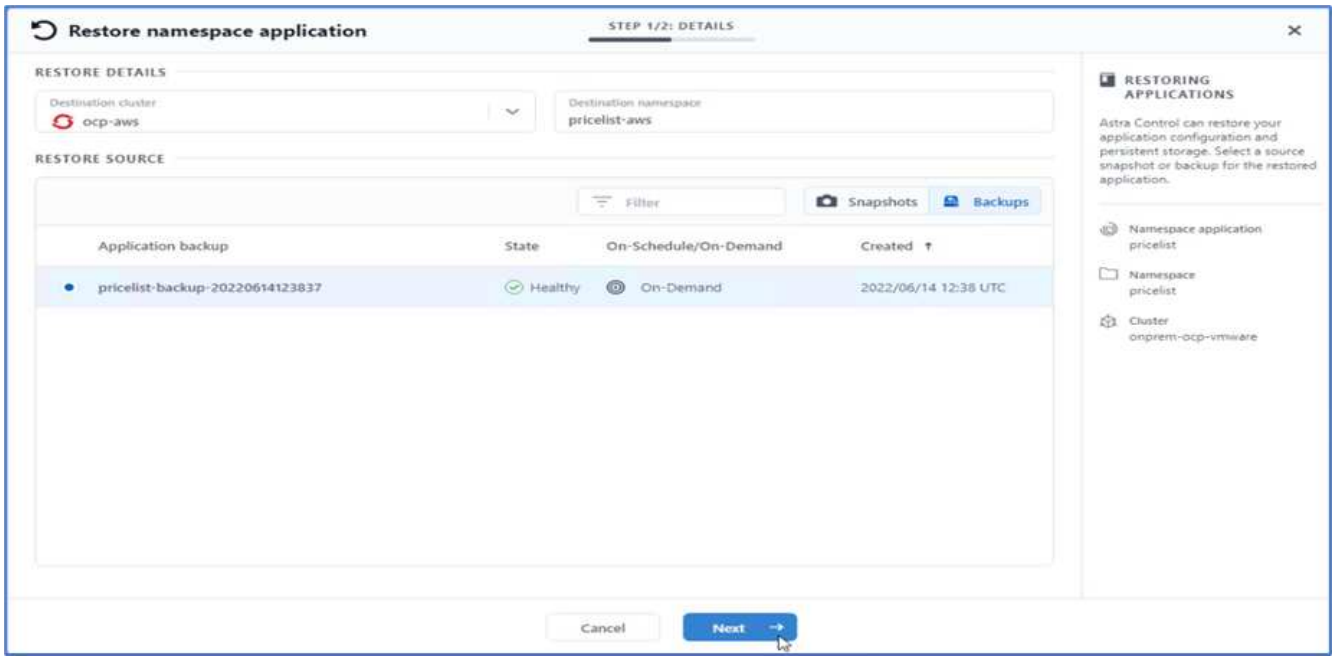
23. Aktualisieren Sie die Website, um den Ausfall zu bestätigen. Die Webseite ist nicht verfügbar.

Wie erwartet, ist die Website ausgefallen, so lassen Sie uns schnell die App vom Remote-Backup wiederherstellen, indem Sie Astra auf den OpenShift-Cluster in AWS ausführen.

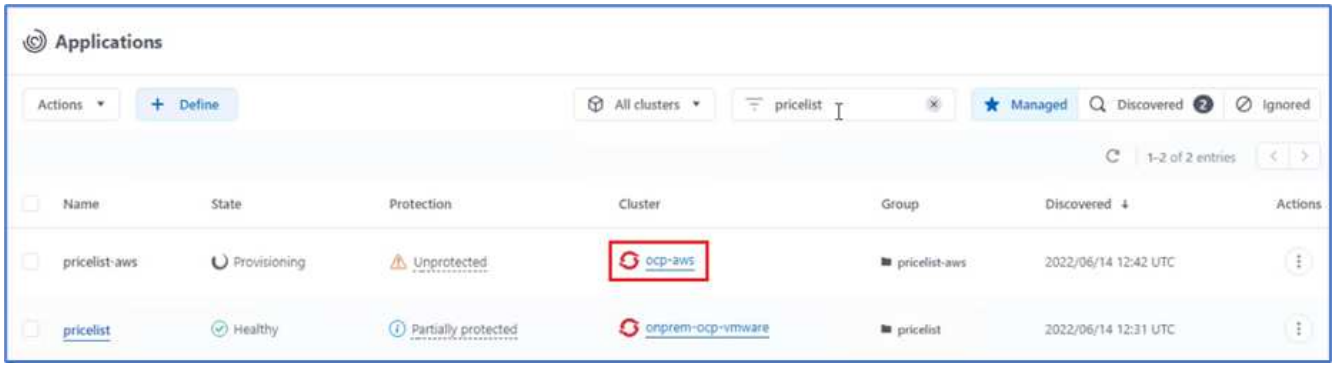
24. Klicken Sie im Astra Control Center auf die Preisliste und wählen Sie Datensicherheit > Backups. Wählen Sie das Backup aus, und klicken Sie unter Aktion auf Anwendung wiederherstellen.



25. Wählen Sie `ocp-aws` Als Ziel-Cluster und geben Sie dem Namespace einen Namen. Klicken Sie auf das On-Demand-Backup, Next und dann auf Restore.

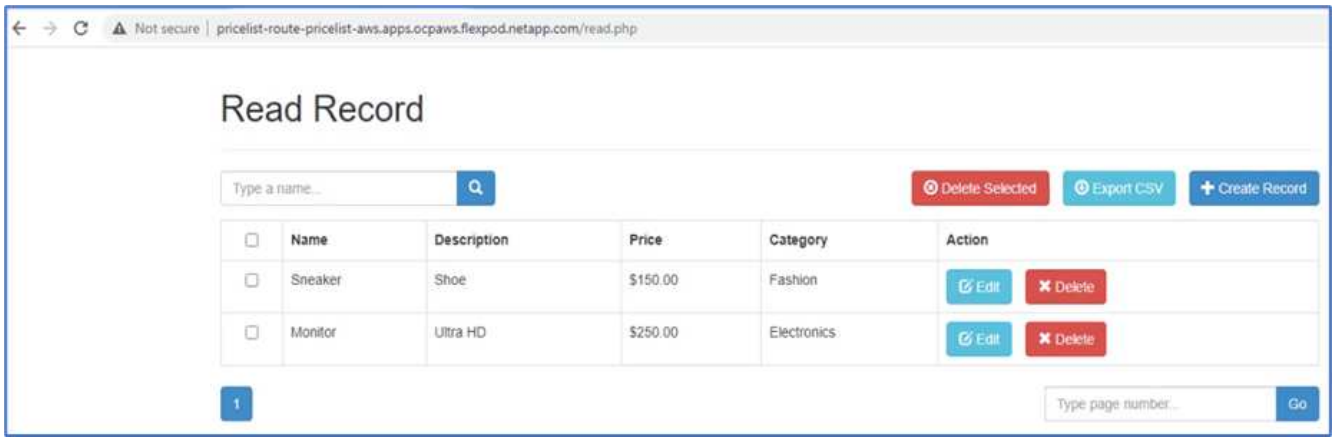


26. Eine neue App mit dem Namen `pricelist-app` Wird auf dem OpenShift-Cluster in AWS beschrieben.



27. Überprüfen Sie das gleiche in der OpenShift Webkonsole.

28. Nach allen Stativen unter dem `pricelist-aws` Projekt läuft, gehen Sie zu Routen und klicken Sie auf die URL, um die Webseite zu starten.



Dieser Prozess bestätigt, dass die Anwendung der Preisliste erfolgreich wiederhergestellt wurde und dass die Datenintegrität auf dem OpenShift-Cluster, das nahtlos auf AWS ausgeführt wird, mit Hilfe des Astra Control Center sichergestellt ist.

Datensicherung mit Snapshot Kopien und Applikationsmobilität für DevTest

Dieser Anwendungsfall besteht aus zwei Teilen, wie in den folgenden Abschnitten beschrieben.

Teil 1

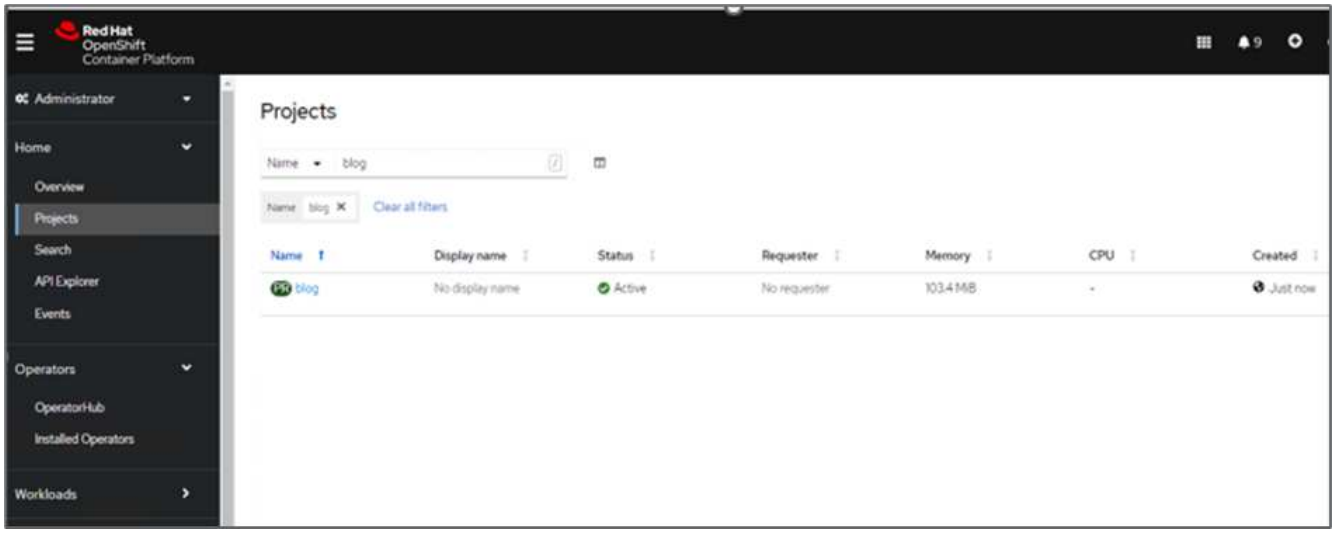
Mit Astra Control Center können Sie applikationsgerechte Snapshots für die lokale Datensicherung erstellen. Wenn Sie Ihre Daten versehentlich löschen oder beschädigt haben, können Sie Ihre Anwendungen und zugehörigen Daten mithilfe eines zuvor aufgenommenen Snapshots in einen bekannten fehlerfreien Zustand zurücksetzen.

In diesem Szenario implementiert ein Entwicklungs- und Testteam (DevTest) eine Beispielanwendung mit Stateful (Blog-Site), die eine Ghost Blog-Anwendung ist, einige Inhalte hinzufügt und die App auf die neueste verfügbare Version aktualisiert. Die Ghost-Anwendung verwendet SQLite für die Datenbank. Vor dem Upgrade der Applikation wird ein Snapshot (On-Demand) mit Astra Control Center zur Datensicherung erstellt. Die detaillierten Schritte lauten wie folgt:

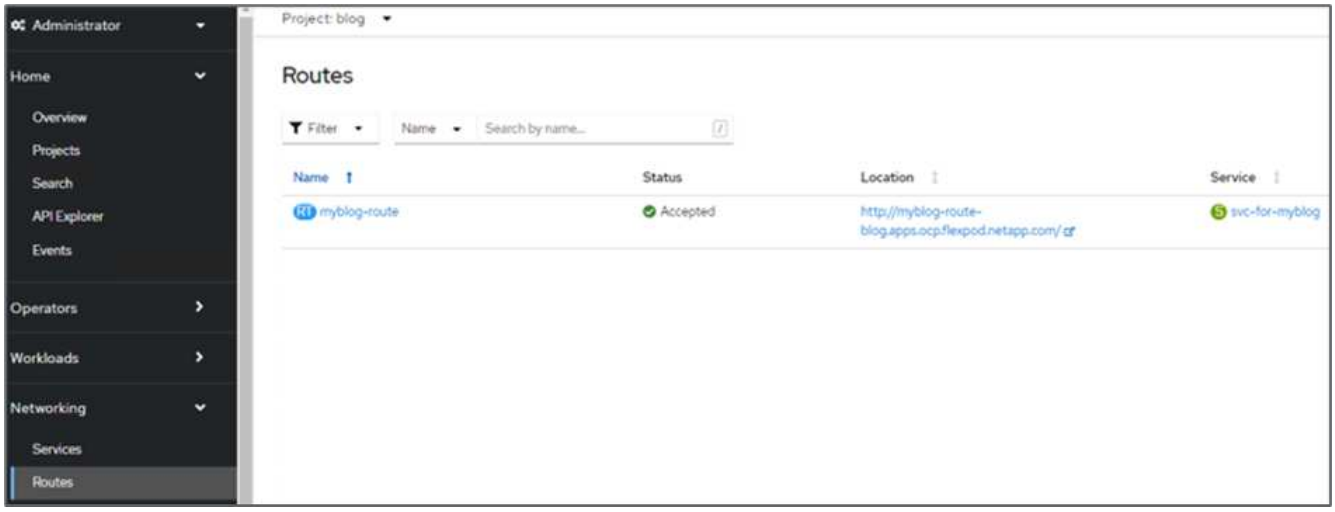
1. Stellen Sie die Beispiel-Blogging-App bereit und synchronisieren Sie sie von ArgoCD.

2. Melden Sie sich beim ersten OpenShift-Cluster an, gehen Sie zu Projekt, und geben Sie in der Suchleiste

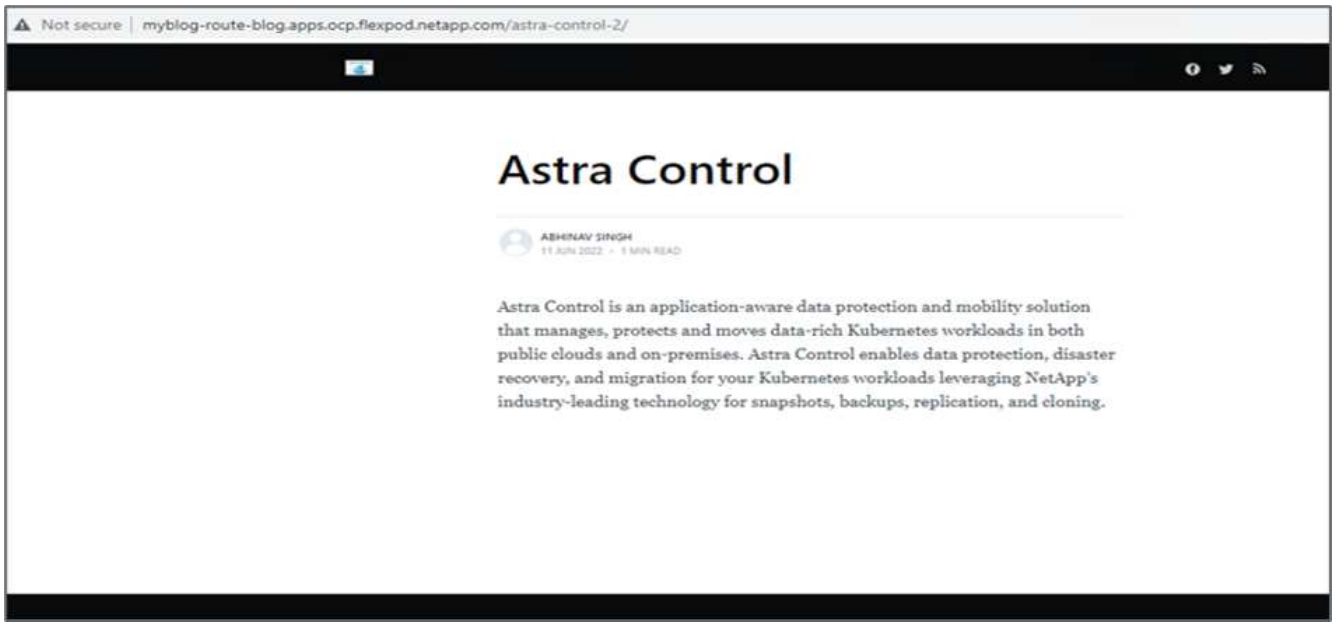
den Blog ein.



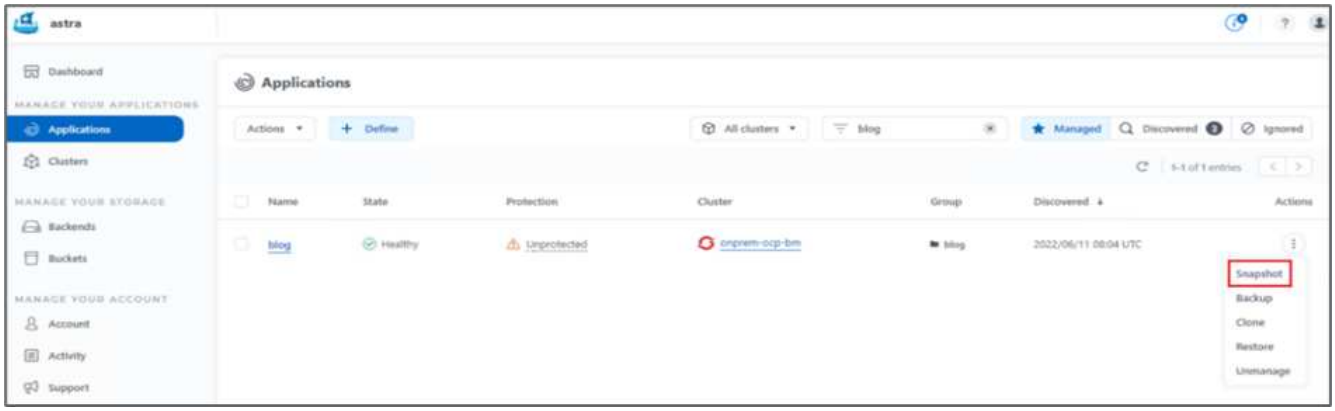
3. Wählen Sie im seitlichen Menü die Option Netzwerk > Routen, und klicken Sie auf die URL.



4. Die Blog-Startseite wird angezeigt. Fügen Sie einige Inhalte zur Blog-Site hinzu und veröffentlichen Sie sie.



5. Gehen Sie zum Astra Control Center. Managen Sie zuerst die Applikation über die Registerkarte „entdeckt“ und erstellen Sie dann eine Snapshot Kopie.

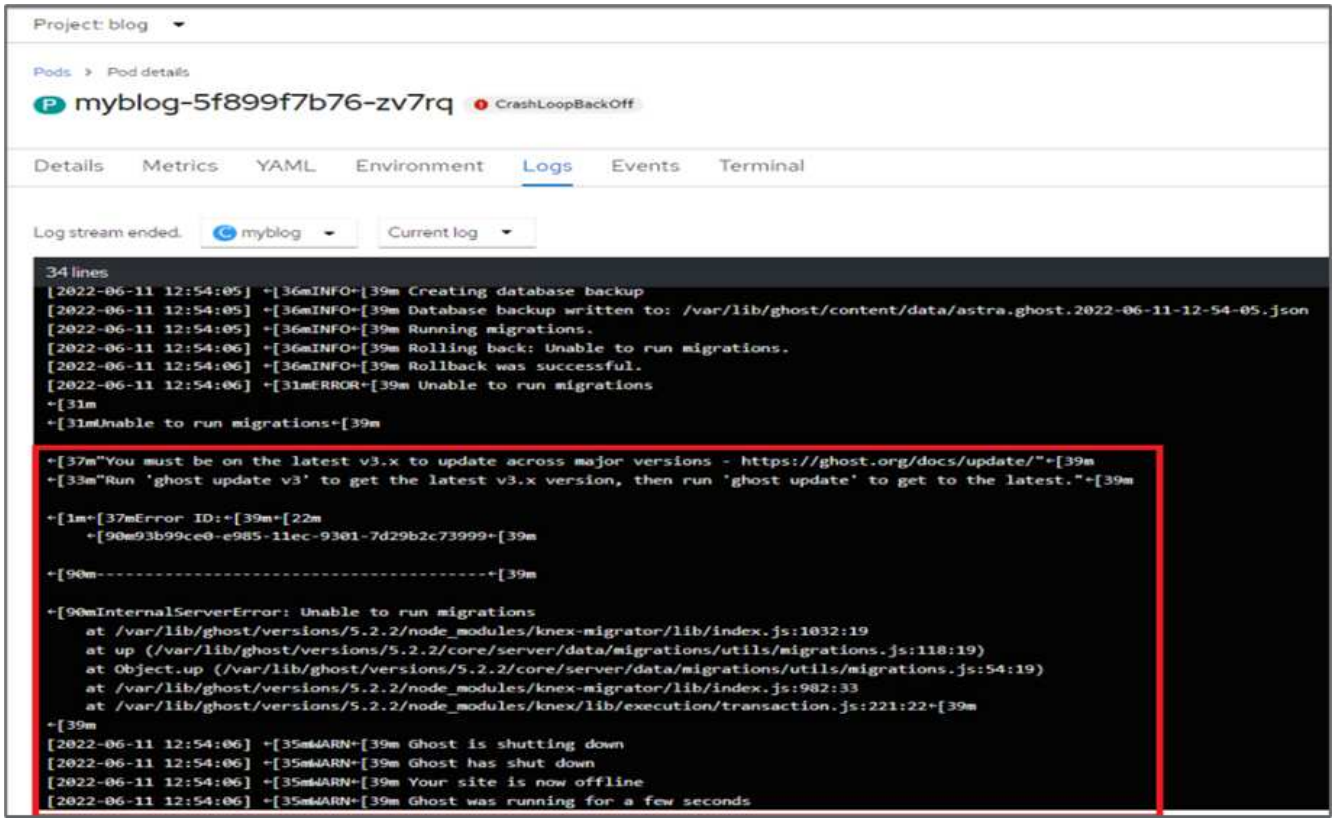


Sie können auch Ihre Applikationen schützen, indem Sie Snapshots, Backups oder beides nach einem definierten Zeitplan erstellen. Weitere Informationen finden Sie unter "Sichern von Applikationen durch Snapshots und Backups".

6. Nachdem der On-Demand-Snapshot erfolgreich erstellt wurde, aktualisieren Sie die App auf die neueste Version. Die aktuelle Bildversion ist `ghost: 3.6-alpine` Und die Zielversion lautet `ghost:latest`. Um die App zu aktualisieren, nehmen Sie die Änderungen direkt am Git-Repository vor und synchronisieren Sie sie auf Argo-CD.

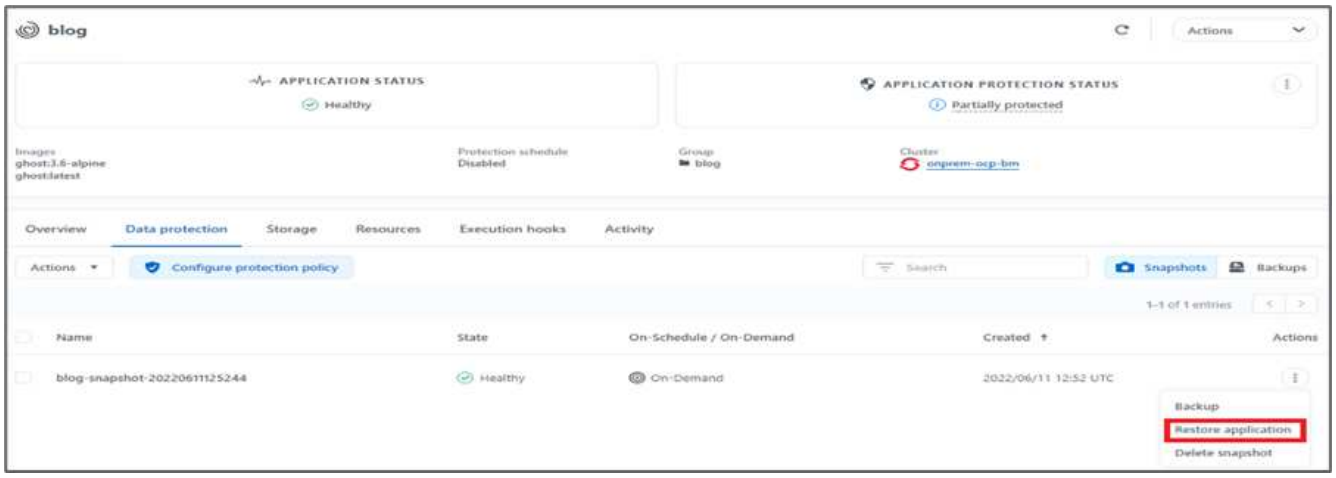
```
spec:
  containers:
  - name: myblog
    image: ghost:latest
    imagePullPolicy: Always
    ports:
    - containerPort: 2368
```

7. Sie können sehen, dass das direkte Upgrade auf die neueste Version nicht unterstützt wird, weil die Blog-Site herunter ist und die gesamte Anwendung beschädigt wird.

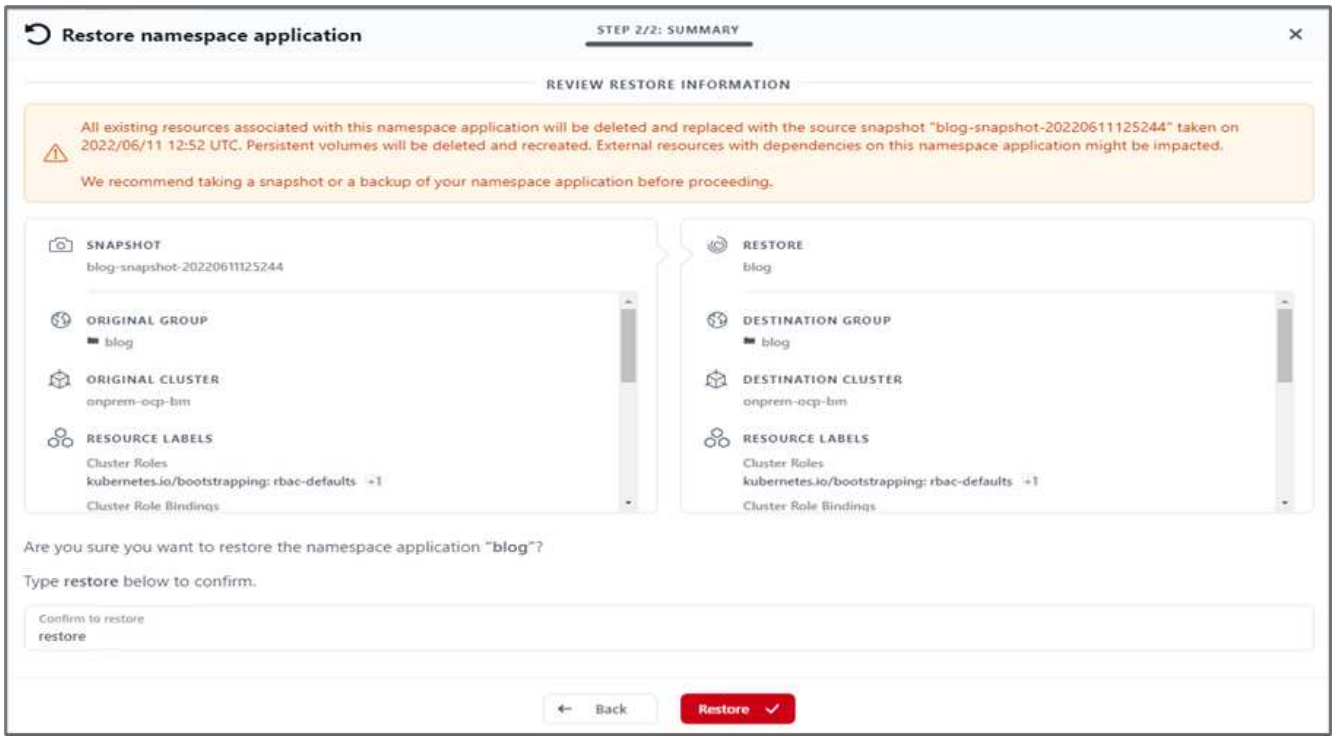


8. Aktualisieren Sie die URL, um die Nichtverfügbarkeit der Blog-Site zu bestätigen.

9. Die Anwendung aus dem Snapshot wiederherstellen.



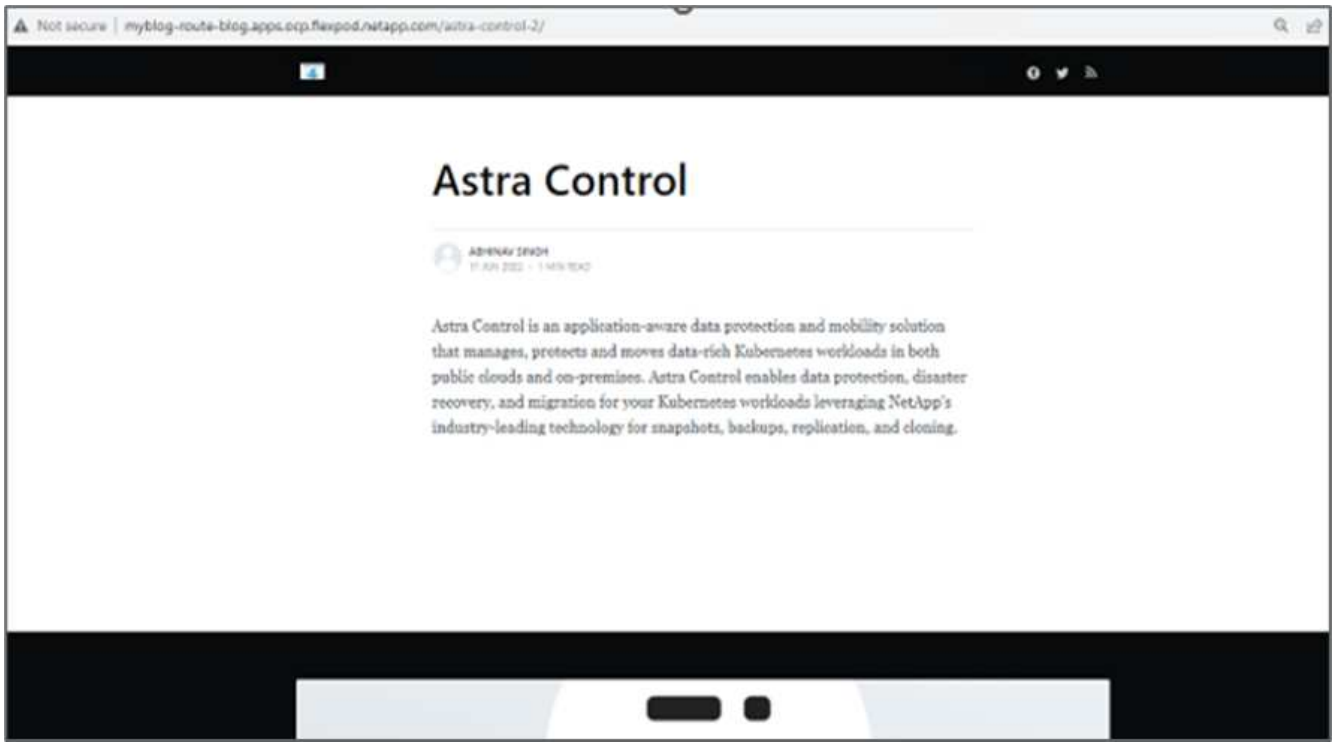
10. Die App wird auf demselben OpenShift-Cluster wiederhergestellt.



11. Die App-Wiederherstellung wird sofort gestartet.

12. In wenigen Minuten wird die App vom verfügbaren Snapshot erfolgreich wiederhergestellt.

13. Um zu sehen, ob die Webseite verfügbar ist, aktualisieren Sie die URL.

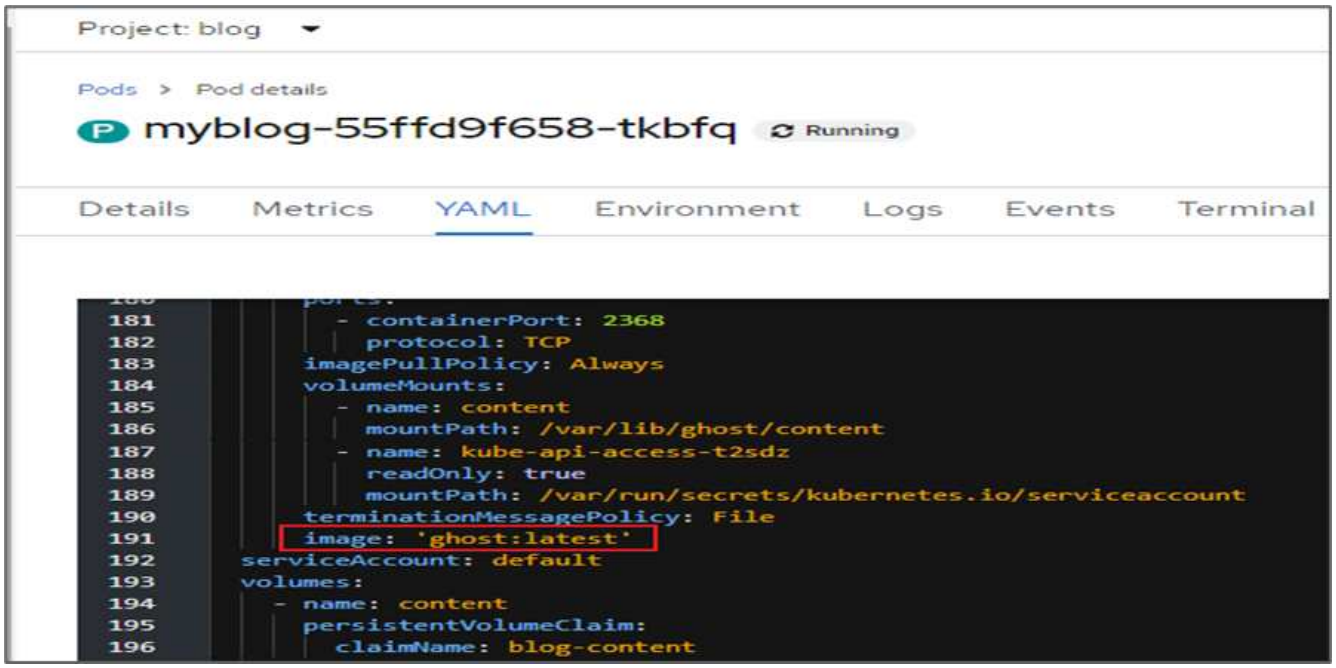


Mithilfe des Astra Control Center kann ein DevTest-Team mithilfe des Snapshots eine Blog-Site-App und die damit verbundenen Daten erfolgreich wiederherstellen.

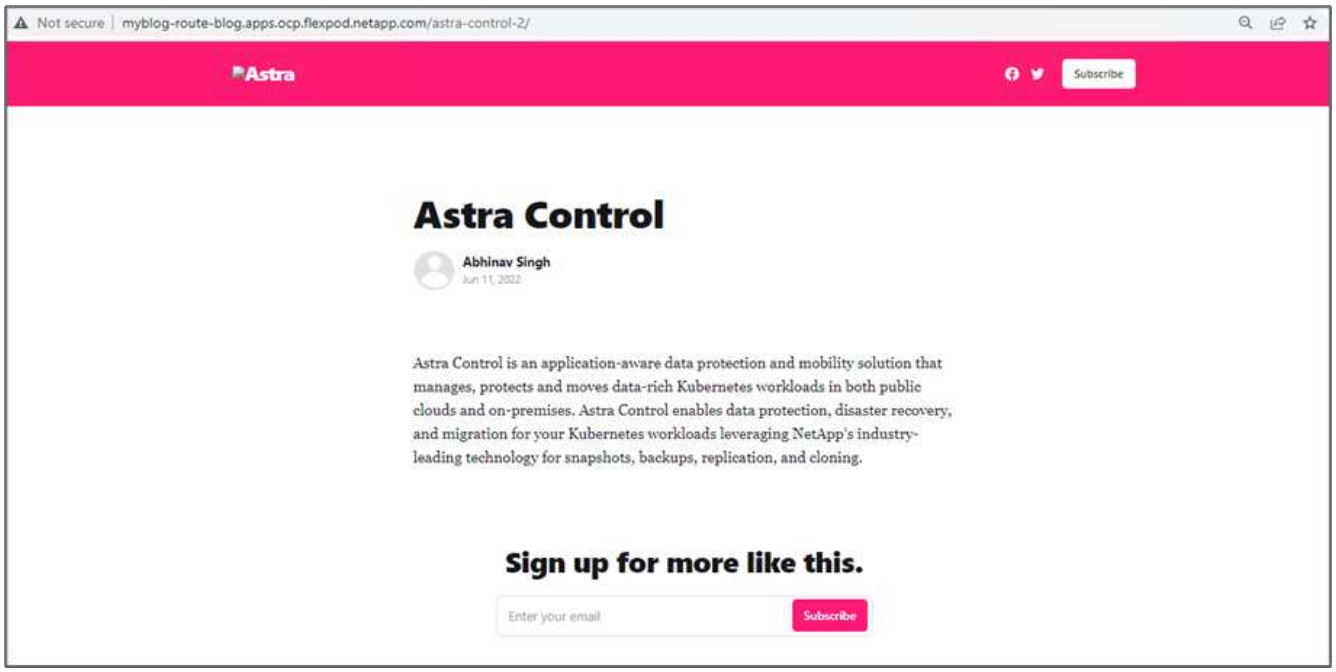
Teil 2

Mit Astra Control Center können Sie eine ganze Applikation zusammen mit den zugehörigen Daten von einem Kubernetes Cluster zu einem anderen verschieben, unabhängig davon, wo sich die Cluster befinden (lokal oder in der Cloud).

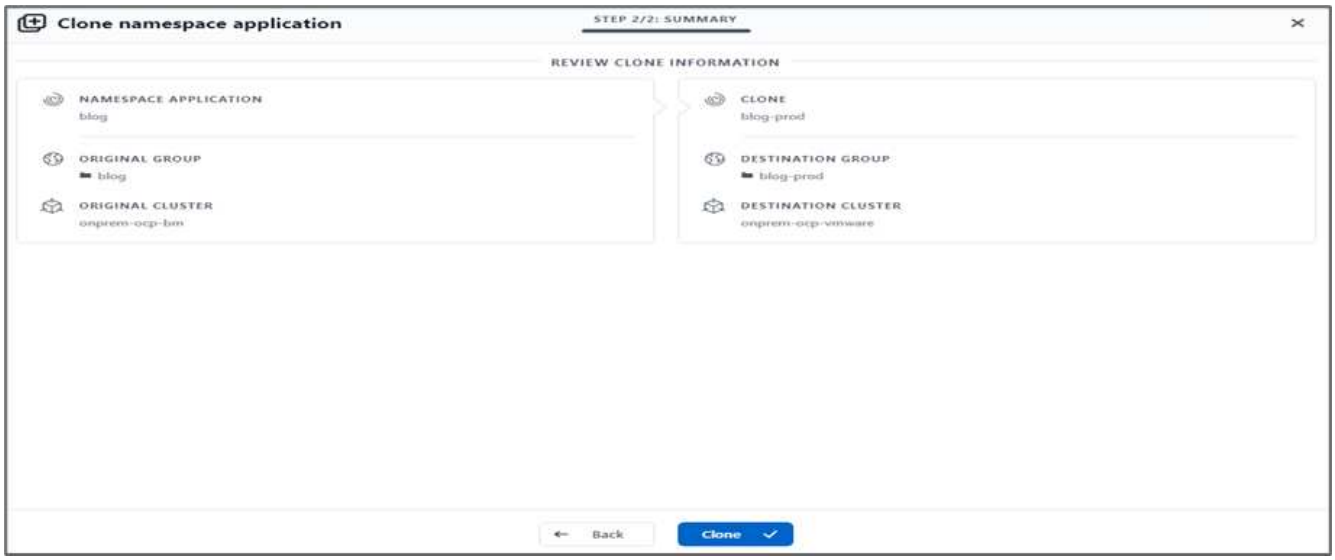
1. Das DevTest-Team aktualisiert zunächst die App auf die unterstützte Version (`ghost-4.6-alpine`) Vor dem Upgrade auf die endgültige Version (`ghost-latest`) Um die Produktion bereit zu machen. Anschließend wird ein Upgrade der App veröffentlicht, die in den OpenShift-Cluster in der Produktion geklont wird, der auf einem anderen FlexPod-System ausgeführt wird.
2. An diesem Punkt wird die Applikation auf die neueste Version aktualisiert und kann im Produktions-Cluster geklont werden.



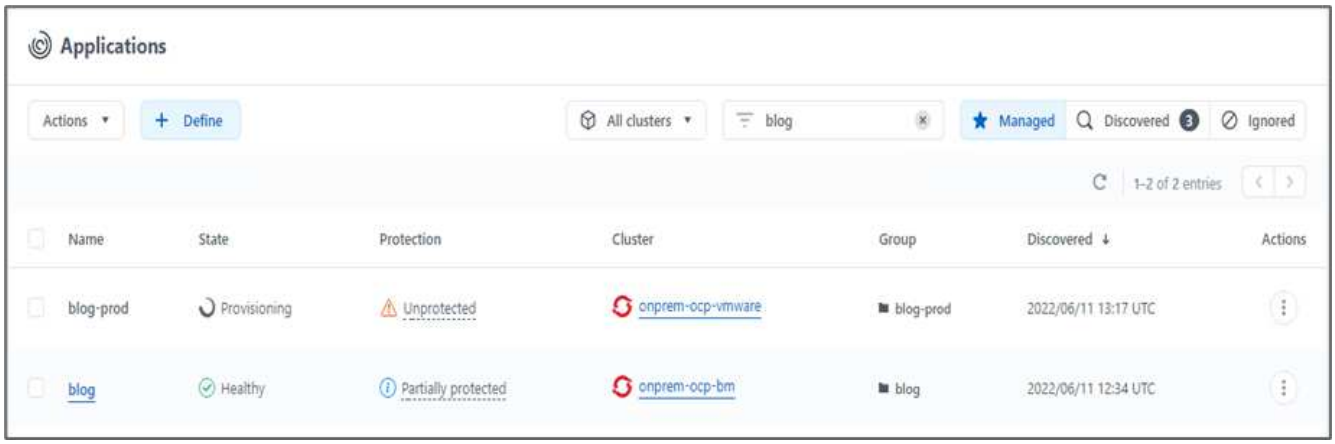
3. Um das neue Thema zu überprüfen, aktualisieren Sie die Blog-Site.



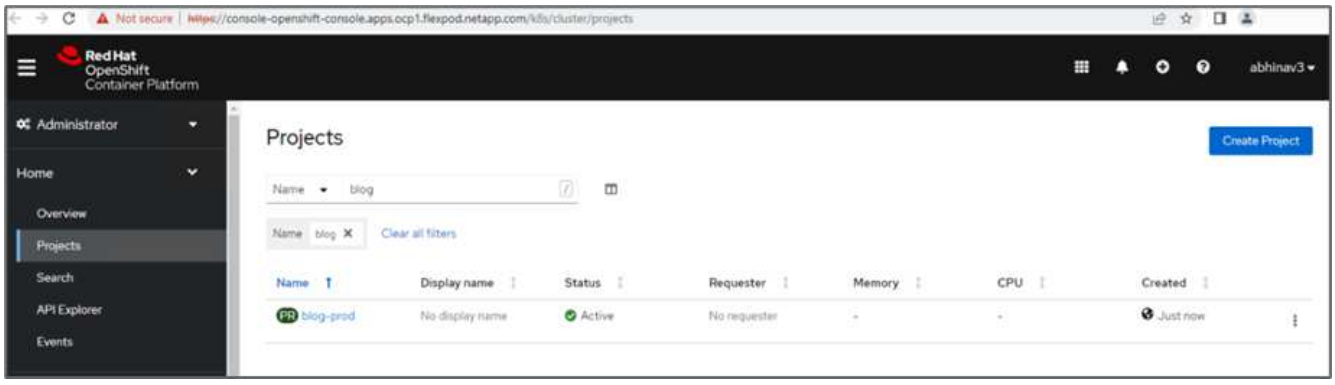
4. Vom Astra Control Center können Sie die App auf den anderen OpenShift-Cluster in der Produktion klonen, der auf VMware vSphere ausgeführt wird.



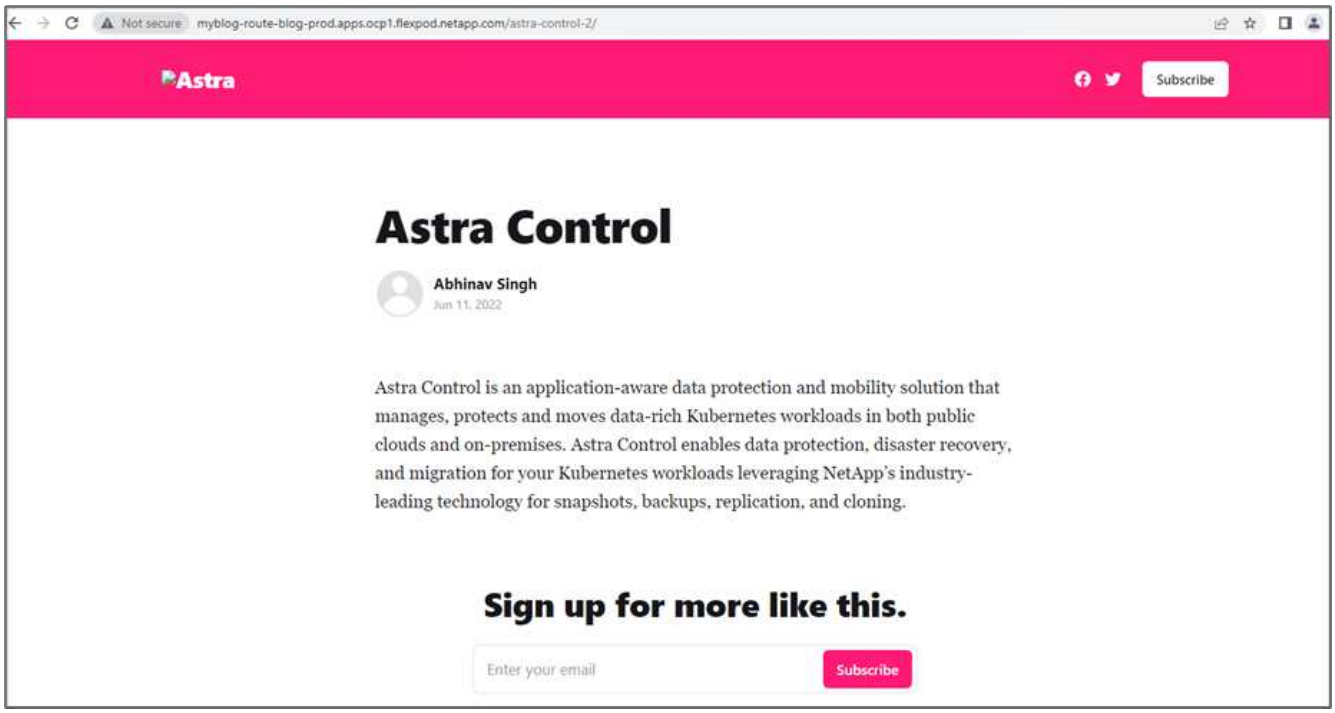
Im OpenShift-Cluster in der Produktion wird nun ein neuer Applikationsklon bereitgestellt.



5. Melden Sie sich im Cluster Production OpenShift an und suchen Sie den Projektblog.



6. Wählen Sie im seitlichen Menü die Option Netzwerk > Routen, und klicken Sie auf die URL unter Ort. Es wird dieselbe Homepage mit dem Inhalt angezeigt.



Damit ist die Validierung der Astra Control Center-Lösung abgeschlossen. Unabhängig von der Position des Kubernetes Clusters können Sie nun eine gesamte Applikation mit ihren Daten von einem Kubernetes Cluster zu einem anderen klonen.

"Weiter: Fazit."

Schlussfolgerung

"Früher: Applikations-Recovery mit Remote Backups."

Bei dieser Lösung haben wir mit dem NetApp Astra Portfolio einen Sicherungsplan für Container-Applikationen implementiert, die auf FlexPod und AWS ausgeführt werden. Die Kernkomponenten dieser Lösung bildeten das NetApp Astra Control Center, Astra Trident und die Cloud Volumes ONTAP, Red hat OpenShift und die FlexPod Infrastruktur.

Wir demonstrierten den Schutz von Applikationen, indem wir Snapshots erfassen, und wir haben komplette Kopien erstellt, um Applikationen über verschiedene K8s Cluster wiederherzustellen, die in Cloud- und lokalen Umgebungen ausgeführt werden.

Wir haben auch das Klonen von Anwendungen über K8s-Cluster hinweg demonstriert, wodurch Kunden ihre Apps auf K8s-Cluster ihrer Wahl an den gewünschten Standorten migrieren können.

FlexPod hat sich ständig weiterentwickelt, sodass Kunden ihre Applikationen und Geschäftsprozesse modernisieren können. Mit dieser Lösung können Kunden von FlexPod zuversichtlich ihren BCDR-Plan für ihre Cloud-nativen Applikationen mit der Public Cloud als Standort für einen transienten oder Vollzeit-DR-Plan erstellen, wobei die Kosten der Lösung gering gehalten werden.

Mit Astra Control können Sie eine ganze Applikation samt den Daten von einem Kubernetes Cluster auf einen anderen verschieben, egal wo sich die Cluster befinden. Sie kann zudem die Implementierung, den Betrieb und die Sicherung Ihrer Cloud-nativen Applikationen beschleunigen.

Fehlerbehebung

Anleitungen zur Fehlerbehebung finden Sie im "Online-Dokumentation".

Wo Sie weitere Informationen finden

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"

- 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"

- FlexPod-Implementierung mit Infrastruktur als Code für VMware mithilfe von Ansible

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html#AnsibleAutomationWorkflowandSolutionDeployment"

- FlexPod-Implementierung mit Infrastruktur als Code für Red hat OpenShift Bare Metal mit Ansible

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_iac_redhat_openshift.html"

- Cisco UCS Hardware and Software Interoperability Tool

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Cisco Intersight – Datenblatt

  "https://intersight.com/help/saas/home"

- NetApp Astra-Dokumentation

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra Control Center

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra Trident

  "https://docs.netapp.com/us-en/trident/index.html"

- NetApp Cloud Manager

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- NetApp Cloud Volumes ONTAP

  "https://docs.netapp.com/us-en/occm/task_getting_started_aws.html"

- Red hat OpenShift

  "https://www.openshift.com/"

- NetApp Interoperabilitäts-Matrix-Tool

  "http://support.netapp.com/matrix/"

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	Juli 2022	Freigabe für ACC 22.04.0.

NetApp Cloud Insights für FlexPod

TR-4868: NetApp Cloud Insights für FlexPod

Alan Cowles, NetApp

In Zusammenarbeit mit: 

Die in diesem technischen Bericht detaillierte Lösung ist die Konfiguration des NetApp Cloud Insights Service zur Überwachung des NetApp AFF A800 Storage-Systems mit NetApp ONTAP, das als Teil einer FlexPod Datacenter-Lösung implementiert wird.

Mehrwert für den Kunden

Die hier vorgestellte Lösung bietet Kunden, die an einer umfassenden Monitoring-Lösung für ihre Hybrid Cloud-Umgebungen interessiert sind und in der ONTAP als primäres Storage-System implementiert wird. Dies umfasst FlexPod Umgebungen, die AFF und FAS Storage-Systeme von NetApp nutzen.

Anwendungsfälle

Diese Lösung trifft auf folgende Anwendungsfälle zu:

- Unternehmen, die verschiedene Ressourcen und Auslastung in ihrem ONTAP Storage-System überwachen möchten, werden als Teil einer FlexPod Lösung implementiert.
- Unternehmen, die Probleme beheben und die Bearbeitungszeit für Vorfälle verkürzen möchten, die in ihrer FlexPod Lösung auf ihren AFF- oder FAS-Systemen auftreten.
- Unternehmen, die an Kostenoptimierungen interessiert sind, darunter individuelle Dashboards, die detaillierte Informationen zu verschwendeten Ressourcen bereitstellen und in denen sich Kosteneinsparungen in ihrer FlexPod-Umgebung – einschließlich ONTAP – realisieren lassen.

Zielgruppe

Die Zielgruppe für die Lösung umfasst die folgenden Gruppen:

- IT-Führungskräfte und diejenigen, die mit Kostenoptimierung und Business Continuity zu tun haben.
- Lösungsarchitekten, die für Datacenter- oder Hybrid-Cloud-Design und -Management interessieren
- Technical Support Engineers, die für die Fehlersuche und die Problembehebung verantwortlich sind.

Sie können Cloud Insights so konfigurieren, dass mehrere nützliche Datentypen zur Unterstützung von Planung, Fehlerbehebung, Wartung und Sicherstellung der Business Continuity verwendet werden können. Durch die Überwachung der FlexPod Datacenter-Lösung mit Cloud Insights und die Darstellung der aggregierten Daten in leicht verdaubaren angepassten Dashboards. Es ist nicht nur möglich, vorherzusagen, wann Ressourcen in einer Implementierung skaliert werden müssen, um den Anforderungen zu entsprechen, sondern auch, um spezielle Applikationen oder Storage Volumes zu identifizieren, die innerhalb des Systems Probleme verursachen. Dadurch wird sichergestellt, dass die zu überwachende Infrastruktur planbar ist und die Anforderungen erfüllt, sodass ein Unternehmen definierte SLAs einhalten und die Infrastruktur nach Bedarf skalieren kann. So werden Verschwendung und zusätzliche Kosten vermieden.

Der Netapp Architektur Sind

In diesem Abschnitt beschäftigen wir uns mit der Architektur einer konvergenten FlexPod Datacenter Infrastruktur, einschließlich eines NetApp AFF A800 Systems, das von Cloud Insights überwacht wird.

Lösungstechnologie

Eine FlexPod Datacenter Lösung umfasst die folgenden Mindestkomponenten, um eine hochverfügbare, leicht skalierbare, validierte und unterstützte konvergente Infrastrukturumgebung bereitzustellen.

- Zwei NetApp ONTAP Storage-Nodes (ein HA-Paar)
- Zwei Cisco Nexus Datacenter Netzwerk-Switches
- Zwei Cisco MDS Fabric Switches (optional für FC-Implementierungen)
- Zwei Cisco UCS Fabric Interconnects
- Ein Cisco UCS Blade Chassis mit zwei Cisco UCS Blade Servern der B-Serie

Oder

- Zwei Cisco UCS C-Series Rack-Server

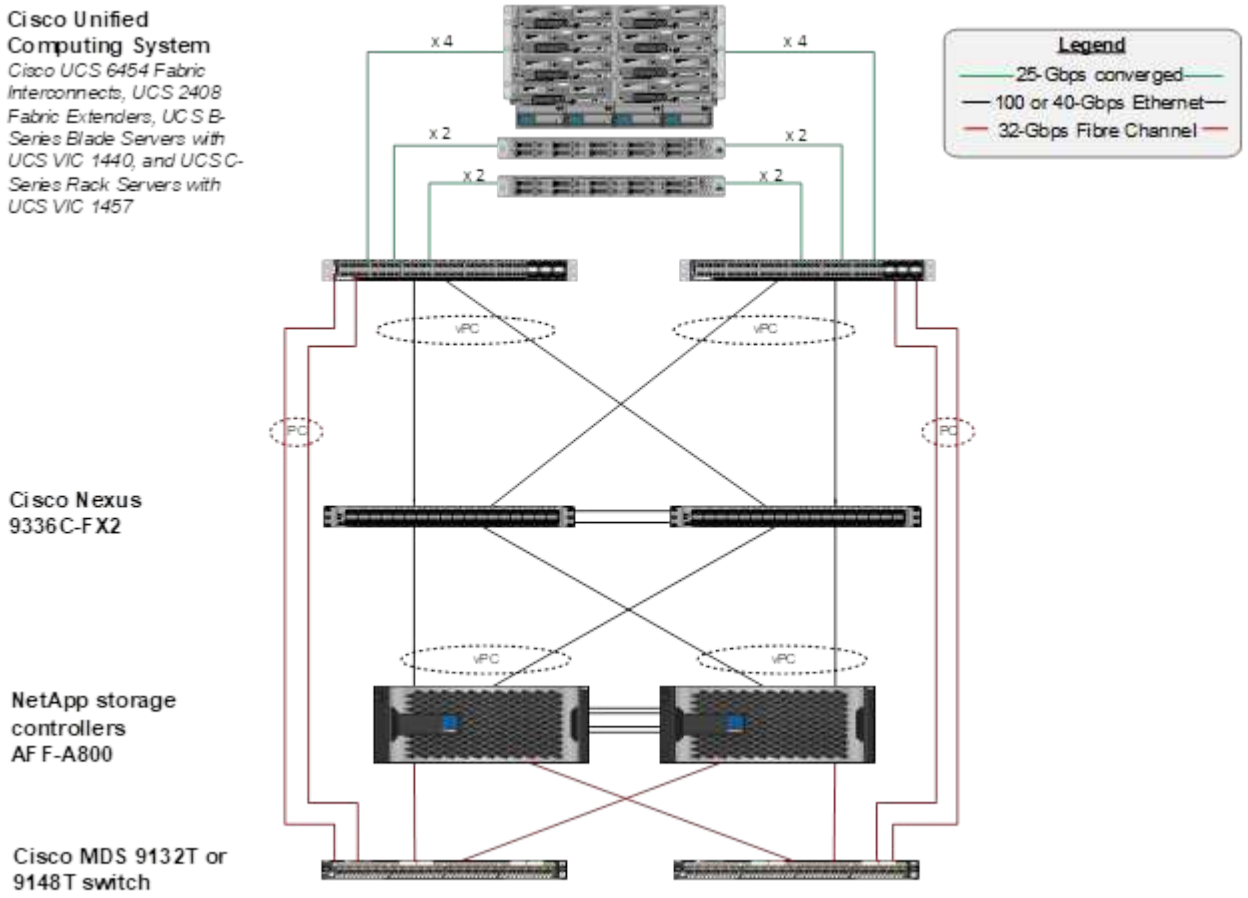
Damit Cloud Insights Daten sammeln kann, muss ein Unternehmen eine Erfassungseinheit als virtuelle oder physische Maschine entweder innerhalb seiner FlexPod-Datacenter-Umgebung oder an einem Ort bereitstellen, an dem die IT-Abteilung die Komponenten kontaktieren kann, von denen sie Daten erfassen. Sie können die Software Acquisition Unit auf einem System installieren, auf dem mehrere unterstützte Windows- oder Linux-Betriebssysteme ausgeführt werden. In der folgenden Tabelle sind die Lösungskomponenten für diese Software aufgeführt.

Betriebssystem	Version
Microsoft Windows	10
Microsoft Windows Server	2012, 2012 R2, 2016, 2019
Red Hat Enterprise Linux	7.2 – 7.6
CentOS	7.2 – 7.6

Betriebssystem	Version
Oracle Enterprise Linux	7.5
Debian	9
Ubuntu	18.04 LTS

Architekturdiagramm

Die folgende Abbildung zeigt die Lösungsarchitektur.



Hardwareanforderungen

In der folgenden Tabelle werden die Hardwarekomponenten aufgeführt, die für die Implementierung der Lösung erforderlich sind. Je nach den Anforderungen des Kunden können die tatsächlich in einer konkreten Implementierung dieser Lösung eingesetzten Hardwarekomponenten abweichen.

Trennt	Menge
Cisco Nexus 9336C-FX2	2
Cisco UCS 6454 Fabric Interconnect	2
Cisco UCS 5108 Blade-Chassis	1
Cisco UCS 2408 Fabric Extender	2
Cisco UCS B200 M5 Blades	2

Trennt	Menge
NetApp AFF A800	2

Softwareanforderungen

In der folgenden Tabelle werden die Softwarekomponenten aufgeführt, die für die Implementierung der Lösung erforderlich sind. Je nach den Anforderungen des Kunden können die in einer konkreten Implementierung dieser Lösung verwendeten Softwarekomponenten abweichen.

Software	Version
Cisco Nexus-Firmware	9.3 (5)
Cisco UCS Version	4.1(2a)
NetApp ONTAP-Version	9.7
NetApp Cloud Insights-Version	September 2020, Basic
Red Hat Enterprise Linux	7.6
VMware vSphere	6.7U3

Einzelheiten zum Anwendungsfall

Diese Lösung trifft auf folgende Anwendungsfälle zu:

- Analyse der Umgebung mit den Daten, die dem digitalen Berater von NetApp Active IQ zur Bewertung der Risiken von Storage-Systemen bereitgestellt werden, und Empfehlungen zur Storage-Optimierung
- Fehlerbehebung im in einem in einem FlexPod Datacenter implementierten ONTAP Storage-System durch Überprüfung der Systemstatistiken in Echtzeit
- Generierung benutzerdefinierter Dashboards zur einfachen Überwachung spezifischer Interessenbereiche für die in einer konvergenten FlexPod Datacenter Infrastruktur implementierten ONTAP Storage-Systeme

Designüberlegungen

Die FlexPod Datacenter Lösung ist eine von Cisco und NetApp entwickelte konvergente Infrastruktur, die eine dynamische, hochverfügbare und skalierbare Datacenter-Umgebung für die Ausführung von Enterprise Workloads bietet. Computing- und Netzwerkressourcen in der Lösung werden von den Produkten Cisco UCS und Nexus bereitgestellt, und die Storage-Ressourcen werden vom ONTAP Storage-System bereitgestellt. Das Lösungsdesign wird regelmäßig erweitert, wenn aktualisierte Hardware- oder Software- und Firmware-Versionen verfügbar sind. Diese Details sowie Best Practices für Lösungsdesign und -Implementierung werden in Dokumenten mit Cisco Validated Design (CVD) oder NetApp Verified Architecture (NVA) festgehalten und regelmäßig veröffentlicht.

Das aktuelle CVD-Dokument mit Details zum Design der FlexPod Datacenter Lösung ist verfügbar "Hier".

Implementieren Sie Cloud Insights für FlexPod

Zum Bereitstellen der Lösung müssen Sie die folgenden Aufgaben ausführen:

1. Melden Sie sich für den Cloud Insights Service an
2. Erstellen Sie eine virtuelle VMware-Maschine (VM), die als Erfassungseinheit konfiguriert werden soll
3. Installieren Sie den Red hat Enterprise Linux-Host (RHEL)
4. Erstellen Sie im Cloud Insights-Portal eine Erfassungseinheit, und installieren Sie die Software
5. Fügen Sie das überwachte Storage-System vom FlexPod Datacenter zu Cloud Insights hinzu.

Melden Sie sich für den NetApp Cloud Insights Service an

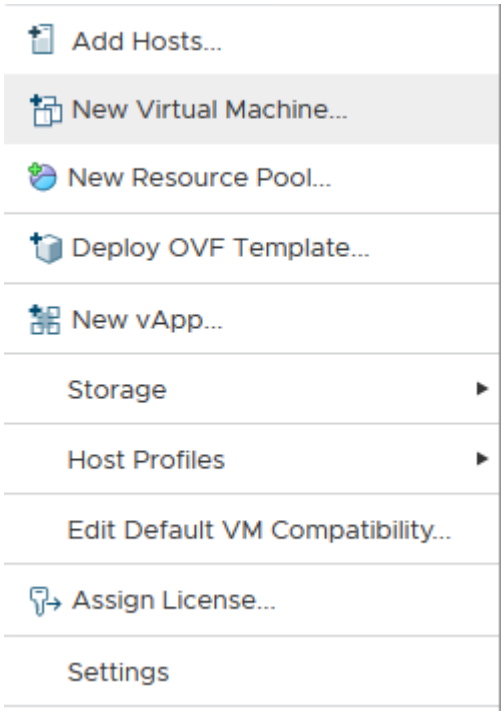
So melden Sie sich für den NetApp Cloud Insights Service an:

1. Gehen Sie zu "https://cloud.netapp.com/cloud-insights"
2. Klicken Sie auf die Schaltfläche in der Mitte des Bildschirms, um die 14-Tage-Testversion zu starten. Oder melden Sie sich über den Link oben rechts an, um sich bei einem bestehenden NetApp Cloud Central Konto anzumelden.

Erstellen Sie eine virtuelle VMware-Maschine, die als Erfassungseinheit konfiguriert werden soll

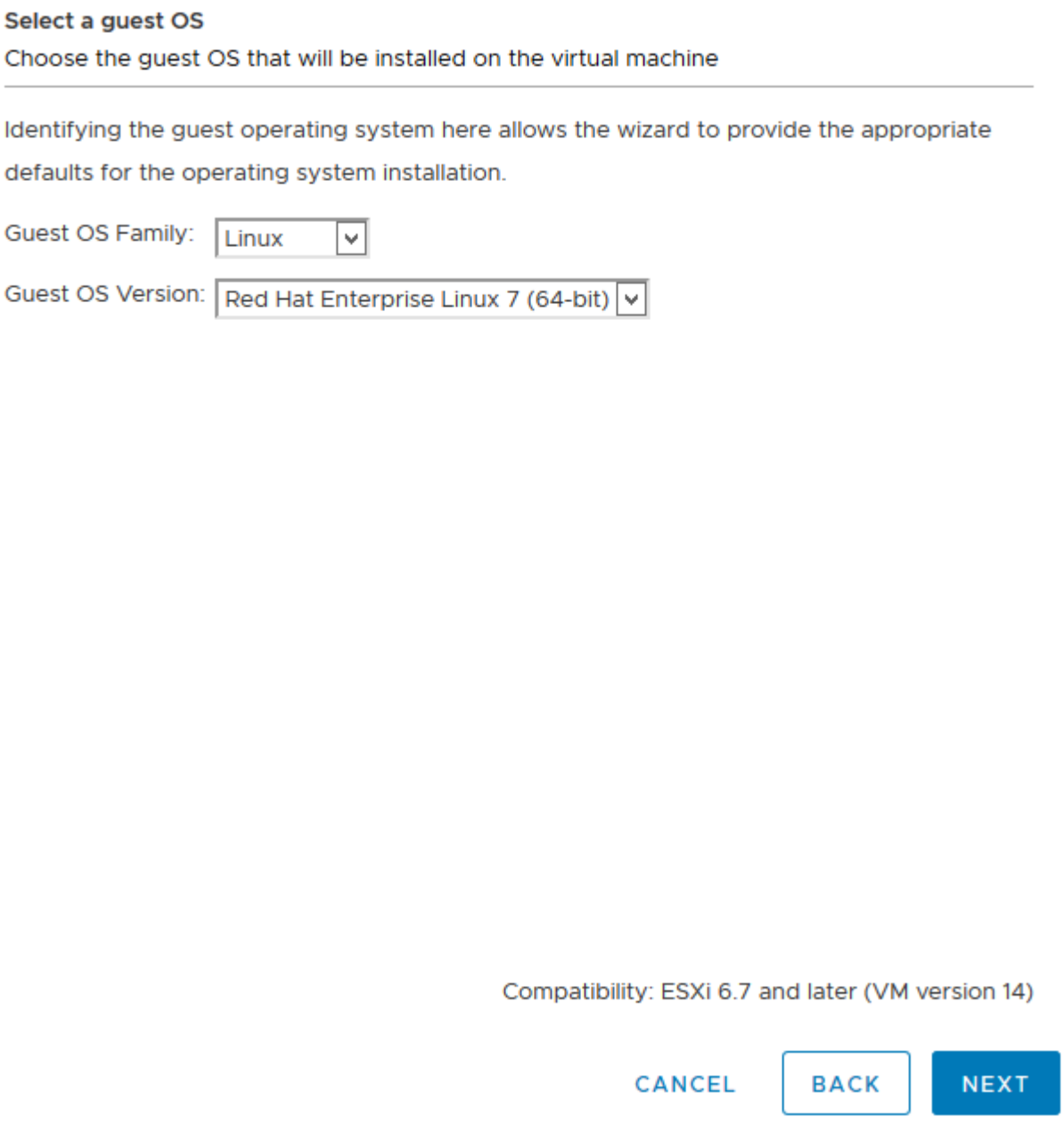
Gehen Sie wie folgt vor, um eine VMware VM zu erstellen, die als Erfassungseinheit konfiguriert werden soll:

1. Starten Sie einen Webbrowser, und melden Sie sich bei VMware vSphere an, und wählen Sie den Cluster aus, der eine VM hosten soll.
2. Klicken Sie mit der rechten Maustaste auf diesen Cluster, und wählen Sie im Menü die Option Create A Virtual Machine aus.



3. Klicken Sie im Assistenten für neue virtuelle Maschinen auf Weiter.

4. Geben Sie den Namen der VM an, und wählen Sie das Datacenter aus, in das sie installiert werden soll, und klicken Sie dann auf Weiter.
5. Wählen Sie auf der folgenden Seite das Cluster, die Nodes oder die Ressourcengruppe aus, für die Sie die VM installieren möchten, und klicken Sie dann auf Weiter.
6. Wählen Sie den gemeinsam genutzten Datenspeicher aus, der Ihre VMs hostet, und klicken Sie auf Weiter.
7. Vergewissern Sie sich, dass der Kompatibilitätsmodus für die VM auf festgelegt ist `ESXi 6.7 or later` Und klicken Sie auf Weiter.
8. Wählen Sie Guest OS Family Linux, Guest OS Version: Red hat Enterprise Linux 7 (64-Bit).



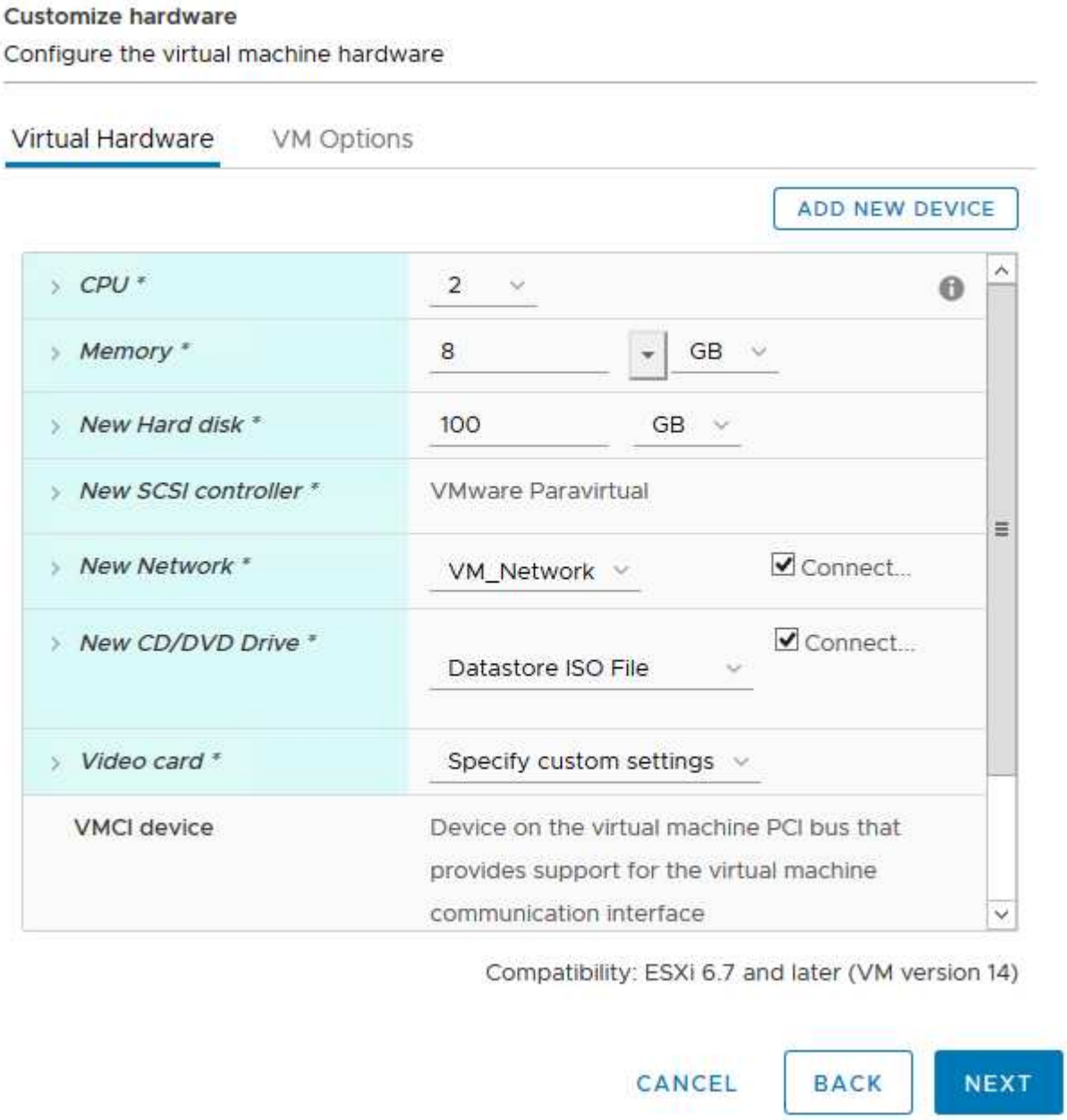
9. Die nächste Seite ermöglicht die Anpassung der Hardwareressourcen auf der VM. Für die Cloud Insights-Erfassungseinheit sind die folgenden Ressourcen erforderlich: Klicken Sie nach Auswahl der Ressourcen auf Weiter:
   a. Zwei CPUs

b. 8 GB RAM

c. 100 GB Festplattenspeicher

d. Ein Netzwerk, das über eine SSL-Verbindung am Port 443 Ressourcen im FlexPod-Datacenter und dem Cloud Insights-Server erreichen kann.

e. Ein ISO-Image der ausgewählten Linux-Distribution (Red hat Enterprise Linux) zum Booten von.

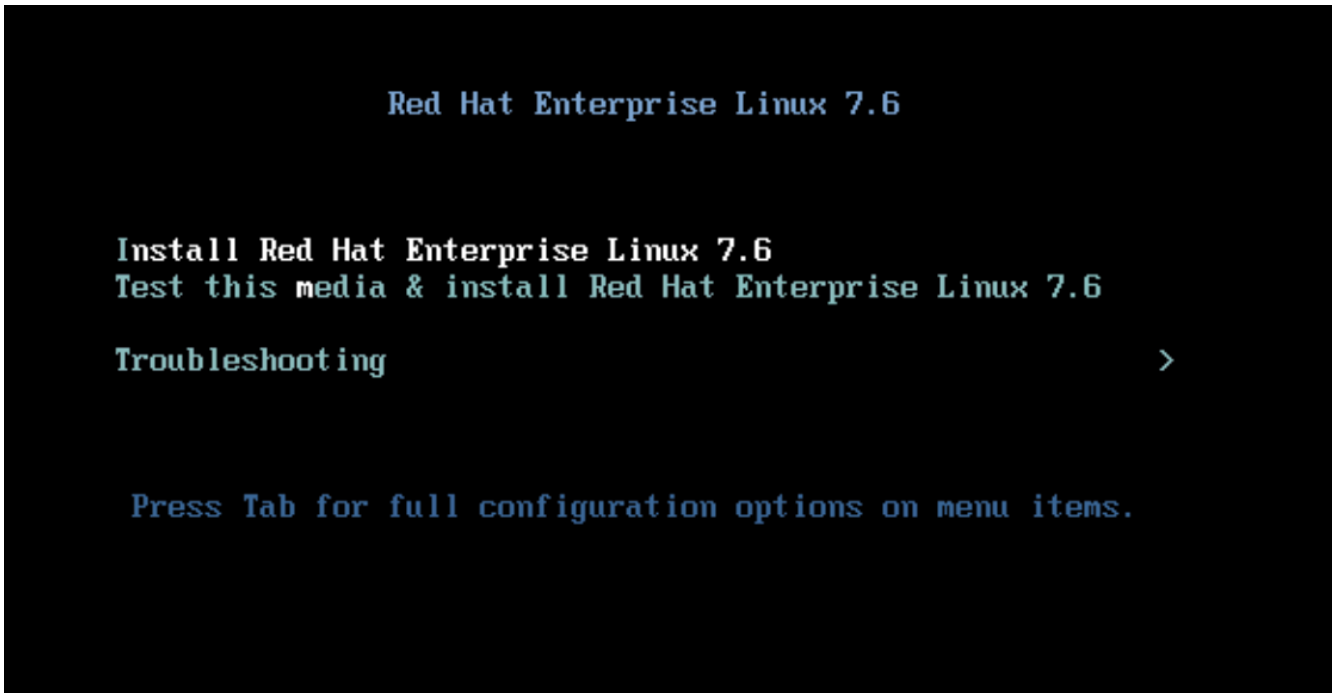


10. Überprüfen Sie zum Erstellen der VM auf der Seite bereit zum Abschließen die Einstellungen, und klicken Sie auf Fertig stellen.

Installieren Sie Red Hat Enterprise Linux

So installieren Sie Red hat Enterprise Linux:

1. Schalten Sie die VM ein, klicken Sie auf das Fenster, um die virtuelle Konsole zu starten, und wählen Sie dann die Option zum Installieren von Red hat Enterprise Linux 7.6 aus.



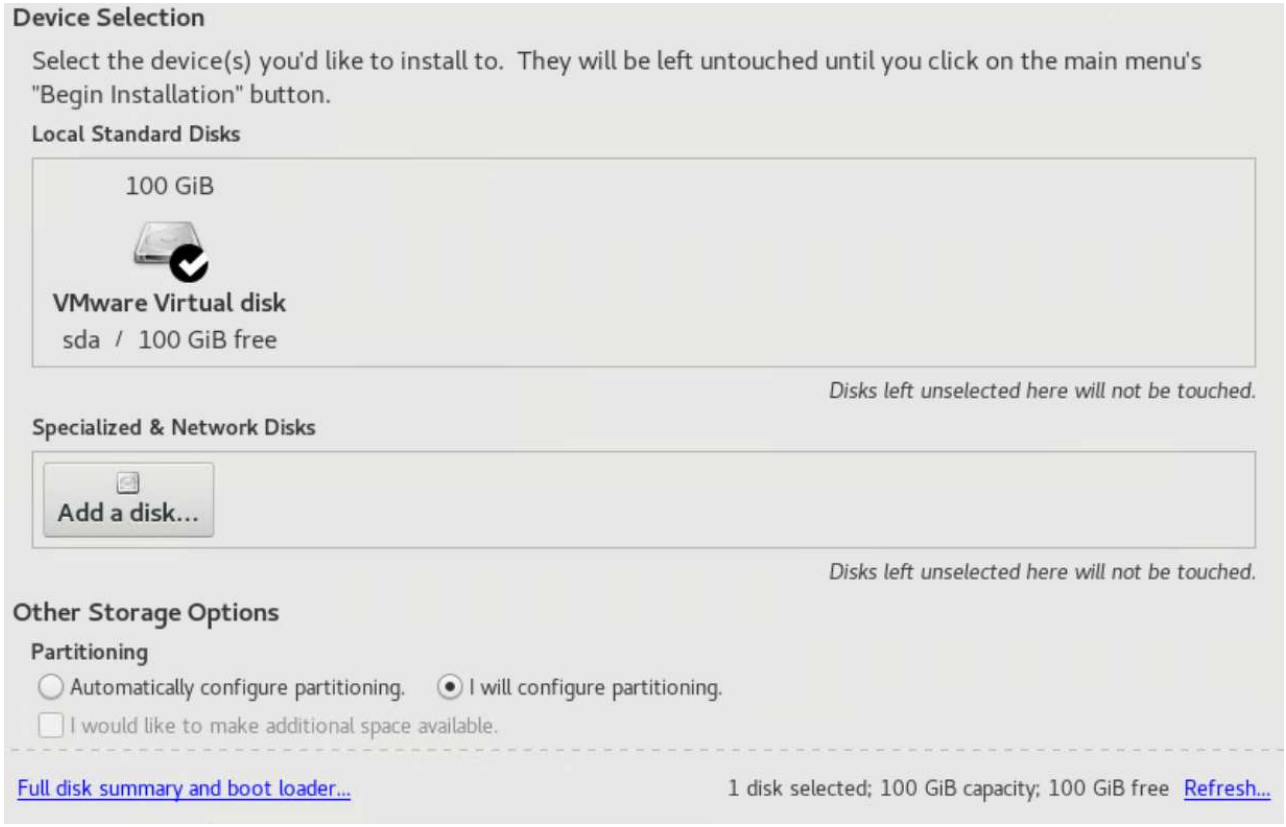
2. Wählen Sie die gewünschte Sprache aus, und klicken Sie auf Weiter.

   Die nächste Seite ist die Zusammenfassung der Installation. Die Standardeinstellungen sollten für die meisten dieser Optionen akzeptabel sein.

3. Sie müssen das Storage-Layout anpassen, indem Sie die folgenden Optionen durchführen:

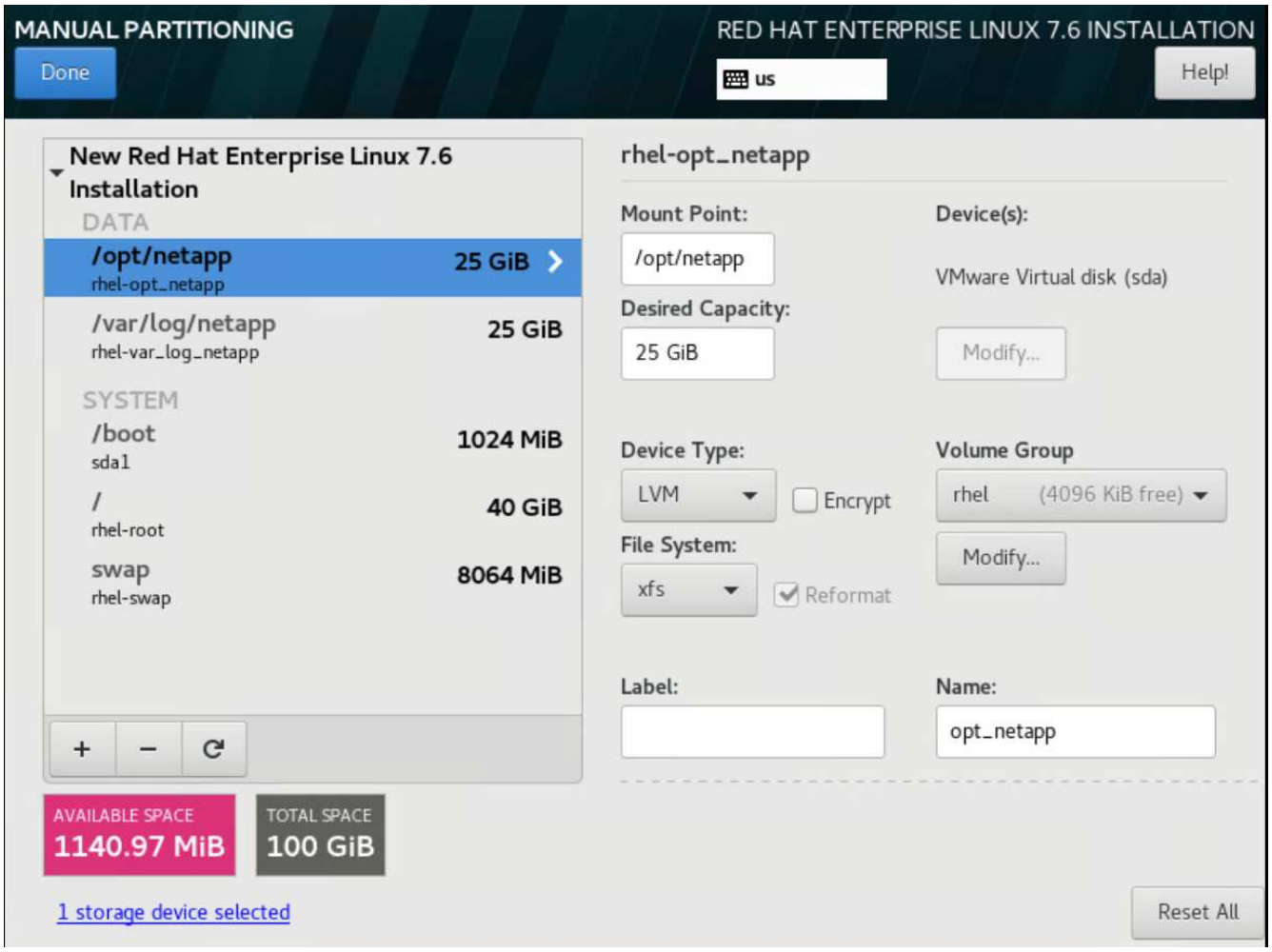
   a. Um die Partitionierung für den Server anzupassen, klicken Sie auf Installationsziel.

   b. Bestätigen Sie, dass die VMware Virtual Disk mit 100 gib mit einem schwarzen Häkchen ausgewählt ist, und aktivieren Sie das Optionsfeld I will Configure Partitioning.



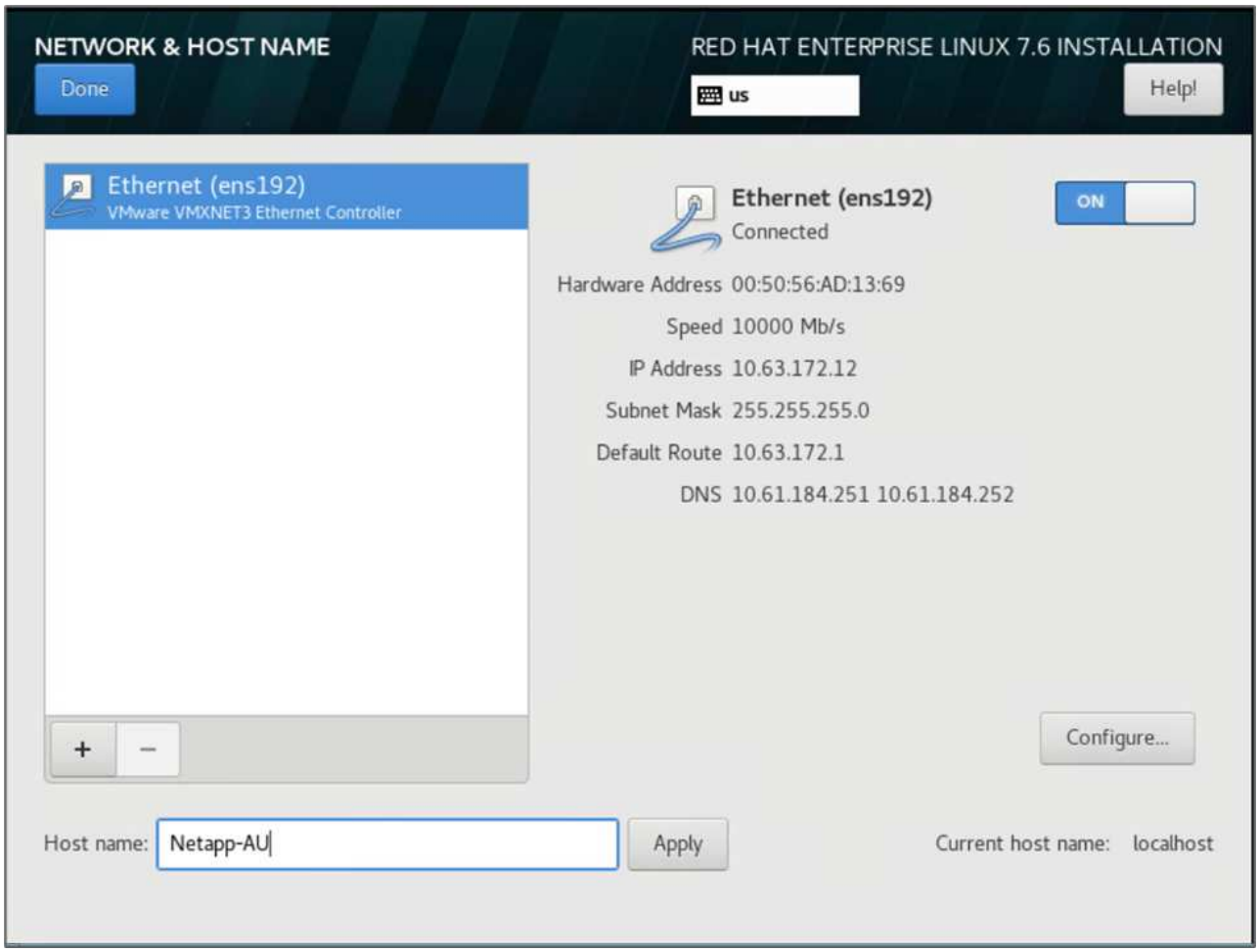
c. Klicken Sie Auf Fertig.

   Es wird ein neues Menü angezeigt, in dem Sie die Partitionstabelle anpassen können. Jeweils 25 GB widmen `/opt/netapp` Und `/var/log/netapp`. Sie können dem System den Rest des Storage automatisch zuweisen.



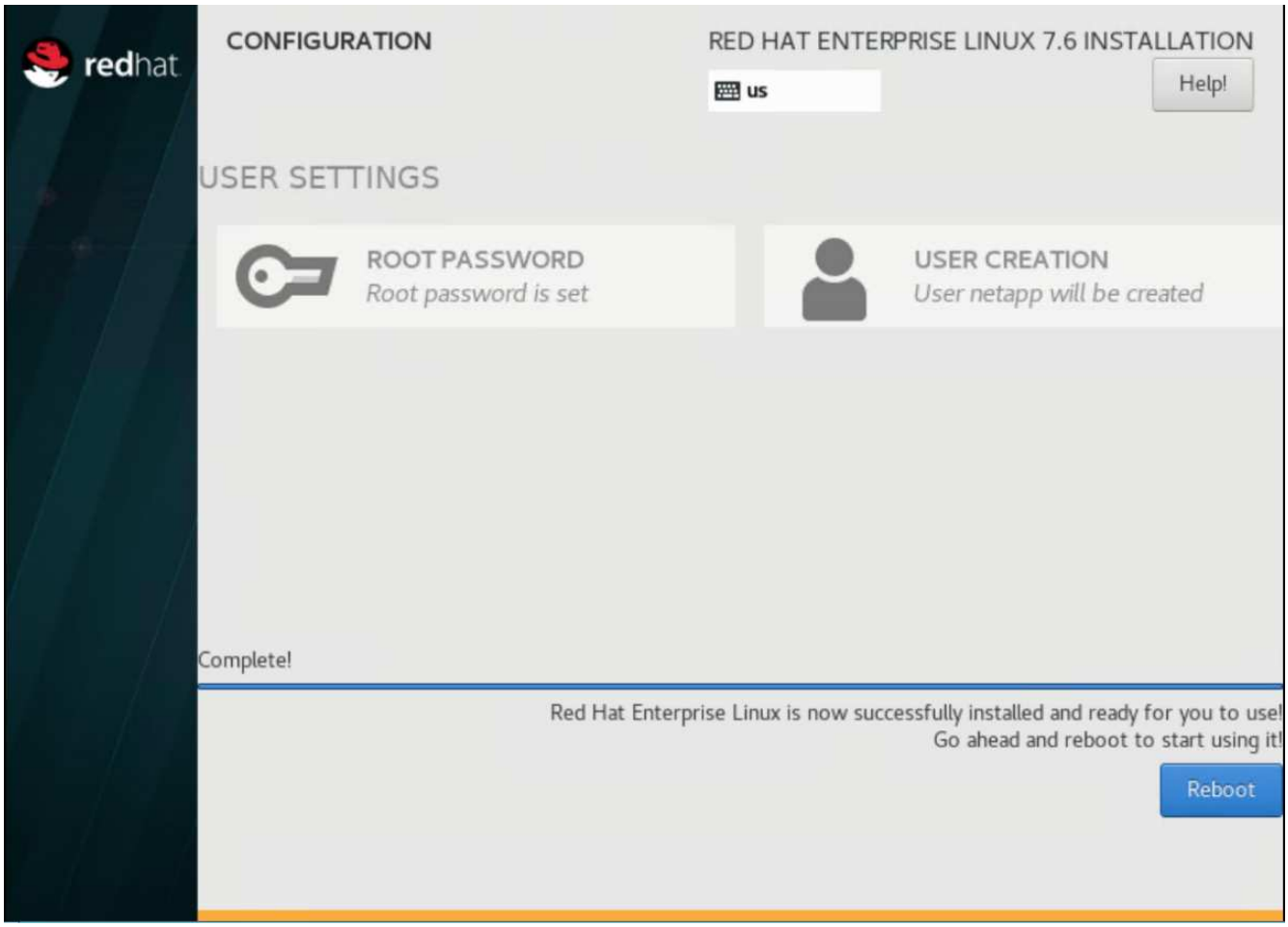
a. Um zur Installationsübersicht zurückzukehren, klicken Sie auf „Fertig“.

4. Klicken Sie auf Netzwerk und Hostname.
   a. Geben Sie einen Hostnamen für den Server ein.
   b. Schalten Sie den Netzwerkadapter ein, indem Sie auf die Schieberegler-Schaltfläche klicken. Wenn DHCP (Dynamic Host Configuration Protocol) in Ihrem Netzwerk konfiguriert ist, erhalten Sie eine IP-Adresse. Falls nicht, klicken Sie auf Konfigurieren, und weisen Sie eine Adresse manuell zu.



c. . Klicken Sie auf „Fertig“, um zur Installationsübersicht zurückzukehren.

5. Klicken Sie auf der Seite Installationsübersicht auf Installation starten.
6. Auf der Seite Installationsfortschritt können Sie das Root-Passwort festlegen oder ein lokales Benutzerkonto erstellen. Klicken Sie nach Abschluss der Installation auf Neu starten, um den Server neu zu starten.



7. Melden Sie sich nach dem Neustart des Systems bei Ihrem Server an, und registrieren Sie ihn bei Red hat Subscription Manager.

```
[root@Netapp-AU ~]# subscription-manager register
Registering to: subscription.rhsm.redhat.com:443/subscription
Username: alan.cowles@netapp.com
Password:
The system has been registered with ID: a47f2e7b-81cd-4757-85c7-eb1818c2c2a1
The registered system name is: Netapp-AU
[root@Netapp-AU ~]#
```

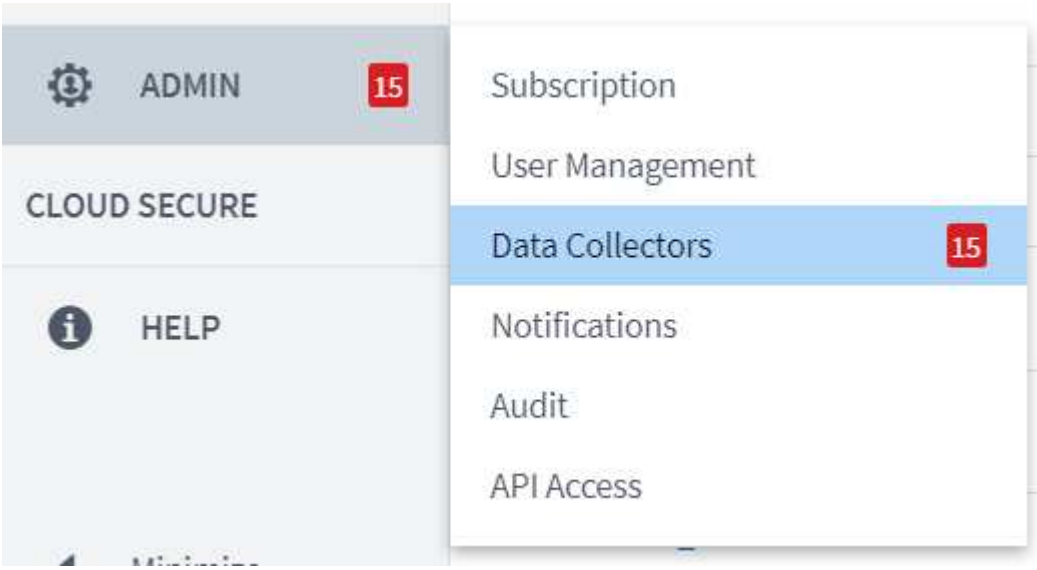
8. Fügen Sie ein verfügbares Abonnement für Red hat Enterprise Linux bei.

```
[root@Netapp-AU ~]# subscription-manager attach --pool=8a85f99b710f3b1901713b90b9e154cf
Successfully attached a subscription for: Red Hat Enterprise Linux, Standard Support (128 Sockets, NFR, Partner Only)
[root@Netapp-AU ~]#
```

Erstellen Sie im Cloud Insights-Portal eine Erfassungseinheit, und installieren Sie die Software

Gehen Sie wie folgt vor, um eine Erfassungseinheit im Cloud Insights-Portal zu erstellen und die Software zu installieren:

1. Bewegen Sie auf der Startseite von Cloud Insights den Mauszeiger über den Eintrag Admin im Hauptmenü links und wählen Sie im Menü Datensammler aus.

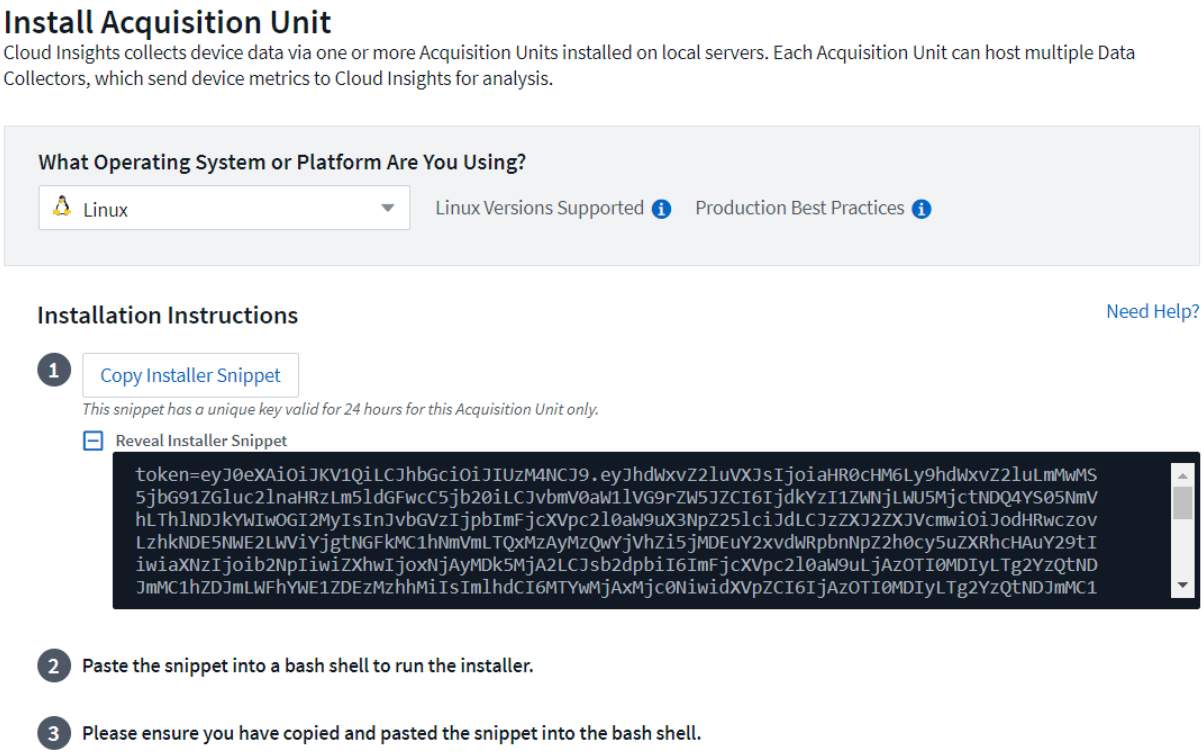


2. Klicken Sie in der oberen Mitte der Seite Data Collectors auf den Link für Acquisition Units.

3. Um eine neue Akquisitionseinheit zu erstellen, klicken Sie auf die Schaltfläche auf der rechten Seite.

4. Wählen Sie das Betriebssystem aus, das Sie zum Hosten Ihrer Erfassungseinheit verwenden möchten, und befolgen Sie die Schritte, um das Installationsskript von der Webseite zu kopieren.

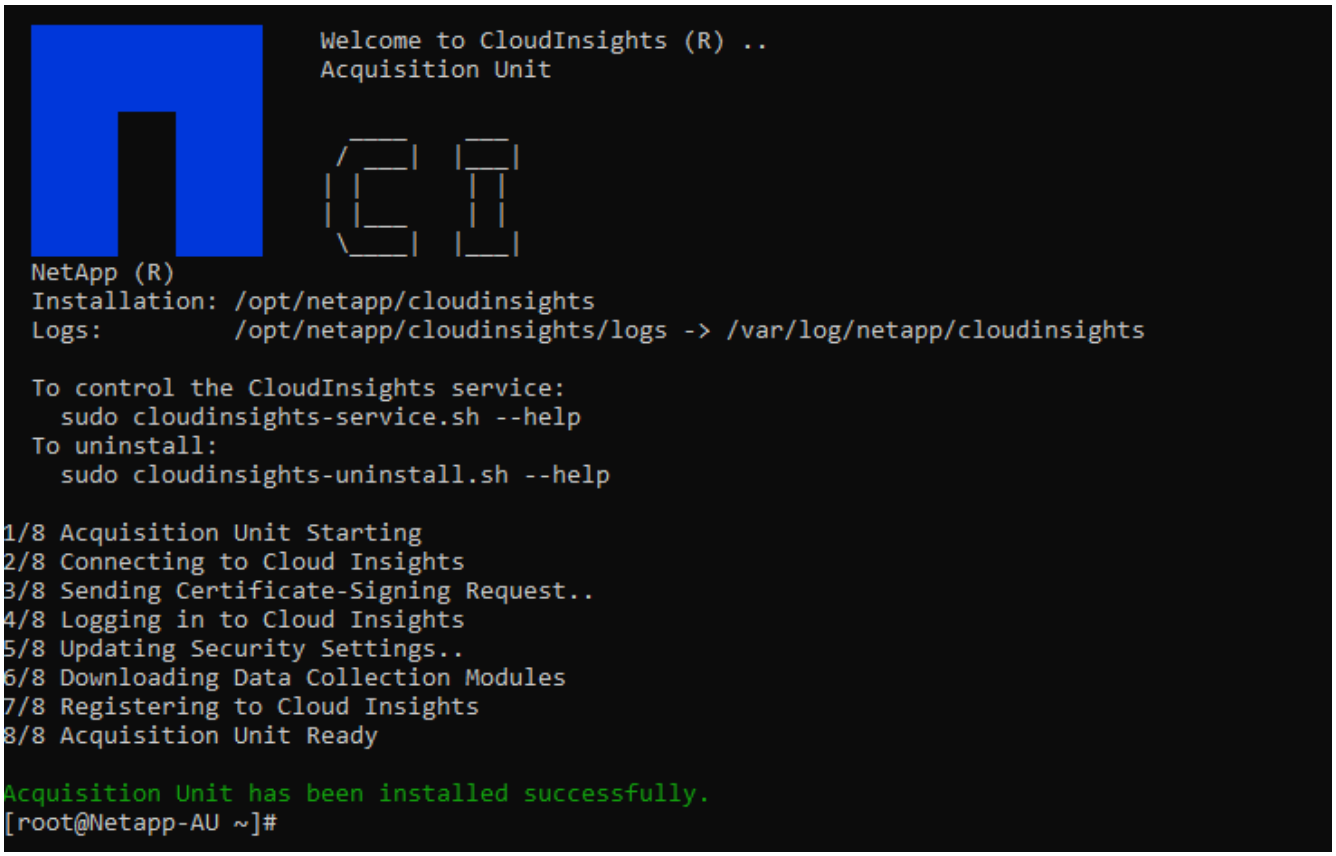
   In diesem Beispiel handelt es sich um einen Linux-Server, der ein Snippet und ein Token zum Einfügen in die CLI auf unserem Host bereitstellt. Auf der Webseite wird darauf gewartet, dass die Erfassungseinheit eine Verbindung herstellt.



5. Fügen Sie das Snippet in die CLI des bereitgestellten Red hat Enterprise Linux-Rechners ein, und klicken Sie auf Enter.

```
[root@Netapp-AU ~]# token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9.eyJhdWxvZ2luVXJsIjoiaHR0cHM6Ly9hdWxvZ2luLmMwMS5jbG91ZGluc
2lnaHRzLm5ldGFwcC5jb20iLCJvbmV0aW1lVG9rZW5JZCI6IjQ5ZTY0MGM5LTY5MTItNDQ4Yi04YmI4LTIwNGY2OTQ2YzY1YSIsInJvbGVzIjpbImFjcXVpc
2l0aW9uX3NpZ25lciJdLCJzZXJ2ZXJVcmwiOiJodHRwczovLzhkNDE5NWE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZi5jMDEuY2xvdWRpbnNpZ2h0cy
y5uZXRhcHAuY29tIiwiaXNzIjoib2NpIiwiZXhwIjoxNjAyMTgyNzg2LCJsb2dpbiI6ImFjcXVpc2l0aW9uLjc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZ
TcxZjk0ODRiZCIsImlhdCI6MTYwMjA5NjMyNiwidXVpZCI6Ijc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZTcxZjk0ODRiZCIsInRlbmFudCI6IjhkNDE5N
WE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZiIsInRlbmFudFN1YmRvbWFpbiI6InBzMTMyNSJ9.RvWLR3wH1_k6fIOCiO_h-Wok2STfFPDj7VksmXqw
-GZ-JqSIe8SZE4Sv3DuWrWM6 domainUrl=https://8d4195a6-ebb8-4ad0-a6ef-41302340b5af.c01.cloudinsights.netapp.com/rest/v1/au
version=1.253.0 bootstrap=cloudinsights-au-install-bootstrap.sh && curl $proxy_auth_scheme -H "Authorization: Bearer $to
ken" -o $bootstrap $domainUrl/installerBootstrap && sudo chmod 755 $bootstrap && sudo /bin/bash -c "TOKEN=$token HTTPS_P
ROXY=$https_proxy PROXY_AUTH_SCHEME=$proxy_auth_scheme AU_VERSION=$version INSTALLER_NAME=cloudinsights-linux-au-install
er-$version INSTALLER_URL=$domainUrl/installers/linux/$version ./$bootstrap"
```

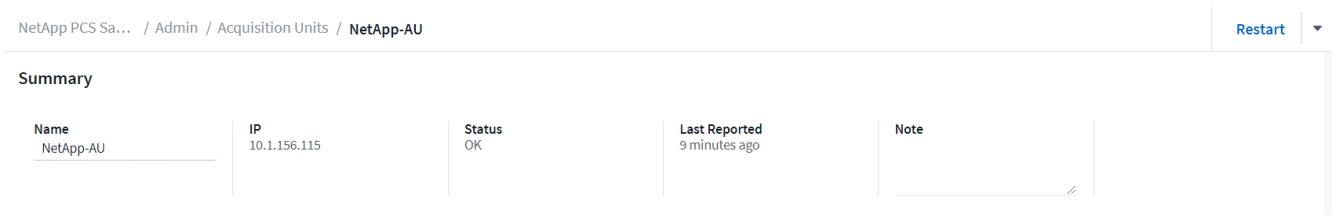
Das Installationsprogramm lädt ein komprimiertes Paket herunter und beginnt mit der Installation. Nach Abschluss der Installation erhalten Sie eine Nachricht, die besagt, dass die Erwerbseinheit bei NetApp Cloud Insights registriert wurde.



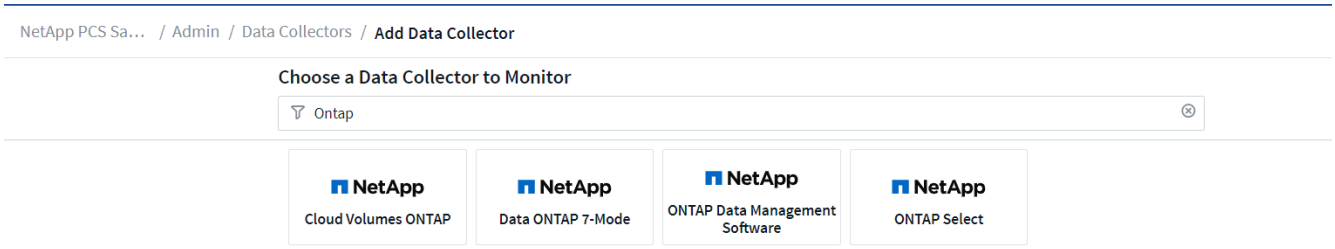
Fügen Sie das überwachte Storage-System vom FlexPod Datacenter zu Cloud Insights hinzu

Um das ONTAP Storage-System aus einer FlexPod Implementierung hinzuzufügen, gehen Sie wie folgt vor:

1. Kehren Sie zur Seite „Acquisition Units“ im Cloud Insights-Portal zurück und suchen Sie die neu registrierte Einheit. Um eine Zusammenfassung des Geräts anzuzeigen, klicken Sie auf das Gerät.

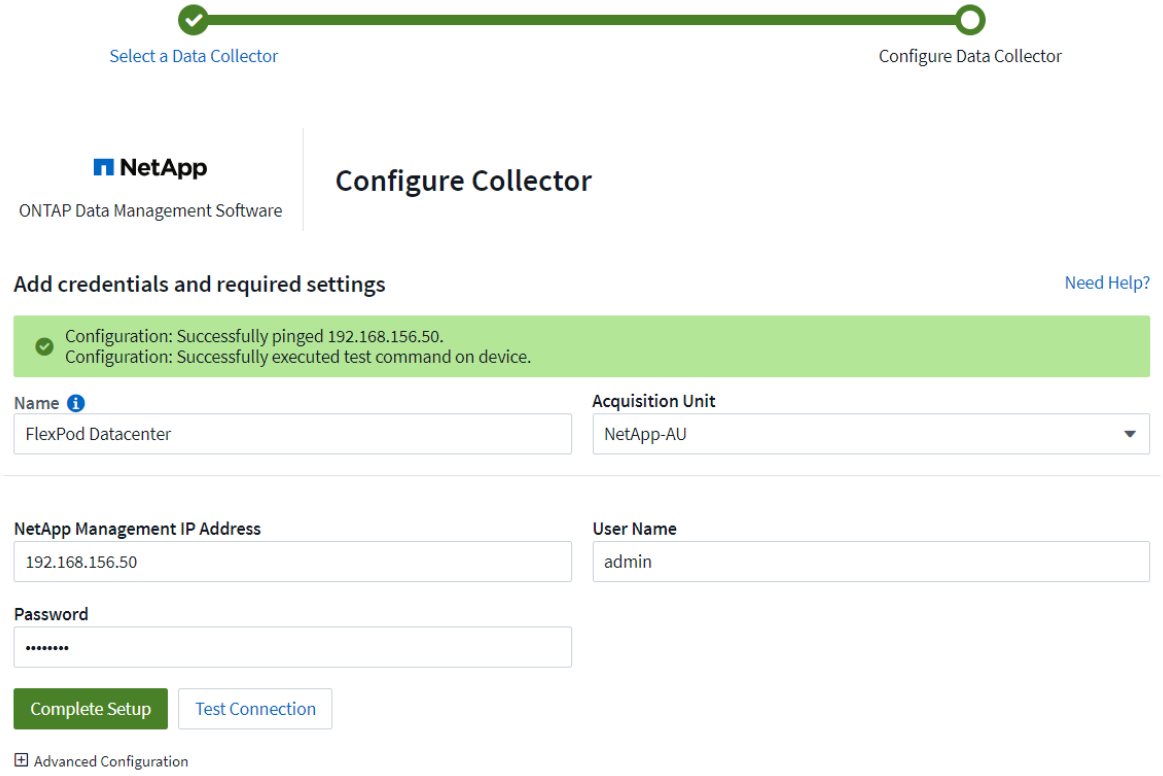


2. Um einen Assistenten zum Hinzufügen des Speichersystems zu starten, klicken Sie auf der Seite Zusammenfassung auf die Schaltfläche zum Erstellen eines Datensammlers. Auf der ersten Seite werden alle Systeme angezeigt, aus denen Daten erfasst werden können. Verwenden Sie die Suchleiste, um nach ONTAP zu suchen.



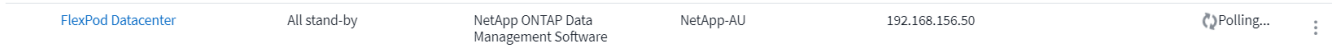
3. Wählen Sie ONTAP Datenmanagement-Software.

   Es wird eine Seite angezeigt, auf der Sie einen Namen für die Bereitstellung festlegen und die zu verwendende Akquisitionseinheit auswählen können. Sie können die Konnektivitätsinformationen und Anmeldeinformationen für das ONTAP System angeben und die Verbindung zur Bestätigung testen.



4. Klicken Sie Auf Setup Abschließen.

   Das Portal kehrt zur Seite Data Collectors zurück und der Data Collector beginnt seine erste Umfrage, bei der Daten aus dem ONTAP Storage-System im FlexPod Datacenter gesammelt werden.



Anwendungsfälle

Mit Cloud Insights für das Monitoring Ihrer FlexPod Datacenter Lösung eingerichtet und

konfiguriert, können wir einige der Aufgaben untersuchen, die Sie auf dem Dashboard durchführen können, um Ihre Umgebung zu bewerten und zu überwachen. In diesem Abschnitt werden fünf primäre Anwendungsfälle für Cloud Insights vorgestellt:

- Active IQ Integration
- Über Echtzeit-Dashboards entdecken
- Erstellen benutzerdefinierter Dashboards
- Erweiterte Fehlerbehebung
- Storage-Optimierung

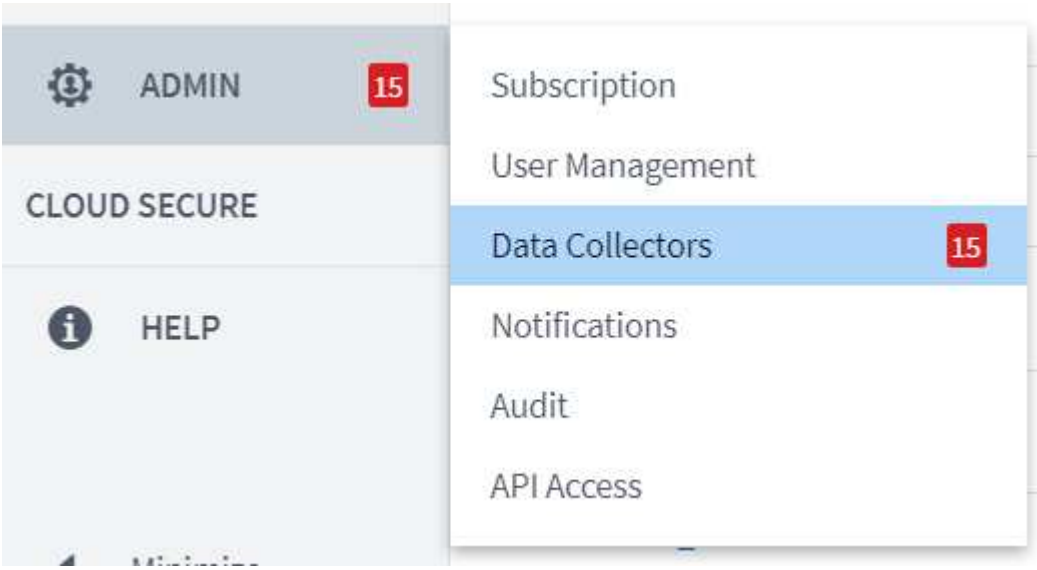
Active IQ Integration

Cloud Insights ist vollständig in die Active IQ Storage-Monitoring-Plattform integriert. Ein ONTAP System, das als Teil einer FlexPod Datacenter Lösung implementiert wird, wird automatisch so konfiguriert, dass es Informationen über die in die einzelnen Systeme integrierte AutoSupport Funktion an NetApp zurücksendet. Diese Berichte werden planmäßig oder dynamisch erzeugt, wenn ein Fehler im System erkannt wird. Die über AutoSupport kommunizierten Daten werden aggregiert und in leicht zugänglichen Dashboards unter dem Active IQ-Menü in Cloud Insights angezeigt.

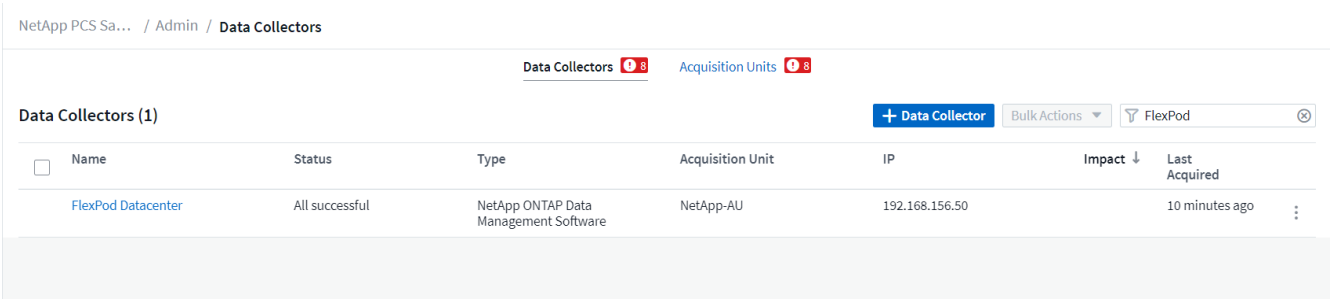
Greifen Sie über das Cloud Insights Dashboard auf Active IQ-Informationen zu

So greifen Sie über das Cloud Insights Dashboard auf Active IQ-Informationen zu:

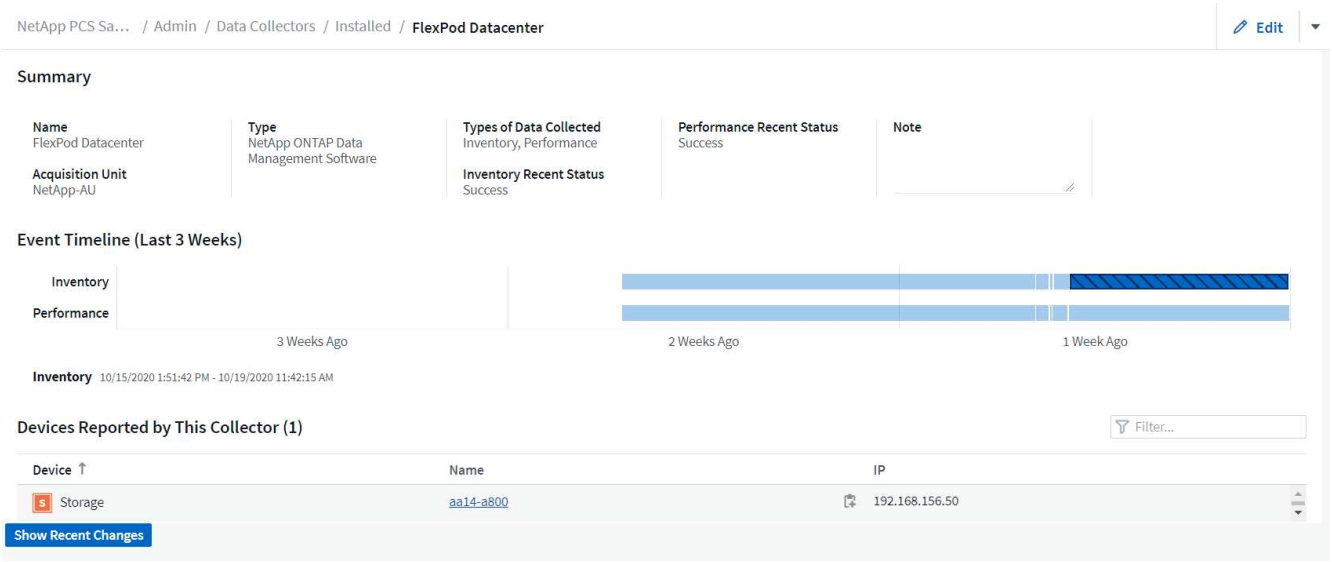
1. Klicken Sie auf die Option Data Collector im Menü Admin auf der linken Seite.



2. Filtern Sie nach dem bestimmten Data Collector in Ihrer Umgebung. In diesem Beispiel wurde der Begriff FlexPod nach dem Begriff gefiltert.

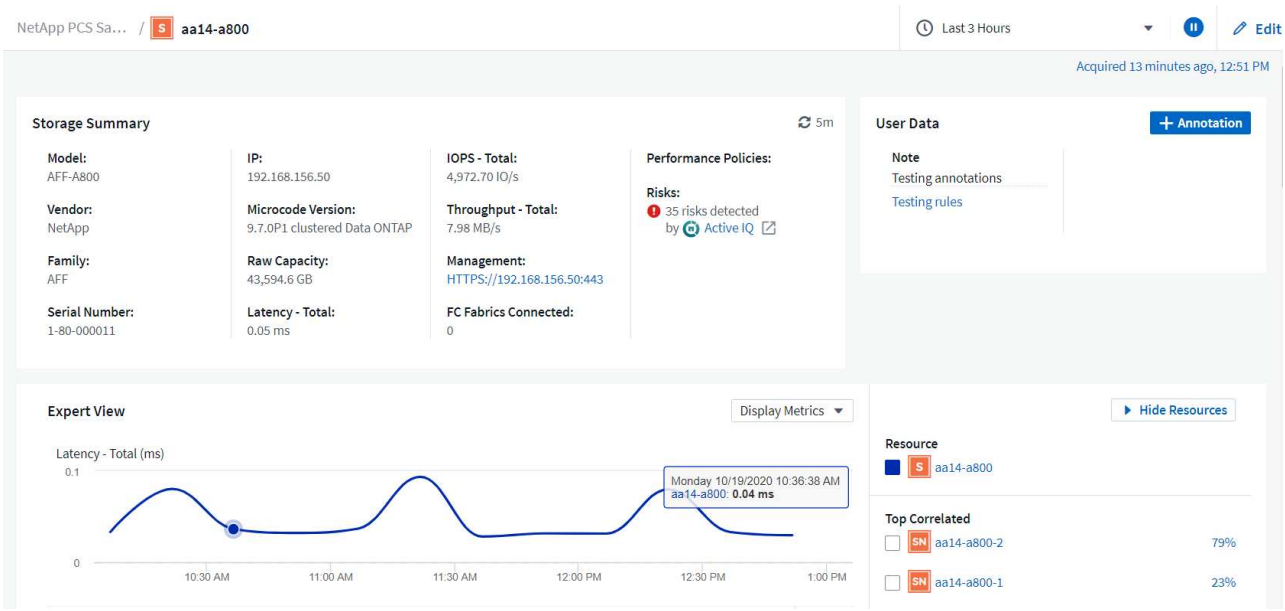


3. Klicken Sie auf den Data Collector, um eine Übersicht über die Umgebung und die Geräte zu erhalten, die von diesem Collector überwacht werden.

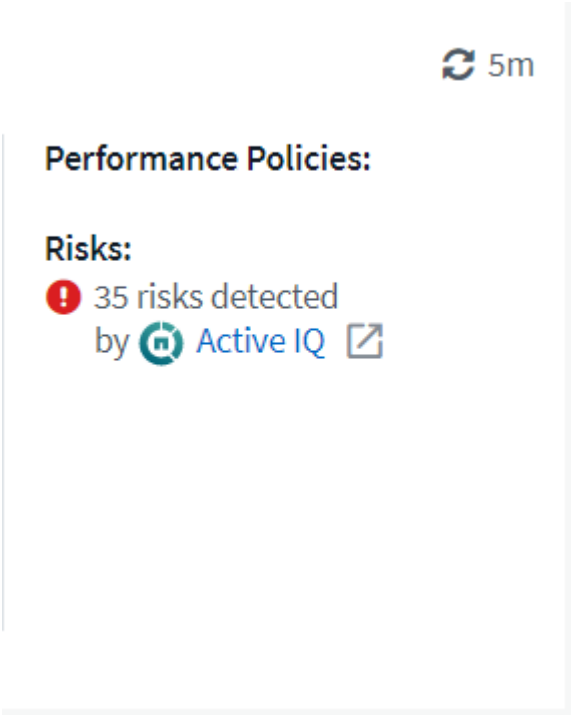


Klicken Sie unter der Geräteliste unten auf den Namen des überwachten ONTAP Storage-Systems. Auf diese Weise wird ein Dashboard mit Informationen angezeigt, die über das System erfasst wurden. Dazu gehören folgende Details:

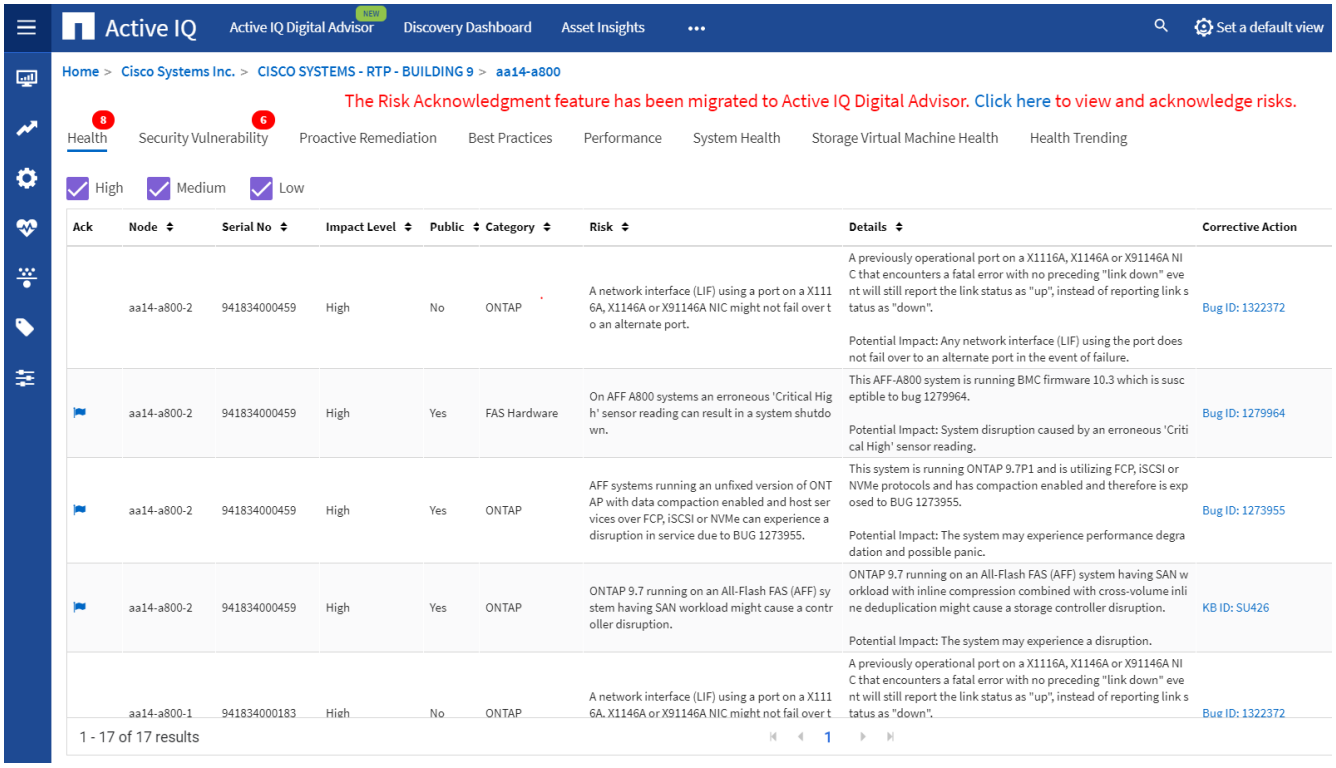
- Modell
- Familie
- ONTAP-Version
- Bruttokapazität
- IOPS-Durchschnitt
- Durchschnittliche Latenz
- Durchschnittlicher Durchsatz



Auf dieser Seite im Abschnitt Leistungsrichtlinien finden Sie außerdem einen Link zu NetApp Active IQ.



4. Zum Öffnen einer Registerkarte für einen neuen Browser gelangen Sie zur Seite zur Risikominimierung, die zeigt, welche Nodes betroffen sind, wie wichtig die Risiken sind und welche Maßnahmen zur Behebung der erkannten Probleme ergriffen werden müssen, klicken Sie auf den Link für Active IQ.

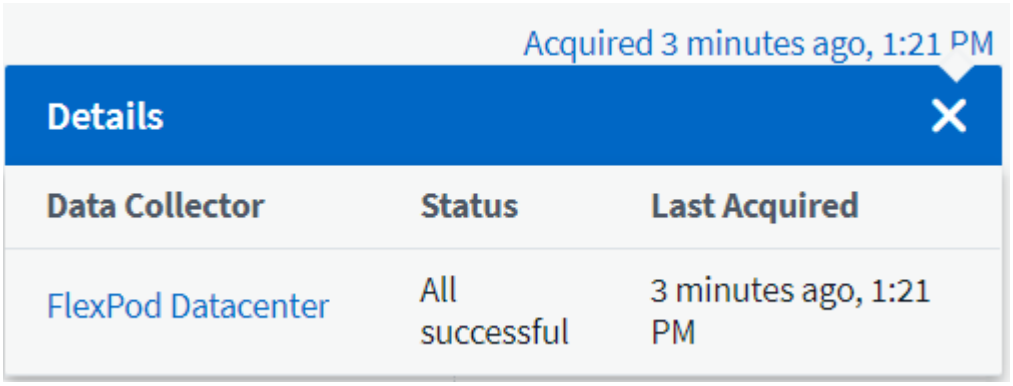


Dashboards in Echtzeit

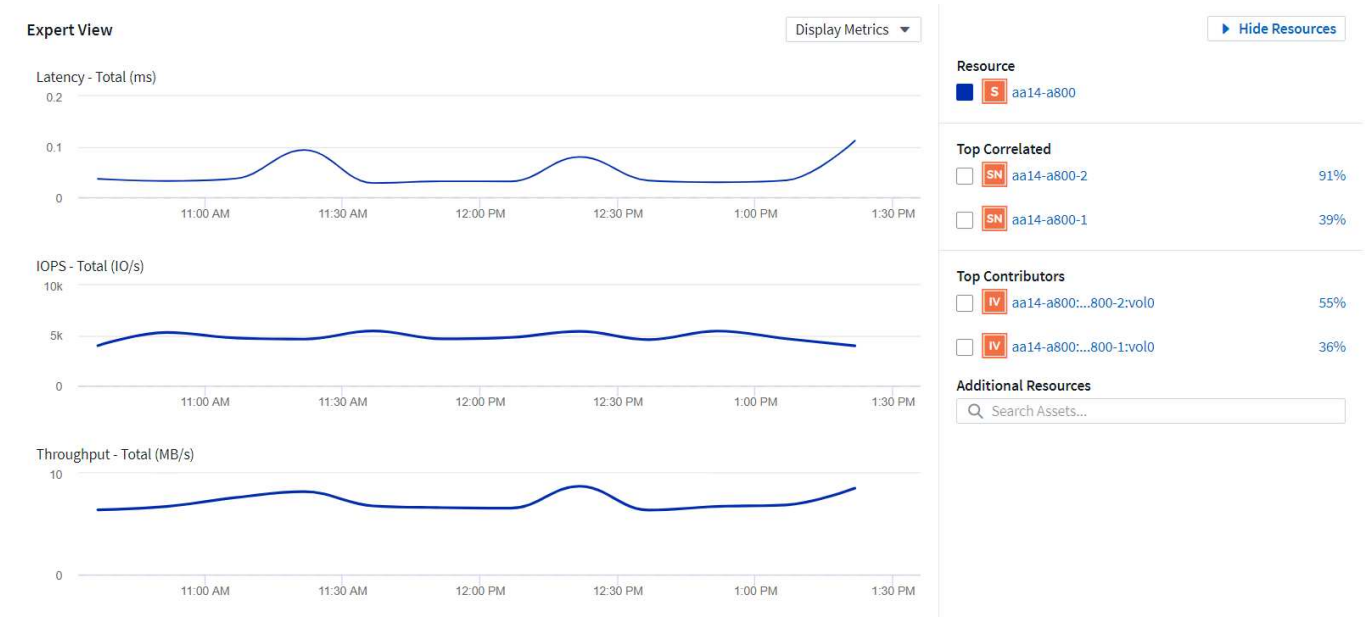
Cloud Insights bietet Echtzeit-Dashboards mit Informationen, die von dem in einer FlexPod Datacenter-Lösung implementierten ONTAP Storage-System abgefragt wurden. Die Cloud Insights-Erfassungseinheit erfasst Daten in regelmäßigen Abständen und füllt das Standard-Storage-System-Dashboard mit den erfassten Informationen aus.

Zugriff auf Echtzeitdiagramme über das Cloud Insights Dashboard

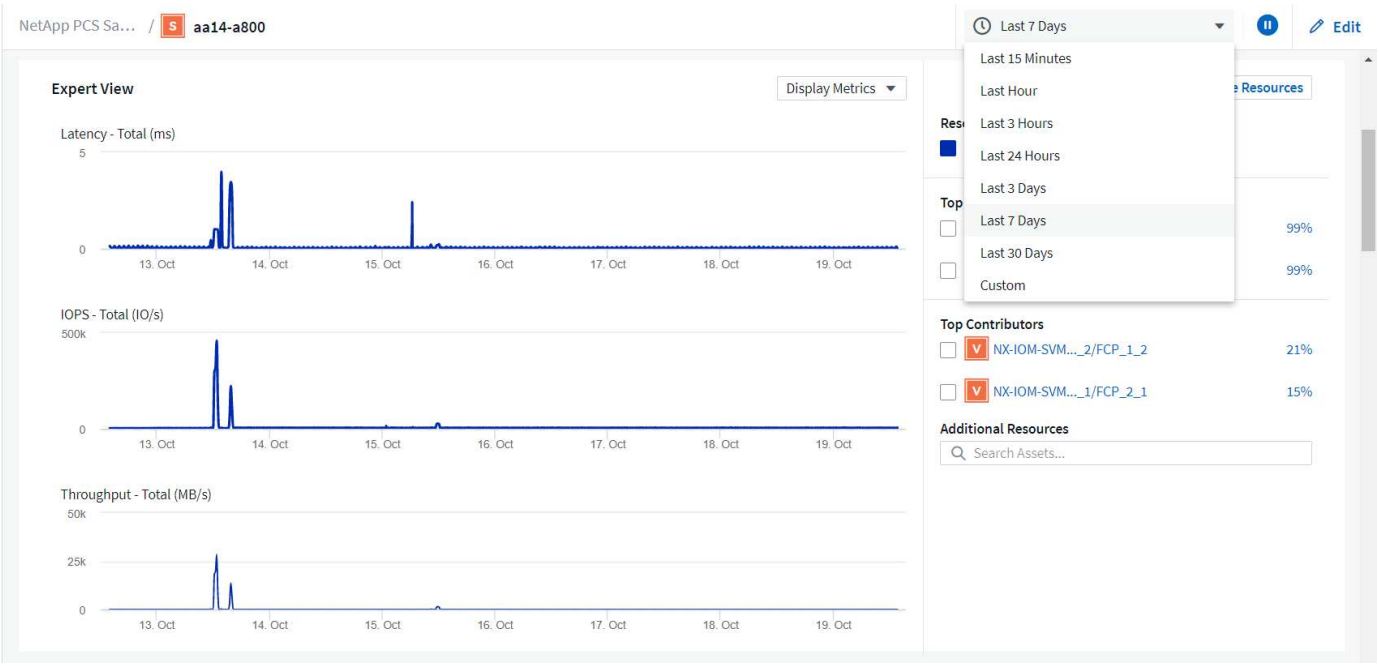
Im Dashboard des Speichersystems wird angezeigt, wenn der Data Collector die Informationen zuletzt aktualisiert hat. Ein Beispiel hierfür ist in der Abbildung unten dargestellt.



Standardmäßig werden auf dem Storage-System-Dashboard mehrere interaktive Diagramme angezeigt, die systemweite Metriken vom zu beforschenden Storage-System oder von jedem einzelnen Node zeigen, darunter Latenz, IOPS und Durchsatz im Abschnitt Expert View. Beispiele für diese Standarddiagramme sind in der folgenden Abbildung dargestellt.



Standardmäßig werden in den Diagrammen Informationen der letzten drei Stunden angezeigt. Sie können diese jedoch in der Dropdown-Liste oben rechts im Dashboard des Storage-Systems auf eine Reihe verschiedener Werte oder einen benutzerdefinierten Wert festlegen. Dies ist in der Abbildung unten dargestellt.



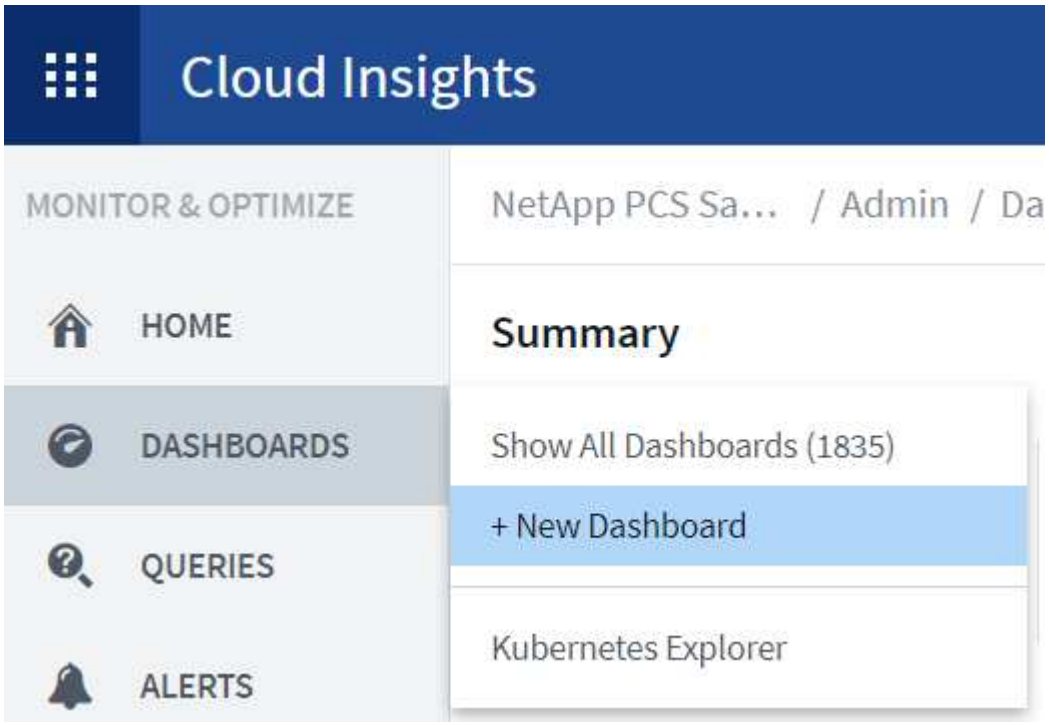
Erstellen benutzerdefinierter Dashboards

Nutzen Sie nicht nur die Standard-Dashboards, die systemweite Informationen anzeigen, sondern erstellen Sie mithilfe von Cloud Insights vollständig angepasste Dashboards, mit denen Sie sich auf die Ressourcenauslastung für bestimmte Storage-Volumes in der FlexPod Datacenter Lösung konzentrieren können. Daher werden die in der konvergenten Infrastruktur implementierten Applikationen, die von diesen Volumes für eine effektive Ausführung abhängen. Auf diese Weise lässt sich eine bessere Visualisierung bestimmter Applikationen und der in der Datacenter-Umgebung genutzten Ressourcen erzielen.

Erstellen Sie ein angepasstes Dashboard zur Bewertung von Storage-Ressourcen

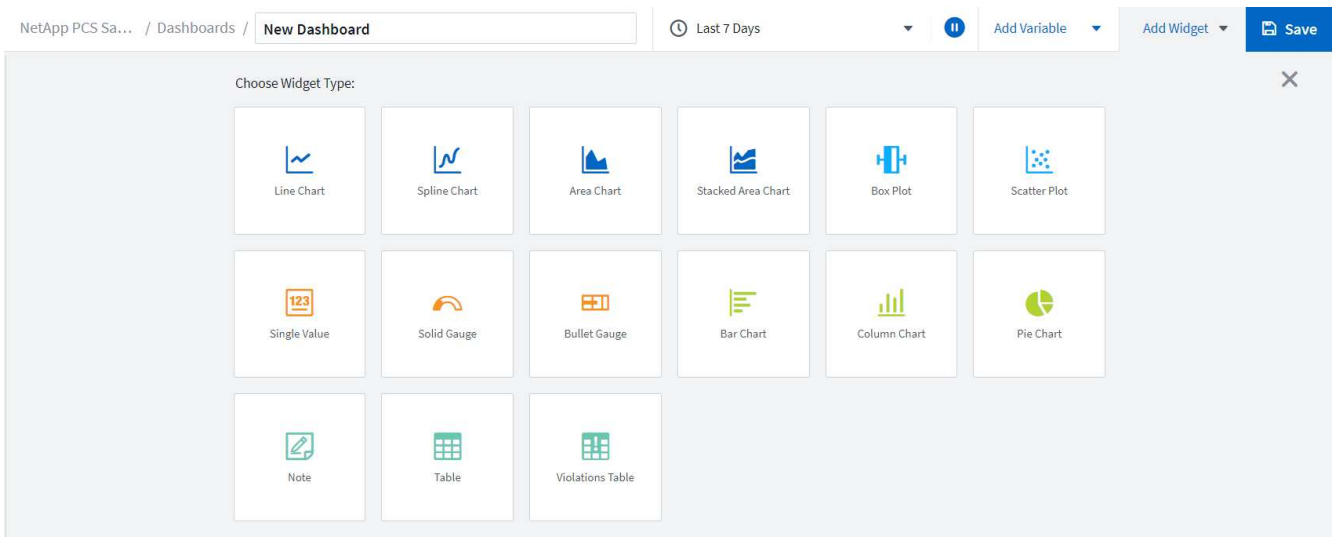
Gehen Sie wie folgt vor, um ein angepasstes Dashboard zur Bewertung von Storage-Ressourcen zu erstellen:

1. Wenn Sie ein angepasstes Dashboard erstellen möchten, bewegen Sie den Mauszeiger über Dashboards im Hauptmenü von Cloud Insights, und klicken Sie in der Dropdown-Liste auf + Neues Dashboard.



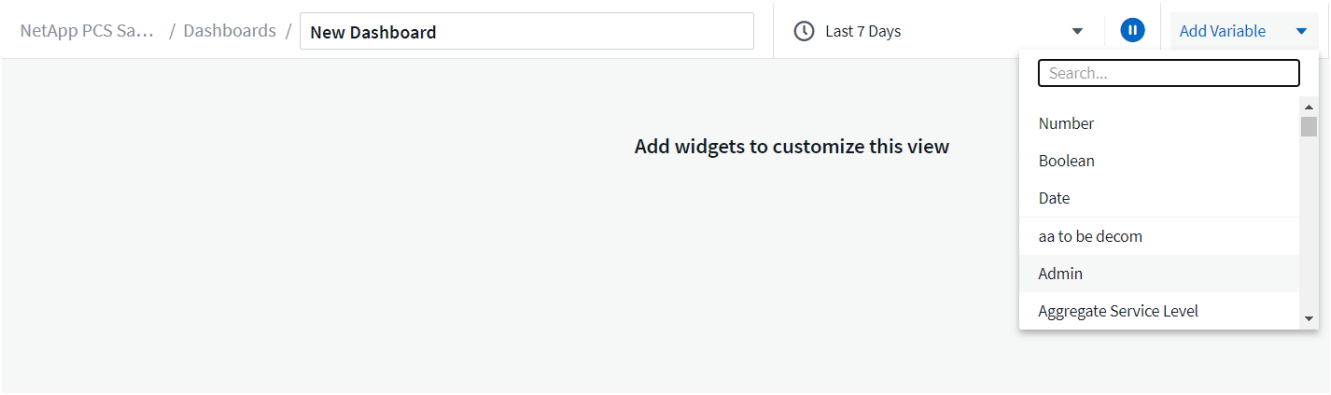
   Das Fenster Neues Dashboard wird geöffnet.

2. Benennen Sie das Dashboard, und wählen Sie den Typ des Widgets aus, mit dem die Daten angezeigt werden. Sie können aus einer Reihe von Diagrammtypen oder sogar Notizen oder Tabellentypen auswählen, um die erfassten Daten anzuzeigen.



3. Wählen Sie im Menü Variable hinzufügen benutzerdefinierte Variablen aus.

   Dadurch können die präsentierten Daten fokussiert werden, um spezifische oder speziellere Faktoren anzuzeigen.



4. Wenn Sie ein benutzerdefiniertes Dashboard erstellen möchten, wählen Sie den Widget-Typ aus, den Sie verwenden möchten, beispielsweise ein Kreisdiagramm zur Anzeige der Storage-Auslastung nach Volume:

   a. Wählen Sie das Widget „TIE-Diagramm“ aus der Dropdown-Liste „Widget hinzufügen“ aus.

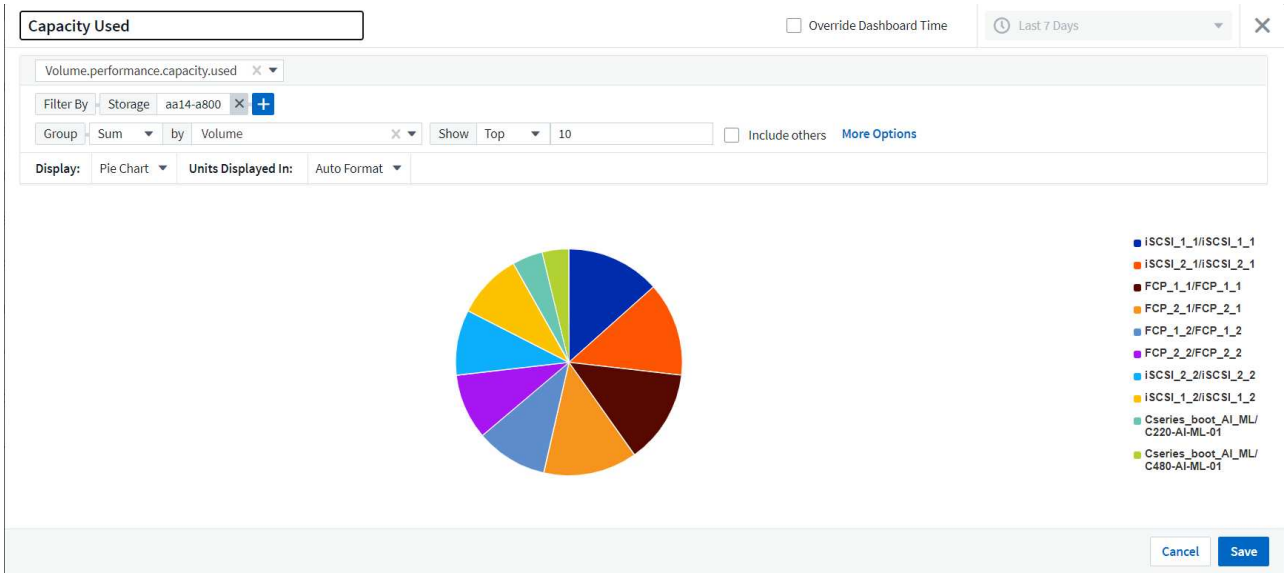
   b. Benennen Sie das Widget mit einer beschreibenden Kennung, z. B. `Capacity Used`.

   c. Wählen Sie das anzuzeigende Objekt aus. Sie können beispielsweise nach dem Schlüsselwort Volume suchen und auswählen `volume.performance.capacity.used`.

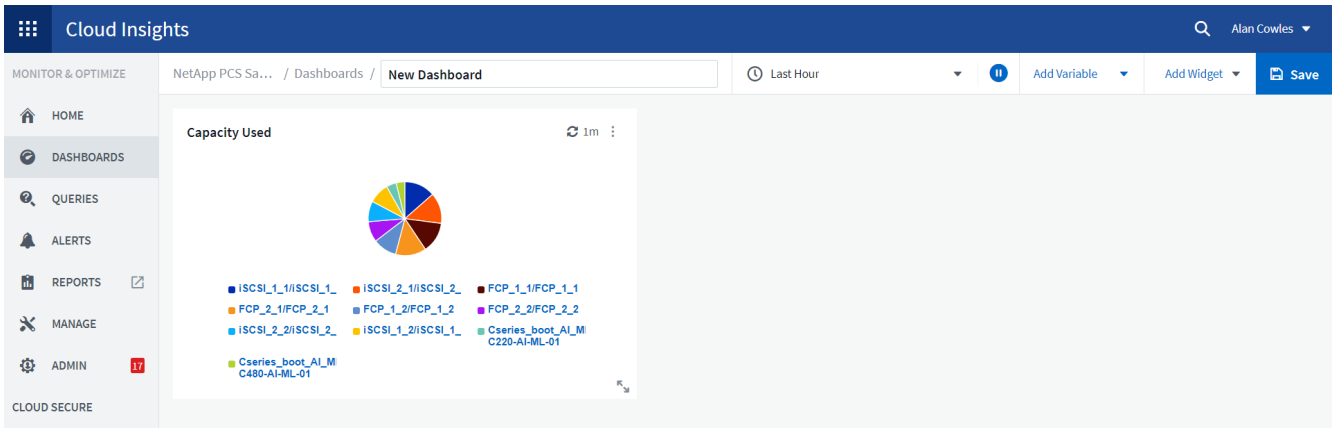
   d. Um nach Storage-Systemen zu filtern, verwenden Sie den Filter, und geben Sie den Namen des Storage-Systems in der FlexPod Datacenter Lösung ein.

   e. Passen Sie die angezeigten Informationen an. Standardmäßig werden bei dieser Auswahl ONTAP-Daten-Volumes angezeigt und die Top 10 aufgelistet.

   f. Um das benutzerdefinierte Dashboard zu speichern, klicken Sie auf Speichern.



   Nach dem Speichern des benutzerdefinierten Widgets kehrt der Browser zur Seite Neues Dashboard zurück, auf der das neu erstellte Widget angezeigt wird, und ermöglicht die Durchführung interaktiver Aktionen, wie z. B. das Ändern des Datenabfragungsperiode.



Erweiterte Fehlerbehebung

Mit Cloud Insights können erweiterte Methoden zur Fehlerbehebung auf alle Storage-Umgebungen in einer konvergenten FlexPod Datacenter Infrastruktur angewendet werden. Unter Verwendung der Komponenten der oben genannten Funktionen: Active IQ Integration, Standard-Dashboards mit Echtzeitstatistiken und angepasster Dashboards können Probleme frühzeitig erkannt und schnell gelöst werden. Mithilfe der Risikoliste in Active IQ können Kunden gemeldete Konfigurationsfehler finden, die zu Problemen führen können oder Fehler erkennen, die gemeldet wurden und in denen Codversionen gepatcht wurden, die sie beheben können. Wenn Sie die Echtzeit-Dashboards auf der Cloud Insights-Startseite aufrufen, können Sie Muster der System-Performance erkennen, die einen frühen Hinweis auf ein Problem darstellen können und die schnelle Lösung dieses Problems ermöglichen. Und schließlich können Kunden durch die Möglichkeit, individuelle Dashboards zu erstellen, können sich auf die wichtigsten Ressourcen ihrer Infrastruktur konzentrieren und diese direkt überwachen, sodass sie ihre Business Continuity-Ziele erreichen können.

Storage-Optimierung

Es besteht nicht nur die Möglichkeit, die durch Cloud Insights erfassten Daten zu nutzen, um das ONTAP Storage-System zu optimieren, das in einer konvergenten FlexPod Datacenter-Infrastrukturlösung implementiert ist. Wenn ein Volume eine hohe Latenz aufweist, werden die Informationen auf dem Cloud Insights Dashboard angezeigt, da mehrere VMs mit hohen Performance-Anforderungen gemeinsam denselben Datenspeicher nutzen. Anhand dieser Informationen kann ein Storage-Administrator eine oder mehrere VMs entweder auf andere Volumes migrieren, Storage-Volumes zwischen Aggregaten oder zwischen Nodes im ONTAP Storage-System migrieren und so eine Umgebung mit Performance-Optimierung erzielen. Die Informationen, die durch die Integration von Active IQ und Cloud Insights erzielt werden, können Konfigurationsprobleme herausstellen, die zu einer schlechteren Performance führen, und die empfohlenen Korrekturmaßnahmen ermöglichen, die bei Implementierung mögliche Probleme beheben und ein optimal abgestimmtes Storage-System sicherstellen können.

Videos und Demos

Hier sehen Sie eine Videovorführung zur Verwendung von NetApp Cloud Insights zur Bewertung von Ressourcen in einer On-Premises-Umgebung "Hier".

Hier wird eine Videovorführung zur Überwachung der Infrastruktur mithilfe von NetApp Cloud Insights angezeigt und es werden Warnungsschwellenwerte für die Infrastruktur festgelegt "Hier".

Hier sehen Sie eine Videovorführung zur Verwendung von NetApp Cloud Insights zur bewerten einzelner Applikationen in der Umgebung "Hier".

Weitere Informationen

Auf den folgenden Websites finden Sie weitere Informationen zu den in diesem Dokument beschriebenen Daten:

- Cisco Produktdokumentation

  "https://www.cisco.com/c/en/us/support/index.html"

- FlexPod Datacenter

  "https://www.flexpod.com"

- NetApp Cloud Insights

  "https://cloud.netapp.com/cloud-insights"

- NetApp Produktdokumentation

  "https://docs.netapp.com"

FlexPod with FabricPool – Inactive Data Tiering in Amazon AWS S3

TR-4801: FlexPod mit FabricPool – Inactive Data Tiering in Amazon AWS S3

Scott Kovacs, NetApp

Flash-Storage-Preise fallen weiter und sind somit für Workloads und Applikationen verfügbar, die zuvor nicht in Betracht gezogen wurden. Eine möglichst effiziente Nutzung der Storage-Investitionen ist für IT-Manager jedoch nach wie vor von zentraler Bedeutung. IT-Abteilungen sehen sich immer noch gezwungen, leistungsstärkere Services mit nur geringen oder gar keinen Budgetzuteilungen bereitzustellen. Zur Erfüllung dieser Anforderungen können Sie mit NetApp FabricPool die Wirtschaftlichkeit der Cloud nutzen, indem Sie selten genutzte Daten aus teurem Flash-Storage vor Ort auf einen kostengünstigeren Storage-Tier in der Public Cloud verschieben. Das Verschieben selten genutzter Daten in die Cloud setzt wertvollen Flash-Storage auf AFF- oder FAS-Systemen frei, sodass geschäftskritische Workloads mehr Kapazität auf das hochperformante Flash-Tier bereitstellen können.

In diesem technischen Bericht wird die FabricPool Daten-Tiering-Funktion von NetApp ONTAP im Rahmen einer konvergenten FlexPod Infrastrukturarchitektur von NetApp und Cisco besprochen. Sie sollten mit der konvergenten Infrastrukturarchitektur für FlexPod Datacenter und der ONTAP Storage-Software vertraut sein, um die in diesem technischen Bericht vorgestellten Konzepte voll nutzen zu können. Da wir mit FlexPod und ONTAP vertraut sind, sprechen wir über FabricPool, seine Funktionsweise und seine Möglichkeiten zur effizienteren Nutzung von Flash-Storage vor Ort. Ein Großteil des Inhalts dieses Berichts wird unter ausführlicher behandelt "TR-4598 FabricPool Best Practices" Und anderer ONTAP Produktdokumentation zu bieten. Der Inhalt wurde für eine FlexPod Infrastruktur komprimiert und deckt nicht alle Anwendungsfälle für FabricPool ab. Alle analysierte Merkmale und Konzepte sind in ONTAP 9.6 erhältlich.

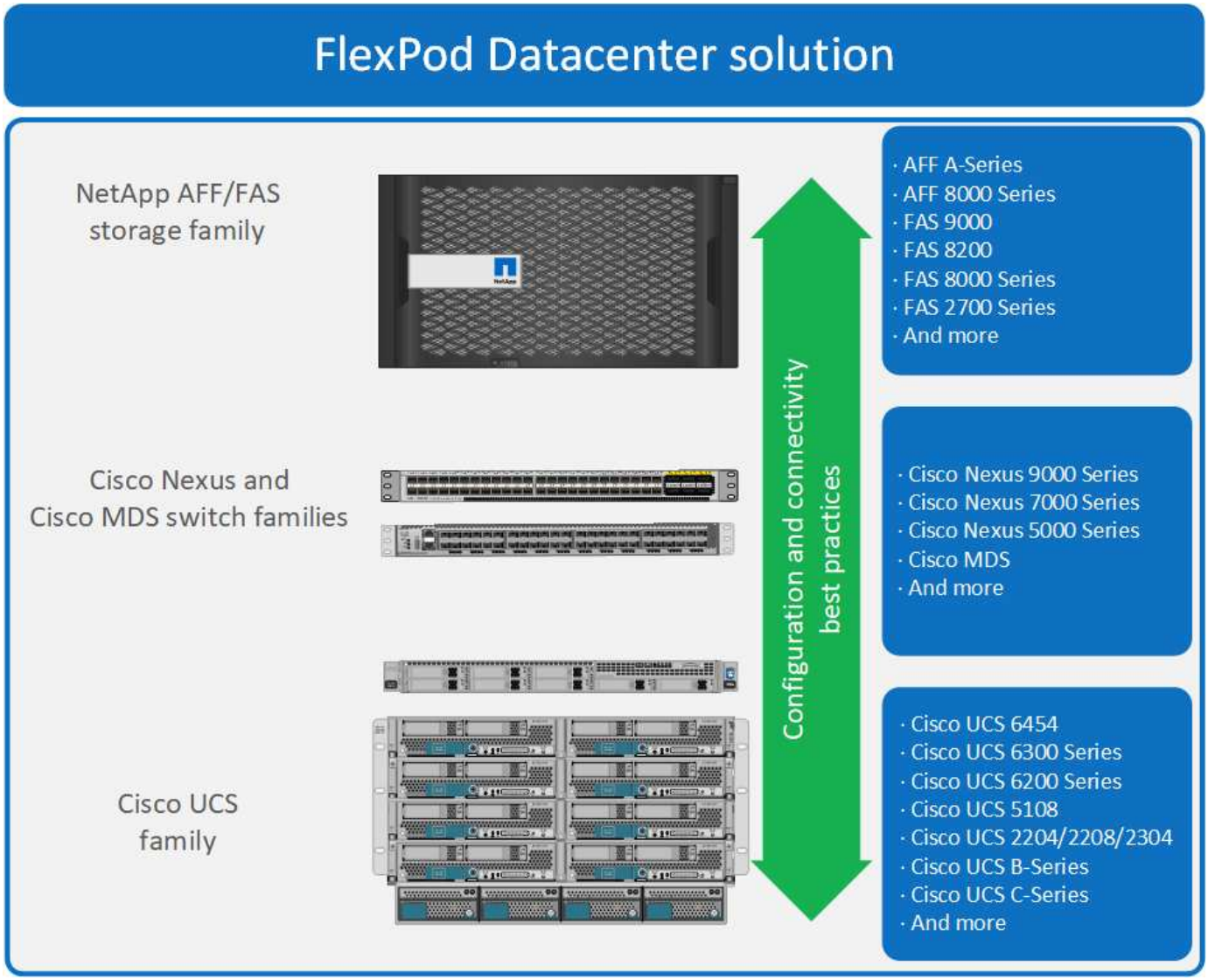
Weitere Informationen zu FlexPod finden Sie in "TR-4036 FlexPod Datacenter – Technische Spezifikationen".

Übersicht über FlexPod und Architektur

Übersicht über FlexPod

FlexPod ist eine definierte Gruppe von Hardware und Software und bildet eine integrierte Grundlage für virtualisierte und nicht virtualisierte Lösungen. FlexPod umfasst NetApp AFF Storage, Cisco Nexus Netzwerkkomponenten, Cisco MDS Storage-Netzwerk, das Cisco Unified Computing System (Cisco UCS) und VMware vSphere Software in einem einzigen Paket. Das Design ist flexibel genug, dass Netzwerk, Computing und Storage sich in ein Datacenter Rack einfügen oder nach dem Datacenter-Design des Kunden bereitgestellt werden können. Dank der Port-Dichte können die Netzwerkkomponenten mehrere Konfigurationen aufnehmen.

Ein Vorteil der FlexPod Architektur besteht in der Möglichkeit, die Umgebung an die Kundenanforderungen anzupassen bzw. flexibel zu gestalten. Eine FlexPod-Einheit kann problemlos nach Bedarf und nach Bedarf skaliert werden. Eine Einheit kann sowohl vertikal (Hinzufügen von Ressourcen zu einer FlexPod-Einheit) als auch horizontal (Hinzufügen weiterer FlexPod-Einheiten) skaliert werden. Die FlexPod Referenzarchitektur unterstreicht die Widerstandsfähigkeit, den Kostenvorteil und die einfache Implementierung einer Fibre Channel- und IP-basierten Storage-Lösung. Ein Storage-System, das mehrere Protokolle über eine einzige Benutzeroberfläche bereitstellt, eröffnet den Kunden die Wahl und schützt ihre Investitionen, da es sich um eine einmalig zu verkabelnde Architektur handelt. Die folgende Abbildung zeigt viele der Hardwarekomponenten von FlexPod.

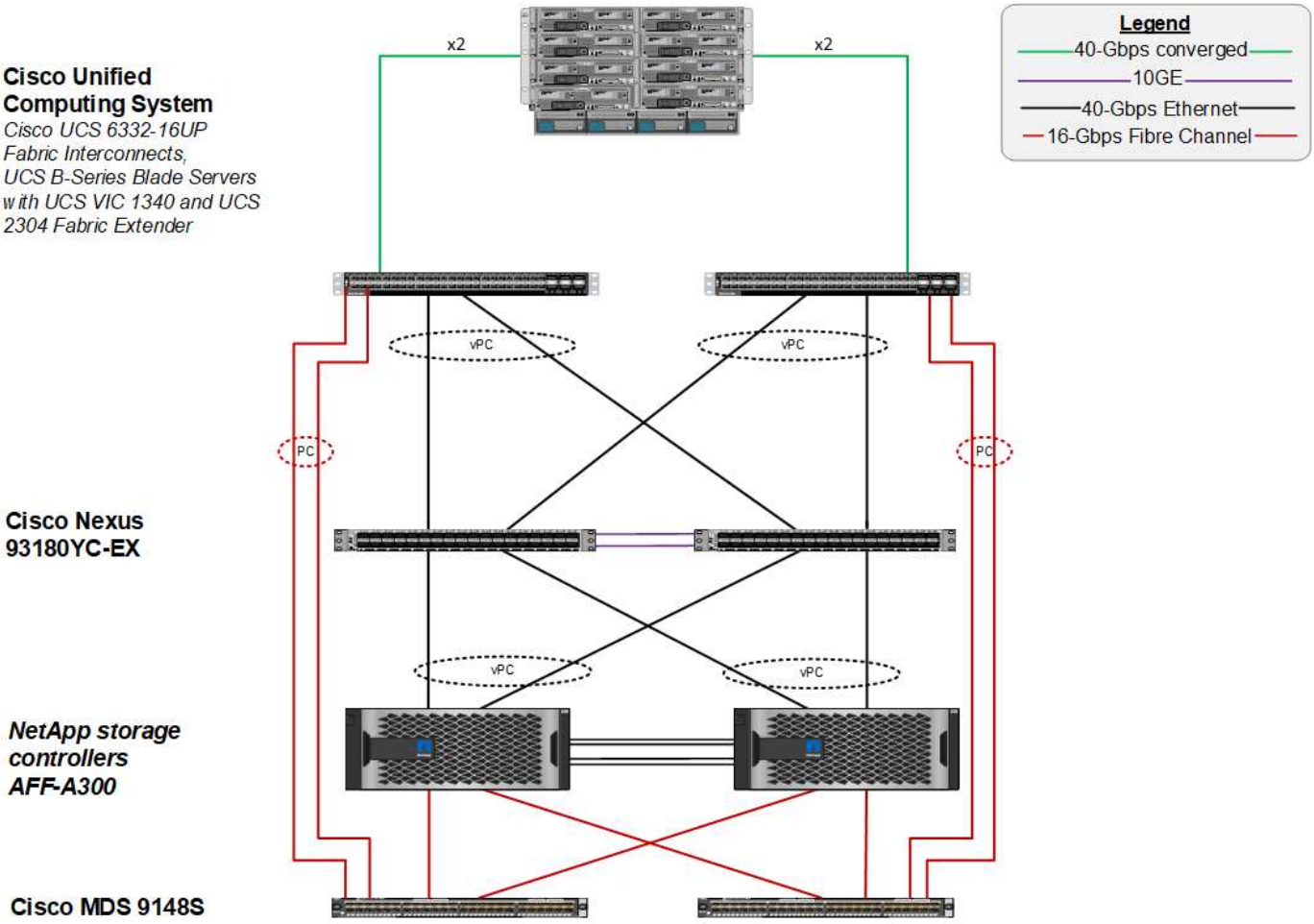


Architektur von FlexPod

Die folgende Abbildung zeigt die Komponenten einer VMware vSphere und FlexPod Lösung und die für Cisco UCS 6454 Fabric Interconnects erforderlichen Netzwerkverbindungen. Dieses Design umfasst die folgenden Komponenten:

- Port-gechannelte 40-Gbit-Ethernet-Verbindungen zwischen dem Cisco UCS 5108 Blade-Chassis und den Cisco UCS Fabric Interconnects
- 40-GB-Ethernet-Verbindung zwischen dem Cisco UCS Fabric Interconnect und dem Cisco Nexus 9000
- 40-GB-Ethernet-Verbindung zwischen dem Cisco Nesxus 9000 und dem NetApp AFF A300 Storage-Array

Diese Infrastrukturoptionen wurden durch die Einführung von Cisco MDS Switches zwischen dem Cisco UCS Fabric Interconnect und der NetApp AFF A300 erweitert. Diese Konfiguration bietet über FC gestartete Hosts mit 16-GB-FC-Zugriff auf Shared Storage auf Blockebene. Die Referenzarchitektur unterstreicht die einmalig zu verkabelnde Strategie, da die Host-Hosts über das Cisco UCS Fabric Interconnect keine Neuablerung benötigen, da die Architektur um zusätzlichen Storage erweitert wird.



FabricPool

Übersicht über FabricPool

FabricPool ist eine Hybrid-Storage-Lösung in ONTAP mit einem All-Flash-Aggregat (SSD) als Performance-Tier und einem Objektspeicher in einem Public-Cloud-Service als Cloud-Tier. Diese Konfiguration ermöglicht richtlinienbasierte Datenverschiebung, je nachdem, ob häufig auf Daten zugegriffen wird. FabricPool wird in ONTAP sowohl für AFF- als auch für rein SSD-basierte Aggregate auf den FAS Plattformen unterstützt. Die Datenverarbeitung erfolgt auf Blockebene, wobei häufig abgerufene Datenblöcke in der All-Flash-Performance-Tier mit als „heiße“ und selten genutzte Blöcke gekennzeichnet sind.

Mit FabricPool können Sie die Storage-Kosten senken, ohne dabei auf Performance, Effizienz, Sicherheit oder Schutz verzichten zu müssen. FabricPool ist transparent für Enterprise-Applikationen und nutzt Cloud-Effizienz durch niedrigere Storage-TCO, ohne dass der Aufbau der Applikationsinfrastruktur umgestaltet werden muss.

FlexPod bietet die Storage Tiering-Funktionen von FabricPool für eine effizientere Nutzung von ONTAP Flash Storage. Inaktive Virtual Machines (VMs), selten genutzte VM-Vorlagen und VM-Backups von NetApp SnapCenter für vSphere können wertvollen Speicherplatz im Datastore-Volume belegen. Durch das Verschieben selten genutzter Daten in die Cloud-Tier werden Speicherplatz und Ressourcen für hochperformante, geschäftskritische Applikationen freigegeben, die in der FlexPod-Infrastruktur gehostet werden.

Die Fibre Channel- und iSCSI-Protokolle dauern im Allgemeinen länger, bevor eine Zeitüberschreitung von 60 bis 120 Sekunden auftritt. Sie versuchen jedoch nicht, eine Verbindung auf die gleiche Weise einzurichten, wie es die NAS-Protokolle tun. Wenn ein SAN-Protokoll nicht mehr verfügbar ist, muss die Anwendung neu gestartet werden. Selbst eine kurze Störung kann verheerende Folgen für Produktionsapplikationen mit SAN-Protokollen haben, da keine Möglichkeit besteht, die Verbindung mit öffentlichen Clouds zu garantieren. Um dieses Problem zu vermeiden, empfiehlt NetApp die Verwendung von Private Clouds beim Tiering von Daten, auf die SAN-Protokolle zugreifen.

In ONTAP 9.6 lässt sich FabricPool mit allen wichtigen Public-Cloud-Providern integrieren: Alibaba Cloud Object Storage Service, Amazon AWS S3, Google Cloud Storage, IBM Cloud Object Storage und Microsoft Azure Blob Storage. In diesem Bericht wird der Schwerpunkt auf Amazon AWS S3 Storage als Cloud-Objekt-Tier der Wahl gelegt.

Das zusammengesetzte Aggregat

Eine FabricPool Instanz wird erstellt, indem ein ONTAP Flash-Aggregat mit einem Cloud-Objektspeicher wie einem AWS S3-Bucket verknüpft wird, um ein gruppiertes Aggregat zu erstellen. Wenn Volumes innerhalb des zusammengesetzten Aggregats erstellt werden, können sie die Tiering-Funktionen von FabricPool nutzen. Wenn Daten auf das Volume geschrieben werden, weist ONTAP jedem der Datenblöcke eine Temperatur zu. Wird der Block zum ersten Mal geschrieben, wird ihm die Temperatur „heiß“ zugewiesen. Im Verlauf der Zeit wird bei nicht abgerufenen Daten ein Kühlvorgang durchlaufen, bis dieser schließlich einem „kalten“ Status zugewiesen wird. Diese selten genutzten Datenblöcke werden dann vom Performance-SSD-Aggregat und in den Cloud-Objektspeicher verschoben.

Die Zeitspanne zwischen dem „Kaltstart“ und dem Verschieben in den Cloud-Objektspeicher wird durch die Volume-Tiering-Richtlinie in ONTAP geändert. Weitere Granularität wird durch Ändern der ONTAP-Einstellungen erreicht, die die Anzahl der Tage, die für einen Block „kalt“ werden, steuern. Kandidaten für Daten-Tiering sind herkömmliche Volume-Snapshots, SnapCenter für vSphere VM-Backups und andere Snapshot-basierte Backups von NetApp und alle unregelmäßig genutzten Blöcke in einem vSphere Datastore, z. B. VM-Vorlagen und selten verwendete VM-Daten.

Berichterstellung für inaktive Daten

In ONTAP steht die Berichterstellung für inaktive Daten (Inactive Data Reporting, IDR) zur Verfügung. Dies unterstützt Sie bei der Bewertung der Menge an kalten Daten, die von einem Aggregat verteilt werden können. IDR ist in ONTAP 9.6 standardmäßig aktiviert und verwendet eine standardmäßige Kühlrichtlinie für 31 Tage, um zu bestimmen, welche Daten im Volume inaktiv sind.

Die Menge der „kalten“ Daten in Tier hängt von den Tiering-Richtlinien ab, die für das Volume festgelegt sind. Diese Menge kann sich von der Menge der kalten Daten unterscheiden, die von IDR unter Verwendung der standardmäßigen 31-Tage-Kühldauer erkannt wurden.

Erstellen von Objekten und Verschieben von Daten

FabricPool arbeitet auf Blockebene von NetApp WAFL, wobei Kühlblöcke, sie in Storage-Objekte verketten und diese Objekte auf eine Cloud-Tier migrieren. Jedes FabricPool Objekt hat 4 MB und besteht aus 1,024 4-KB-Blöcken. Die Objektgröße wurde auf 4 MB festgelegt, basierend auf Performance-Empfehlungen führender Cloud-Provider und kann nicht geändert werden. Wenn „kalte“ Blöcke gelesen und wieder „heiß“ werden, werden nur die angeforderten Blöcke im 4-MB-Objekt abgerufen und zurück zur Performance-Tier verschoben. Weder das gesamte Objekt noch die gesamte Datei werden zurückmigriert. Es werden nur die erforderlichen Blöcke migriert.

Wenn ONTAP eine Möglichkeit für sequenzielle Leseköpfe erkennt, fordert die IT Blöcke aus dem Cloud-Tier an, bevor sie gelesen werden, um die Performance zu verbessern.

Daten werden standardmäßig nur dann in den Cloud-Tier verschoben, wenn das Performance-Aggregat zu mehr als 50 % genutzt wird. Dieser Schwellenwert kann auf einen niedrigeren Prozentsatz festgelegt werden, um eine kleinere Menge an Daten-Storage auf dem Flash-Tier mit der Performance in die Cloud zu verschieben. Dies könnte nützlich sein, wenn die Tiering-Strategie dazu dient, nur kalte Daten zu verschieben, wenn sich das Aggregat der Kapazität nähert.

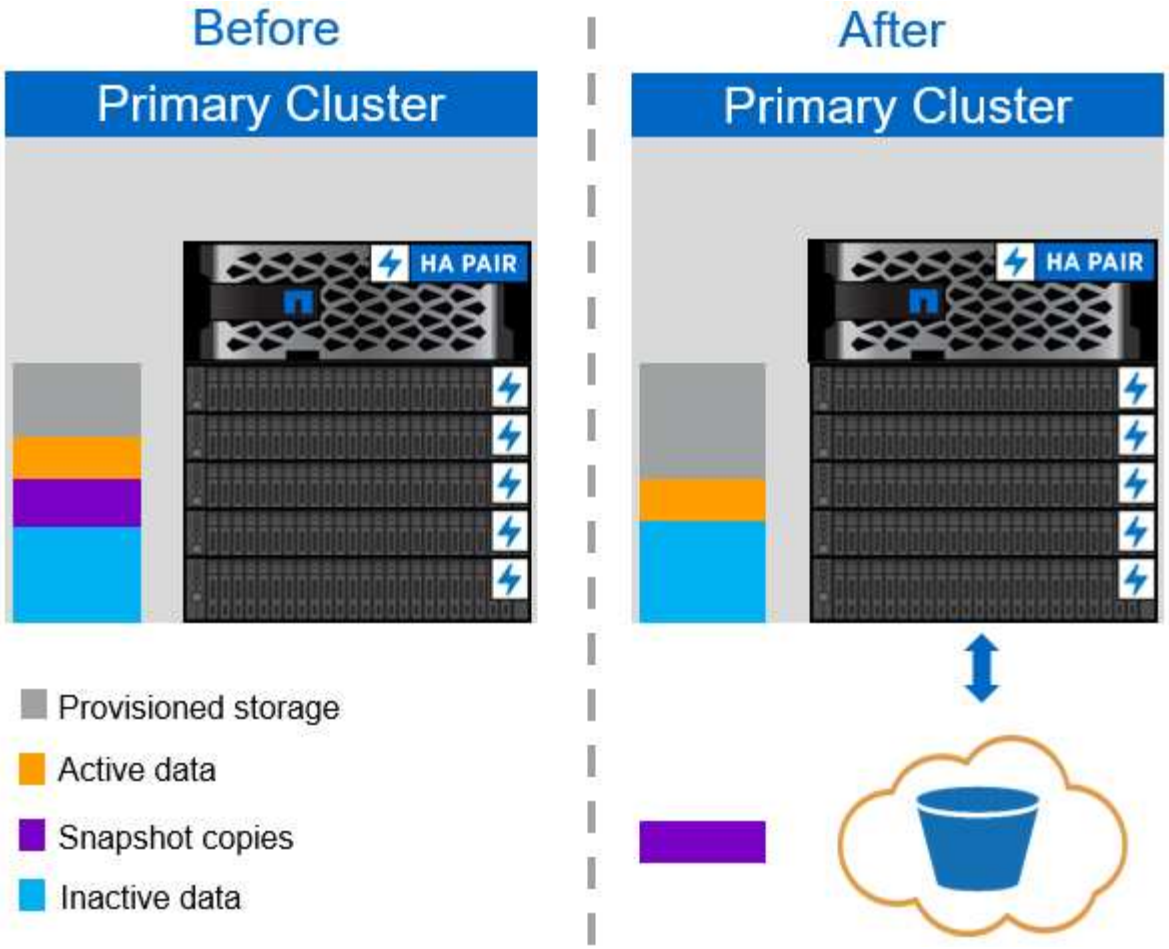
Wenn die Performance-Tier-Auslastung bei einer Kapazität von mehr als 70 % liegt, werden kalte Daten direkt aus der Cloud-Tier gelesen, ohne zurück in die Performance-Tier geschrieben zu werden. Durch Verhinderung von Datenschreibbacks auf stark ausgelasteten Aggregaten erhält FabricPool das Aggregat für aktive Daten aufrecht.

Performance-Tier-Speicherplatz zurückgewinnen

Wie bereits erwähnt, besteht der primäre Anwendungsfall für FabricPool darin, hochperformante On-Premises-Flash-Storage am effizientesten zu nutzen. „Kalte“ Daten in Form von Volume-Snapshots und VM-Backups der virtuellen FlexPod Infrastruktur beanspruchen unter kann viel teuren Flash-Storage. Wertvolle Performance-Tiered Storage kann durch die Implementierung von zwei Tiering-Richtlinien freigegeben werden: Nur Snapshot oder Auto.

Richtlinie für ausschließlich Snapshot-Tiering

Mit der in der folgenden Abbildung gezeigten Richtlinie zum ausschließlich Snapshot Tiering werden Snapshot Daten für kalte Volumes und SnapCenter für vSphere Backups von VMs, die Speicherplatz belegen, aber keine Blöcke gemeinsam mit dem aktiven Filesystem an einen Cloud-Objektspeicher freigeben. Die reine Snapshot-Tiering-Richtlinie verschiebt selten genutzte Datenblöcke auf die Cloud-Tier. Wenn eine Wiederherstellung erforderlich ist, werden kalte Blöcke in der Cloud als „heiße“ und zurück in das Flash-Tier mit der Performance vor Ort verschoben.

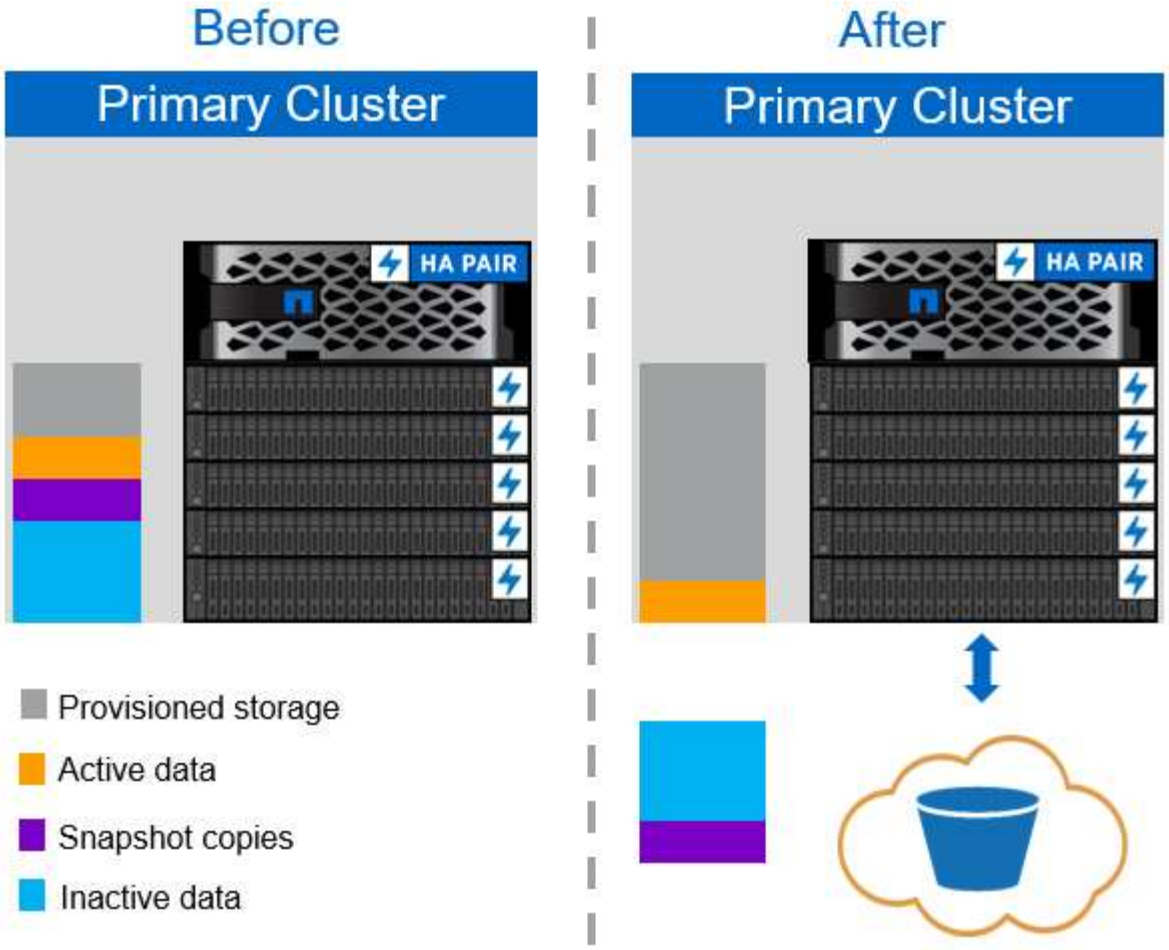


Automatisches Tiering

Die in der folgenden Abbildung dargestellte FabricPool Auto Tiering-Richtlinie verschiebt nicht nur kalte Snapshot Datenblöcke in die Cloud, sondern auch alle kalten Blöcke im aktiven Filesystem. Dies kann VM-Vorlagen und sämtliche nicht verwendeten VM-Daten im Datastore Volume enthalten. Welche kalten Blöcke bewegt werden, wird vom gesteuert `tiering-minimum-cooling-days` Einstellung für die Lautstärke. Wenn kalte Blöcke im Cloud-Tier von einer Applikation zufällig gelesen werden, werden diese Blöcke „heiß“ gemacht und zurück auf die Performance-Tier gebracht. Wenn jedoch kalte Blöcke durch einen sequenziellen Prozess wie einen Virenschutzscanner gelesen werden, bleiben die Blöcke im Cloud-Objektspeicher erhalten und bleiben erhalten. Sie werden nicht zurück auf die Performance-Tier verschoben.

Bei Verwendung der Auto-Tiering-Richtlinie werden Blöcke, auf die selten zugegriffen wird, mit denen die Daten häufig abgerufen werden, von der Cloud-Tier mit der Geschwindigkeit der Cloud-Konnektivität zurückgeholt. Dies kann sich auf die VM-Performance auswirken, wenn die Applikation latenzempfindlich ist. Dies sollte vor der Verwendung der Auto-Tiering-Richtlinie für den Datastore in Betracht gezogen werden. NetApp empfiehlt, LIFs über Ports mit einer Geschwindigkeit von 10 GbE zu aktivieren, um eine ausreichende Performance zu erzielen.

Der Objektspeicher-Profiler sollte verwendet werden, um die Latenz und den Durchsatz beim Objektspeicher zu testen, bevor sie an ein FabricPool Aggregat angehängt werden.



Alle Tiering-Richtlinien

Im Gegensatz zu den reinen Snapshot- und Auto-Richtlinien werden bei der All-Tiering-Richtlinie ganze Datenvolumen sofort in die Cloud-Tier verschoben. Diese Richtlinie eignet sich am besten für sekundäre Datensicherungs- oder Archivierungs-Volumes, für die Daten zwar zu historischen oder gesetzlichen Zwecken aufbewahrt werden müssen, aber nur selten benötigt werden. Die Richtlinie „Alle“ wird für VMware Datastore Volumes nicht empfohlen, da alle in den Datastore geschriebenen Daten sofort in die Cloud-Tier verschoben werden. Nachfolgende Lesezugriffe werden aus der Cloud durchgeführt und können möglicherweise zu Performance-Problemen für VMs und Applikationen im Datastore Volume führen.

Sicherheit

Die Sicherheit spielt für die Cloud und für FabricPool eine zentrale Rolle. Alle nativen Sicherheitsfunktionen von ONTAP werden in der Performance-Tier unterstützt und das Verschieben von Daten ist bei der Übertragung in die Cloud-Tier sicher. FabricPool verwendet das "AES-256-GCM" Der Verschlüsselungsalgorithmus auf der Performance-Tier bleibt über eine End-to-End-Verschlüsselung in der Cloud-Tier erhalten. Datenblöcke, die in den Cloud-Objektspeicher verschoben werden, sind mit TLS (Transport Layer Security) v1.2 gesichert, um die Datenvertraulichkeit und -Integrität zwischen Storage Tiers zu wahren.

Die Kommunikation mit dem Cloud-Objektspeicher über eine unverschlüsselte Verbindung wird von NetApp unterstützt, wird aber nicht empfohlen.

Datenverschlüsselung

Die Datenverschlüsselung ist entscheidend für den Schutz geistigen Eigentums, Handelsinformationen und persönlich identifizierbare Kundeninformationen. FabricPool unterstützt sowohl NetApp Volume Encryption (NVE) als auch NetApp Storage Encryption (NSE) vollständig, um bestehende Datensicherungsstrategien zu beibehalten. Alle verschlüsselten Daten auf der Performance-Tier bleiben beim Verschieben in die Cloud-Tier verschlüsselt. Die Client-seitige Verschlüsselung befindet sich im Eigentum von ONTAP, und die serverseitigen Objektspeicherschlüssel sind im Eigentum des jeweiligen Cloud-Objektspeichers. Nicht mit NVE verschlüsselte Daten werden über den AES-256-GCM-Algorithmus verschlüsselt. Keine anderen AES-256-Chiffren werden unterstützt.

Die Verwendung von NSE oder NVE ist optional und muss nicht FabricPool verwenden.

FabricPool-Anforderungen erfüllt

FabricPool erfordert ONTAP 9.2 oder höher und die Verwendung von SSD-Aggregaten auf allen in diesem Abschnitt aufgeführten Plattformen. Zusätzliche FabricPool-Anforderungen hängen von dem Cloud-Tier ab, der angehängt wird. Bei AFF-Plattformen der Einstiegsklasse mit relativ geringer Kapazität wie der NetApp AFF C190 ist FabricPool besonders effektiv, um inaktive Daten auf die Cloud-Tier zu verschieben.

Plattformen

FabricPool wird auf folgenden Plattformen unterstützt:

- NetApp AFF
  - A800
  - A700S, A700
  - A320, A300
  - A220, A200
  - C190
  - AFF8080, AFF8060 UND AFF8040
- NetApp FAS
  - FAS9000
  - FAS8200
  - FAS8080, FAS8060 UND FAS8040
  - FAS2750, FAS2720
  - FAS2650, FAS2620

Nur SSD-Aggregate auf FAS Plattformen können FabricPool verwenden.

- Cloud-Tiers
  - Alibaba Cloud Objekt-Storage-Service (Standard, Infrequent Access)
  - Amazon S3 (Standard, Standard-IA, One Zone-IA, Intelligent Tiering)
  - Kommerzielle Amazon Cloud Services (C2S)

- Google Cloud Storage (Regional, Regional, Nearline, Coldline)
- IBM Cloud Objekt-Storage (Standard, Vault, Cold Vault, Flex)
- Microsoft Azure Blob Storage (Hot und Cool)

Intercluster LIFs

Cluster-HA-Paare (High Availability, Hochverfügbarkeit), die FabricPool verwenden, erfordern zur Kommunikation mit der Cloud-Tier zwei Cluster-übergreifende logische Schnittstellen (LIFs). NetApp empfiehlt die Erstellung einer Intercluster-LIF auf zusätzlichen HA-Paaren, um auch Aggregate auf diesen Nodes nahtlos mit Cloud-Tiers verbinden zu können.

Die logische Schnittstelle, die ONTAP für die Verbindung mit dem AWS S3 Objektspeicher verwendet, muss sich auf einem 10-Gbit/s-Port beziehen.

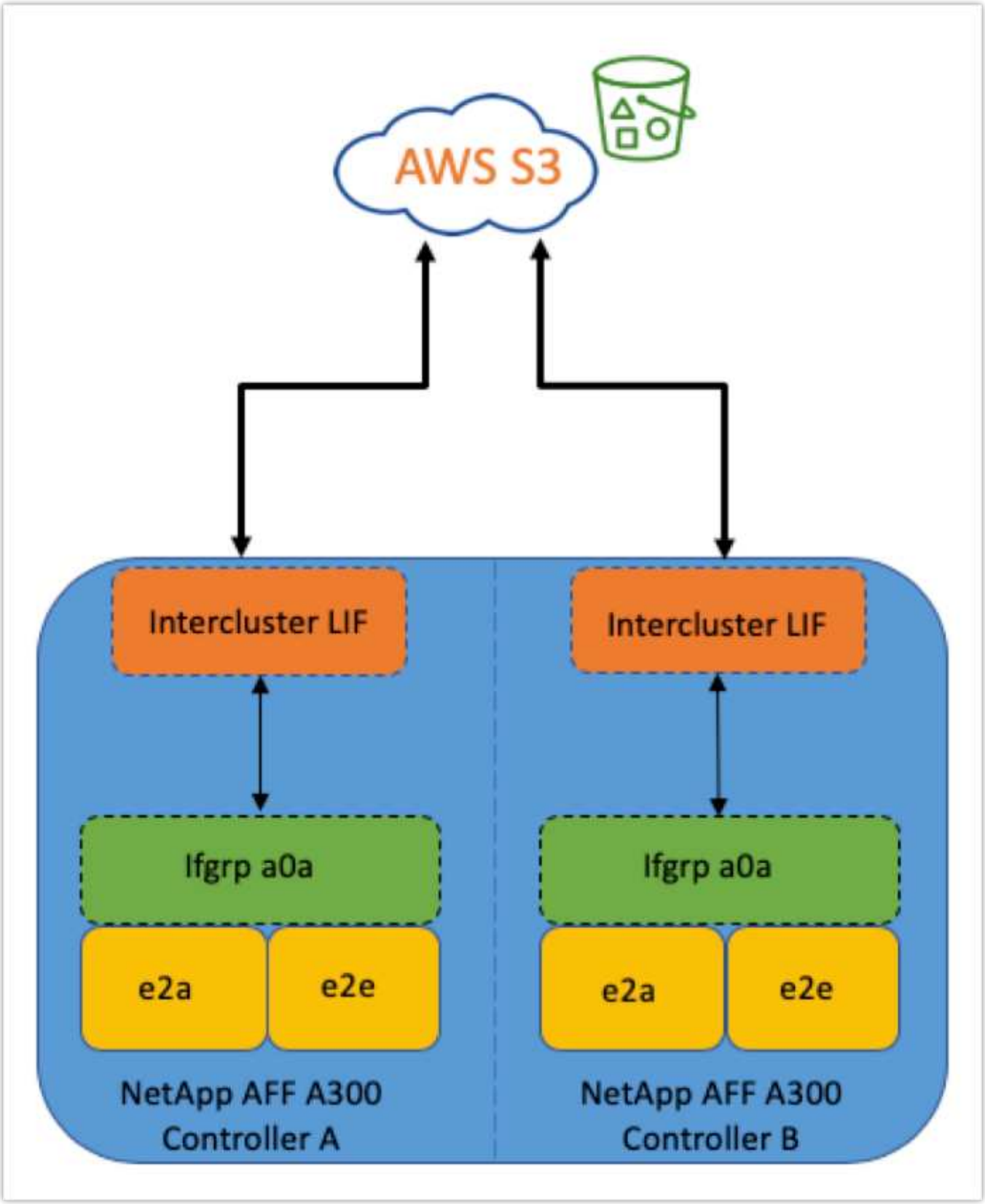
Wenn mehr als eine Intercluser LIF auf einem Node mit unterschiedlichem Routing verwendet wird, empfiehlt NetApp, sie in verschiedenen IPspaces zu platzieren. Während der Konfiguration kann FabricPool aus mehreren IPspaces auswählen, es ist jedoch nicht in der Lage, bestimmte Intercluster LIFs innerhalb eines IPspaces auszuwählen.

Durch das Deaktivieren oder Löschen einer Intercluster-LIF wird die Kommunikation mit der Cloud-Ebene unterbrochen.

Konnektivität

Die FabricPool Leselatenz ist eine Funktion der Verbindung zum Cloud-Tier. Intercluster-LIFs mit 10-Gbit/s-Ports, dargestellt in der folgenden Abbildung, sorgen für eine angemessene Performance. NetApp empfiehlt, die Latenz und den Durchsatz der spezifischen Netzwerkumgebung zu validieren, um die Auswirkungen auf die FabricPool-Performance zu bestimmen.

Beim Einsatz von FabricPool in hochperformanten Umgebungen müssen weiterhin minimale Performance-Anforderungen für Client-Applikationen eingehalten werden, und die Recovery-Zeitvorgaben sollten entsprechend angepasst werden.



Objektspeicher-Profiler

Der Objektspeicher-Profiler, ein Beispiel aus dem folgenden Bild gezeigt und über die ONTAP CLI verfügbar ist, testet die Latenz und Durchsatz-Performance von Objektspeichern, bevor sie mit einem FabricPool Aggregat verbunden sind.

Das Cloud-Tier muss ONTAP hinzugefügt werden, bevor es mit dem Objektspeicher-Profiler verwendet werden kann.

Starten Sie den Objektspeicher-Profiler im erweiterten Berechtigungsmodus in ONTAP mit dem folgenden Befehl:

```
storage aggregate object-store profiler start -object-store-name <name>
-node <name>
```

Um die Ergebnisse anzuzeigen, führen Sie den folgenden Befehl aus:

```
storage aggregate object-store profiler show
```

Cloud-Tiers bieten keine Performance ähnlich wie bei der Performance-Tier (normalerweise GB pro Sekunde). Obwohl FabricPool Aggregate problemlos SATA-ähnliche Performance bieten, sind sie für Tiering-Lösungen, die keine SATA-ähnliche Performance benötigen, auch Latenzzeiten von bis zu 10 Sekunden und einen niedrigen Durchsatz tolerierbar.

```
bb09-a300-2::*> storage aggregate object-store profiler show
Object store config name: aws_infra_fp_bk_1
Node name: bb09-a300-2-1
Status: Active. Issuing GETs
Start time: 10/3/2019 12:37:24

Op      Size       Total     Failed            Latency(ms)          Throughput
                                          min       max       avg
-------------------------------------------------------------------------------
PUT     4MB        1084      0         336       5951      2817     69.55MB
GET     4KB        158636    0         27        1132      41       32.22MB
GET     8KB        0         0         0         0         0        0B
GET     32KB       0         0         0         0         0        0B
GET     256KB      0         0         0         0         0        0B
5 entries were displayed.
```

Volumes

Storage Thin Provisioning ist eine Standardpraxis für den Administrator der virtuellen FlexPod Infrastruktur. Die NetApp Virtual Storage Console (VSC) stellt Storage Volumes für VMware Datastores ohne Speicherplatzzusage (Thin Provisioning) und mit optimierten Einstellungen zur Storage-Effizienz gemäß NetApp Best Practices bereit. Wenn VSC zur Erstellung von VMware Datastores verwendet wird, müssen keine weiteren Maßnahmen ergriffen werden, da dem Datastore Volume keine Speicherplatzzusagen zugewiesen werden sollten.

FabricPool kann eine Cloud-Schicht nicht an ein Aggregat anhängen, das Volumes mit einer anderen Speicherplatzgarantie als „Keine“ enthält (z. B. Volume).

```
volume modify -space-guarantee none
```

Einstellen des `space-guarantee none` Der Parameter liefert Thin Provisioning für das Volume. Der von Volumes mit diesem Garantietyp verbrauchte Speicherplatz wächst mit, wenn Daten hinzugefügt werden, anstatt durch die anfängliche Volume-Größe bestimmt zu werden. Dieser Ansatz ist für FabricPool unverzichtbar, da das Volume über Cloud-Tiering-Daten verfügen muss, die häufig aufgerufen werden und wieder auf die Performance-Tier verlagert werden.

Lizenzierung

FabricPool erfordert eine kapazitätsbasierte Lizenz, wenn Objekt-Storage-Provider (z. B. Amazon S3) als Cloud-Tier für AFF und FAS Hybrid-Flash-Systeme angeschlossen werden können.

FabricPool Lizenzen sind im unbefristeten oder langfristigen Format (1 Jahr oder 3 Jahre) verfügbar.

Tiering in das Cloud-Tier stoppt, wenn die auf dem Cloud-Tier gespeicherten Datenmengen (genutzte Kapazität) die lizenzierte Kapazität erreichen. Zusätzliche Daten, einschließlich SnapMirror Kopien auf Volumes mit der All-Tiering-Richtlinie, können erst abgestuft werden, wenn die Lizenzkapazität erhöht wird. Obwohl das Tiering unterbrochen wird, sind die Daten trotzdem über das Cloud-Tier zugänglich. Zusätzliche „kalte“ Daten bleiben auf SSDs, bis die lizenzierte Kapazität erhöht wird.

Eine kostenlose 10-TB-Kapazität, die term-basierte FabricPool Lizenz ist beim Kauf eines neuen ONTAP 9.5 oder höheren Clusters enthalten. Unter Umständen fallen zusätzliche Support-Kosten an. FabricPool Lizenzen (einschließlich zusätzlicher Kapazität für vorhandene Lizenzen) können in 1-TB-Schritten erworben werden.

Eine FabricPool Lizenz kann nur aus einem Cluster gelöscht werden, das keine FabricPool-Aggregate enthält.

FabricPool Lizenzen gelten für das gesamte Cluster. Beim Erwerb einer Lizenz sollten Sie die UUID zur Verfügung haben (`cluster identify show`). Weitere Informationen zur Lizenzierung finden Sie im "NetApp Knowledge Base".

Konfiguration

Software-Versionen

Die folgende Tabelle zeigt validierte Hardware- und Software-Versionen.

Schicht	Gerät	Bild	Kommentare
Storage	NetApp AFF A300	ONTAP 9.6P2	
Computing	Cisco UCS B200 M5 Blade Server mit Cisco UCS VIC 1340	Version 4.0(4b)	
Netzwerk	Cisco Nexus 6332-16UP Fabric Interconnect	Version 4.0(4b)	
	Cisco Nexus 93180YC-EX Switch im Standalone-Modus mit NX-OS	Version 7.0(3)I7(6)	
Datennetzwerk Storage-Netzwerk	Cisco MDS 9148S	Version 8.3(2)	

Schicht	Gerät	Bild	Kommentare
Hypervisor		VMware vSphere ESXi 6.7U2	ESXi 6.7.0,13006603
		VMware vCenter Server	VCenter Server 6.7.0.30000, Build 13639309
Cloud-Provider		Amazon AWS S3	Standard-S3-Bucket mit Standardoptionen

Die grundlegenden Anforderungen für FabricPool sind in beschrieben "FabricPool-Anforderungen erfüllt". Nachdem alle grundlegenden Anforderungen erfüllt sind, gehen Sie zur Konfiguration von FabricPool wie folgt vor:

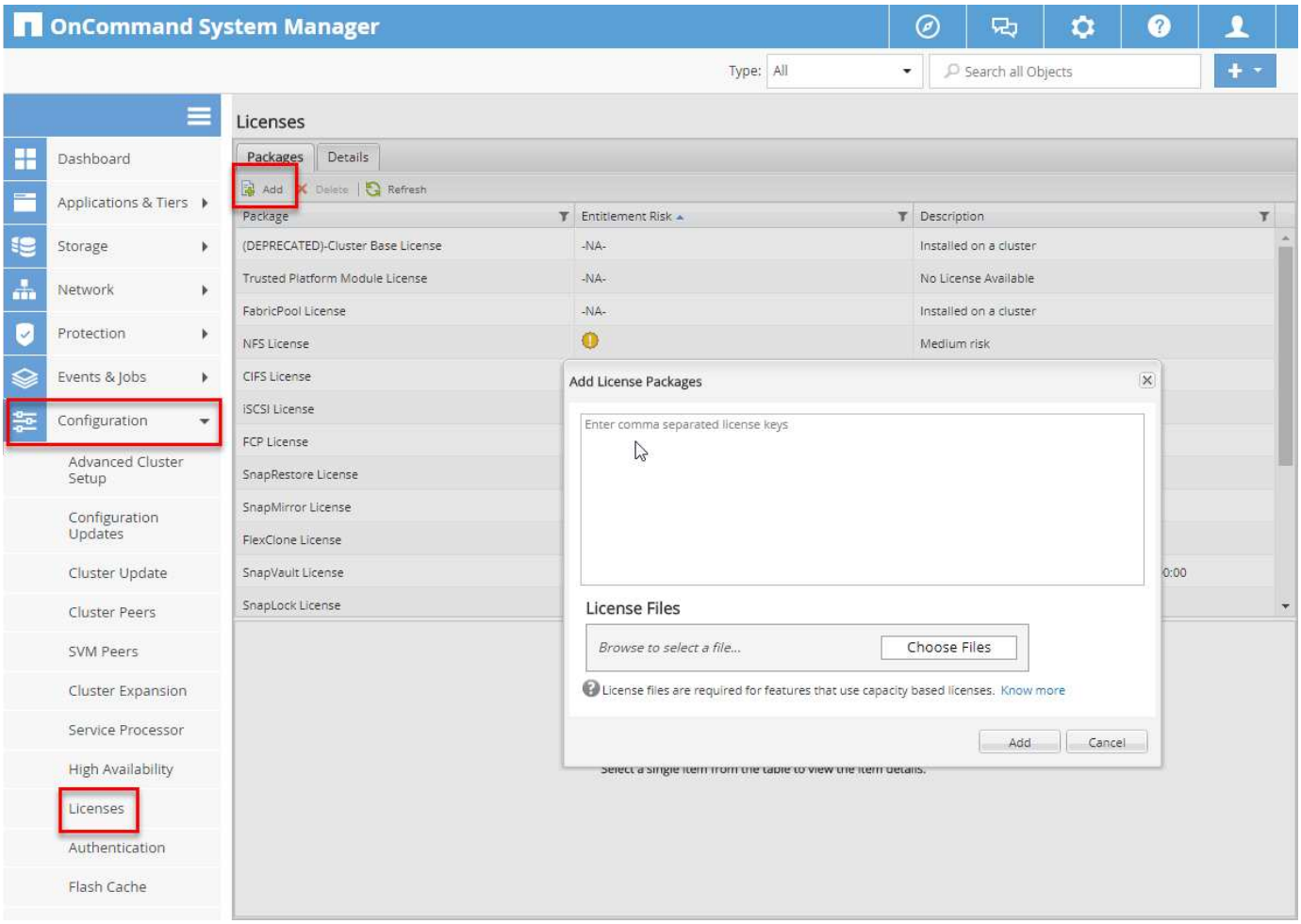
1. Installieren Sie eine FabricPool Lizenz.
2. Erstellen eines AWS S3-Objektspeicher-Buckets
3. Hinzufügen einer Cloud-Tier zu ONTAP
4. Verbinden Sie die Cloud-Tier mit einem Aggregat.
5. Legen Sie die Tiering-Richtlinie für Volumes fest.

"Als Nächstes: Lizenz für FabricPool installieren."

Installieren Sie die FabricPool Lizenz

Nachdem Sie eine NetApp Lizenzdatei erworben haben, können Sie sie mit dem OnCommand System Manager installieren. Gehen Sie wie folgt vor, um die Lizenzdatei zu installieren:

1. Klicken Sie Auf Konfigurationen.
2. Klicken Sie Auf Cluster.
3. Klicken Sie Auf Lizenzen.
4. Klicken Sie Auf Hinzufügen.
5. Klicken Sie auf Dateien auswählen, um eine Datei zu durchsuchen und auszuwählen.
6. Klicken Sie Auf Hinzufügen.



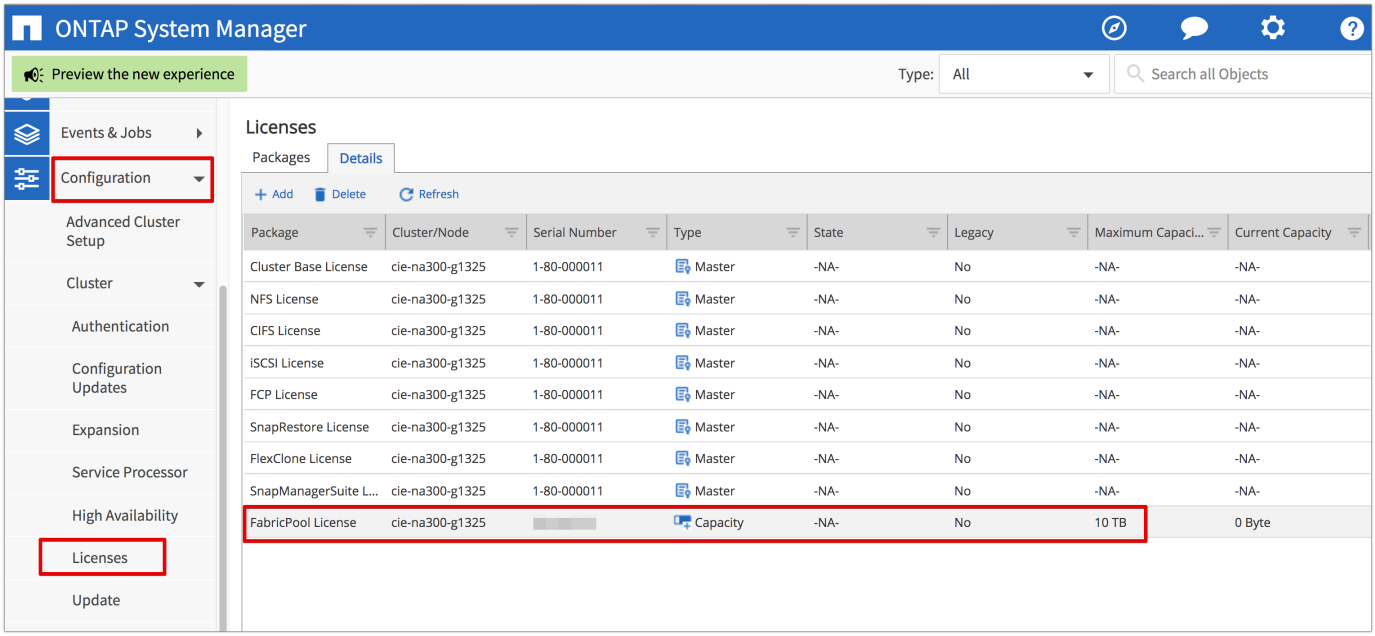
Lizenzkapazität

Sie können die Lizenzkapazität entweder mit der ONTAP CLI oder mit OnCommand System Manager anzeigen. Führen Sie zum Anzeigen der lizenzierten Kapazität den folgenden Befehl in der ONTAP CLI aus:

```
system license show-status
```

Führen Sie in OnCommand System Manager die folgenden Schritte aus:

1. Klicken Sie Auf Konfigurationen.
2. Klicken Sie Auf Lizenzen.
3. Klicken Sie auf die Registerkarte Details.



Die maximale Kapazität und die aktuelle Kapazität sind in der Zeile FabricPool-Lizenz aufgeführt.

"Als Nächstes: AWS S3-Bucket erstellen"

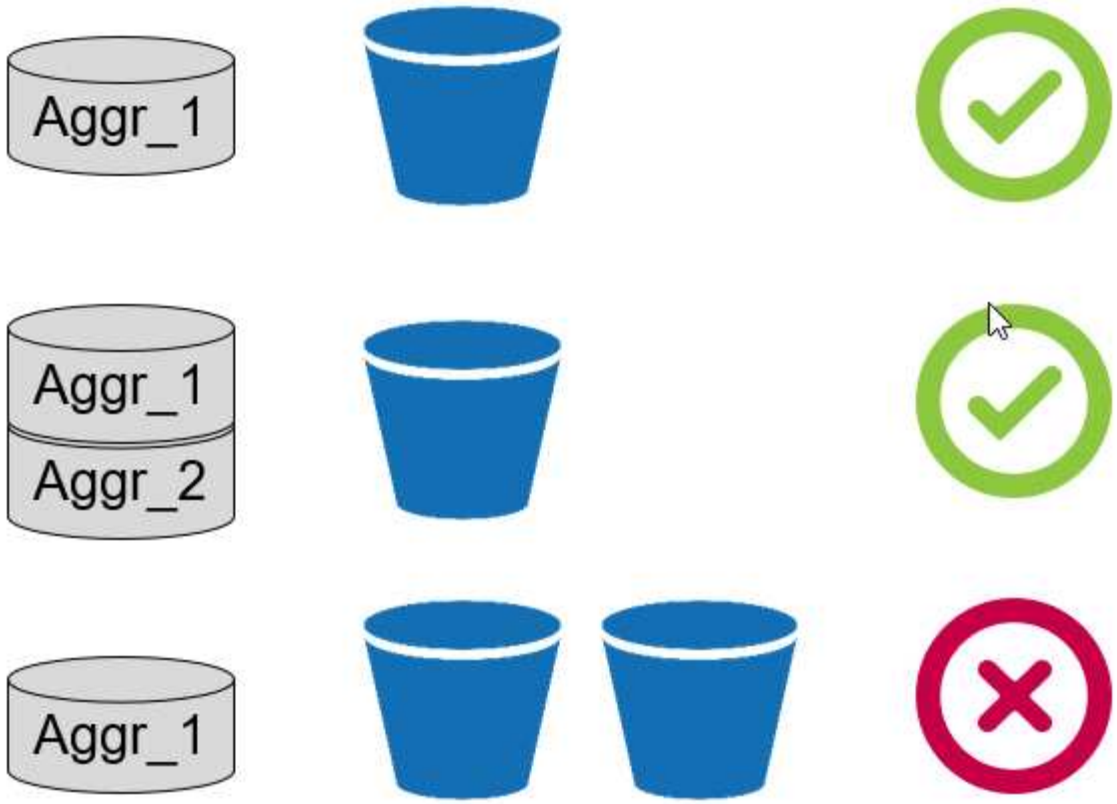
AWS S3 Bucket erstellen

Buckets sind Objektspeicher-Container, in denen Daten gespeichert sind. Name und Speicherort des Buckets, in dem Daten gespeichert werden, müssen angegeben werden, bevor sie zu einem Aggregat als Cloud-Tier hinzugefügt werden können.

Buckets können nicht mit OnCommand System Manager, OnCommand Unified Manager oder ONTAP erstellt werden.

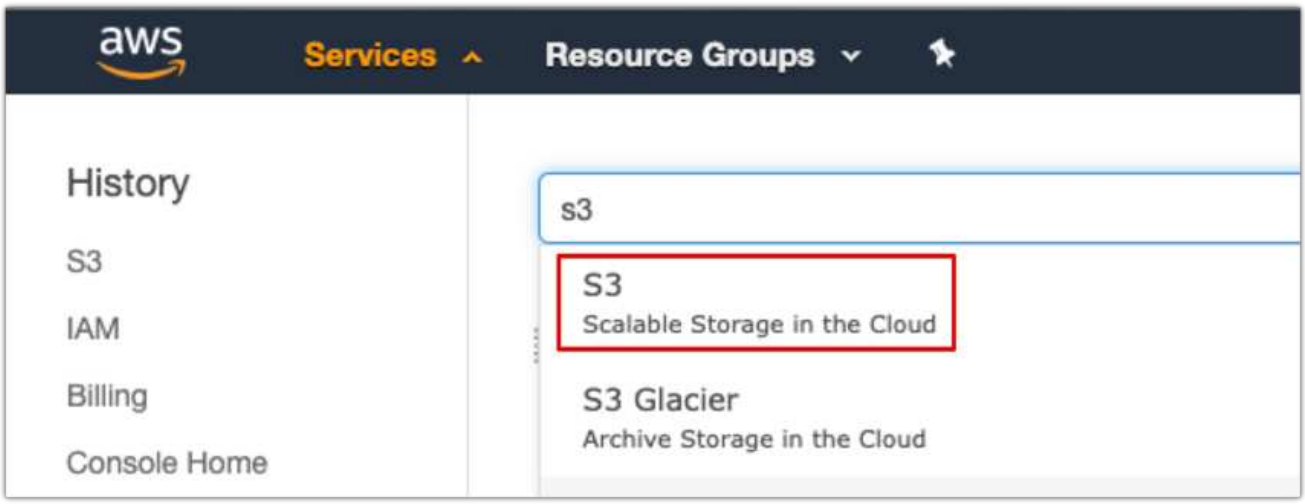
FabricPool unterstützt den Anhang eines Buckets pro Aggregat, wie in der folgenden Abbildung dargestellt. Ein einzelner Bucket kann mit einem einzelnen Aggregat verbunden werden, und ein einzelner Bucket kann mit mehreren Aggregaten verbunden werden. Jedoch kann ein einzelnes Aggregat nicht an mehrere Buckets angehängt werden. Obwohl ein einzelner Bucket an mehrere Aggregate in einem Cluster angeschlossen werden kann, empfiehlt NetApp nicht, einen einzelnen Bucket an Aggregate in mehreren Clustern anzuschließen.

Bedenken Sie bei der Planung einer Storage-Architektur, wie sich die Bucket-to-Aggregat-Beziehung auf die Performance auswirken kann. Viele Objektspeicher-Provider legen eine maximal unterstützte Anzahl an IOPS auf Bucket- oder Container-Ebene fest. Umgebungen, die maximale Performance erfordern, sollten mehrere Buckets verwenden, um die Möglichkeit zu verringern, dass Objekt-Storage-IOPS-Einschränkungen die Performance über mehrere FabricPool Aggregate beeinträchtigen könnten. Das Anschließen eines einzelnen Buckets oder Containers an alle FabricPool-Aggregate in einem Cluster könnte für Umgebungen von Vorteil sein, in denen eine Performance-Managebarkeit gegenüber der Cloud-Tier wichtig ist.

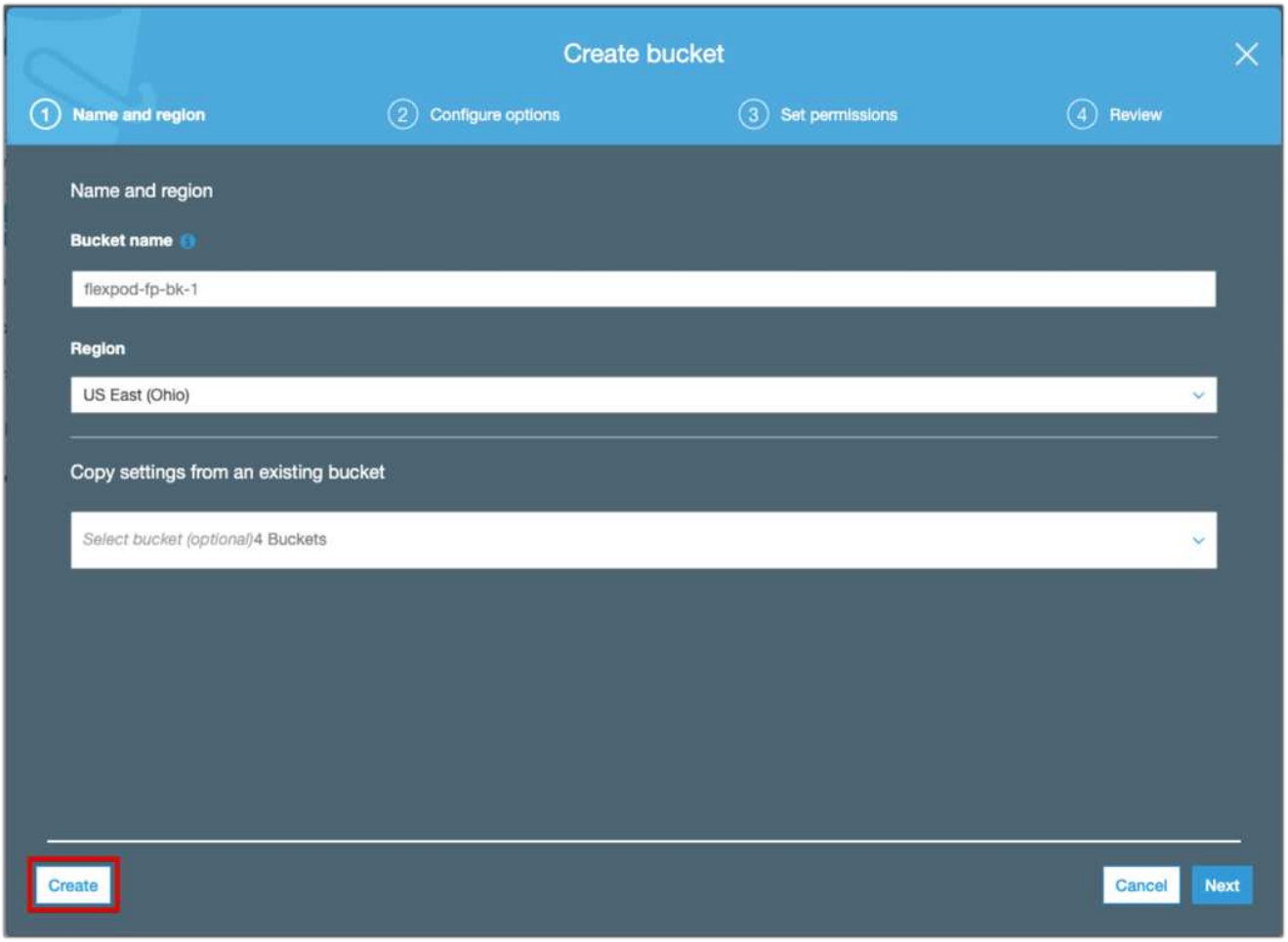


Erstellen eines S3-Buckets

1. Geben Sie in der AWS Management-Konsole von der Startseite aus S3 in die Suchleiste ein.
2. Wählen Sie in der Cloud skalierbaren S3-Storage aus.



3. Wählen Sie auf der S3-Startseite die Option Create Bucket aus.
4. Geben Sie einen DNS-konformen Namen ein, und wählen Sie die Region aus, die zum Erstellen des Buckets dienen soll.



5. Klicken Sie auf Erstellen, um den Objektspeicher-Bucket zu erstellen.

"Als Nächstes: Cloud-Tier zu ONTAP hinzufügen"

Hinzufügen einer Cloud-Tier zu ONTAP

Bevor ein Objektspeicher an ein Aggregat angehängt werden kann, muss er zu ONTAP hinzugefügt und von ihm identifiziert werden. Dieser Vorgang kann mit OnCommand System Manager oder der ONTAP CLI abgeschlossen werden.

FabricPool unterstützt Amazon S3, IBM Object Cloud Storage und Microsoft Azure Blob Storage-Objektspeicher als Cloud-Tiers.

Sie benötigen die folgenden Informationen:

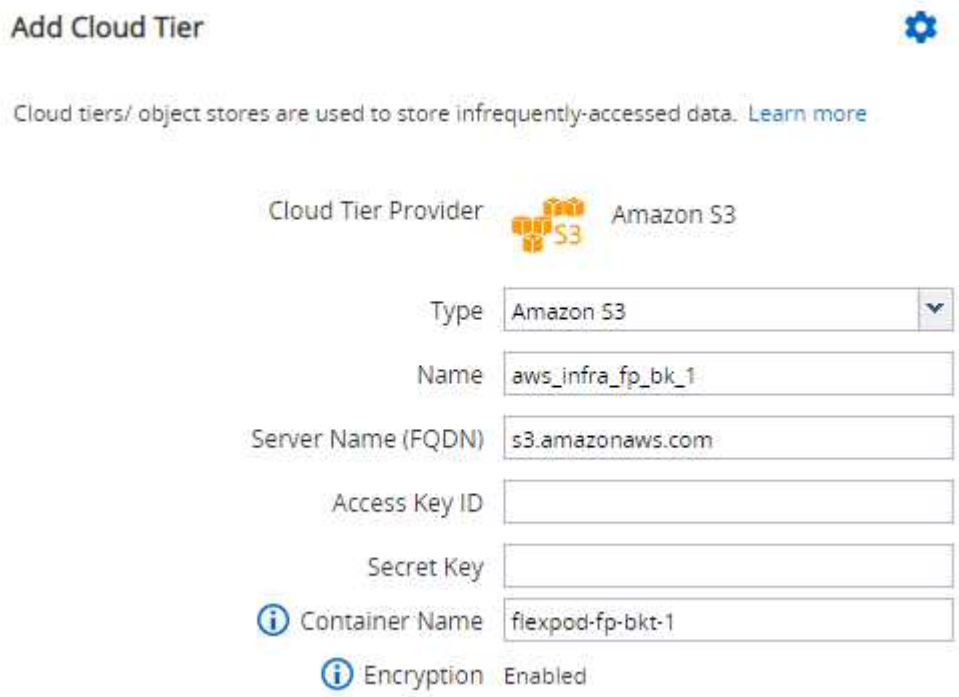
- Servername (FQDN), z. B. `s3.amazonaws.com`
- Zugriffsschlüssel-ID
- Geheimer Schlüssel
- Container-Name (Bucket-Name)

OnCommand System Manager

Um eine Cloud-Ebene mit OnCommand System Manager hinzuzufügen, gehen Sie wie folgt vor:

1. Starten Sie den OnCommand System Manager.
2. Klicken Sie Auf Storage.
3. Klicken Sie Auf Aggregate & Disks.
4. Klicken Sie Auf Cloud Tiers.
5. Wählen Sie einen Objektspeicheranbieter aus.
6. Füllen Sie die Textfelder aus, die für den Objektspeicheranbieter erforderlich sind.

   Geben Sie im Feld Container-Name den Bucket- oder Containernamen des Objektspeichers ein.
7. Klicken Sie auf Save and Attach Aggregates.



CLI VON ONTAP

Geben Sie die folgenden Befehle ein, um mit der ONTAP CLI eine Cloud-Tier hinzuzufügen:

```
object-store config create
-object-store-name <name>
-provider-type <AWS>
-port <443/8082> (AWS)
-server <name>
-container-name <bucket-name>
-access-key <string>
-secret-password <string>
-ssl-enabled true
-ipspace default
```

"Als Nächstes: Cloud-Tier an ein ONTAP Aggregat anschließen."

Cloud-Tier mit einem ONTAP Aggregat verbinden

Nachdem ein Objektspeicher von ONTAP hinzugefügt und von ihm identifiziert wurde, muss er an ein Aggregat angehängt werden, um eine FabricPool zu erstellen. Dieser Schritt kann entweder mit OnCommand System Manager oder mit der ONTAP CLI abgeschlossen werden.

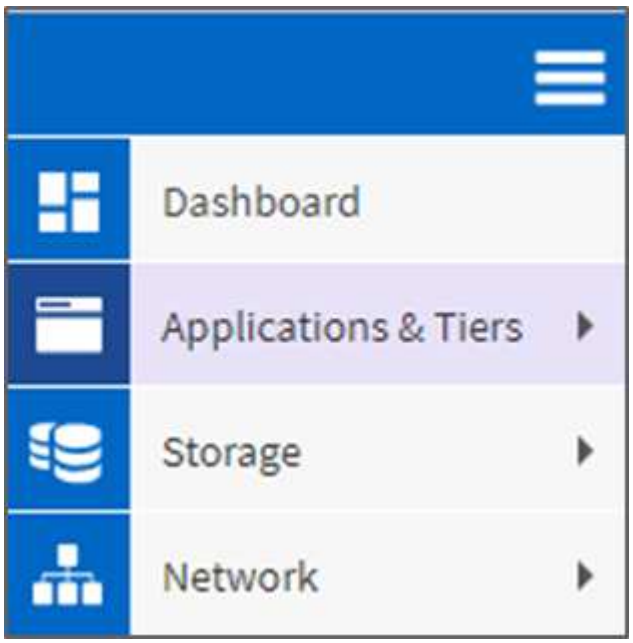
Mit einem Cluster kann mehrere Objektspeichertypen verbunden werden. Mit jedem Aggregat kann jedoch nur ein Objektspeichertyp verbunden werden. So kann beispielsweise ein Aggregat Google Cloud verwenden, ein anderes Aggregat Amazon S3 verwenden, aber an beide kann kein Aggregat angeschlossen werden.

Das Hinzufügen eines Cloud Tier zu einem Aggregat ist eine dauerhafte Aktion. Eine Cloud-Ebene kann nicht von einem Aggregat, an das sie angeschlossen wurde, aufgehoben werden.

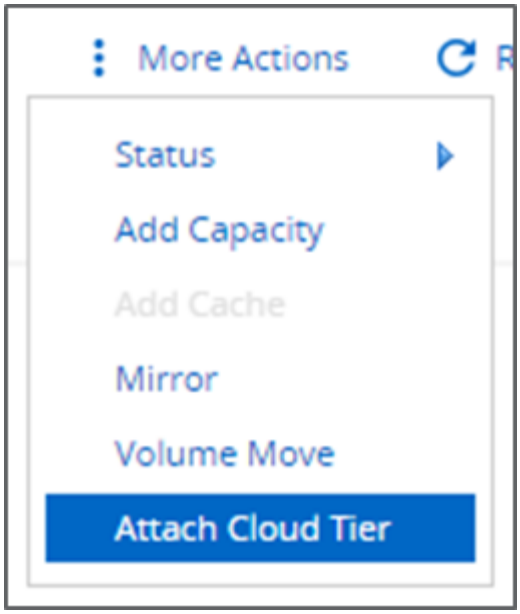
OnCommand System Manager

Gehen Sie wie folgt vor, um ein Cloud-Tier mit OnCommand System Manager an ein Aggregat anzuhängen:

1. Starten Sie den OnCommand System Manager.
2. Klicken Sie Auf Applikationen Und Tiers.



3. Klicken Sie Auf Storage Tiers.
4. Klicken Sie auf ein Aggregat.
5. Klicken Sie auf Aktionen und wählen Sie Cloud Tier anhängen.



6. Wählen Sie eine Cloud-Tier.
7. Anzeigen und Aktualisieren der Tiering-Richtlinien für die Volumes im Aggregat (optional) Standardmäßig wird die Tiering-Richtlinie für Volumes nur als Snapshot festgelegt.
8. Klicken Sie auf Speichern .

CLI VON ONTAP

Führen Sie die folgenden Befehle aus, um ein Cloud-Tier mit einem Aggregat über die ONTAP-CLI anzuhängen:

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <name>
```

Beispiel:

```
storage aggregate object-store attach -aggregate aggr1 -object-store-name
- aws_infra_fp_bk_1
```

"Weiter: Legen Sie eine Volume-Tiering-Richtlinie fest."

Legen Sie eine Volume-Tiering-Richtlinie fest

Standardmäßig verwenden Volumes die Tiering-Richtlinie „Keine Volumes“. Nach der Erstellung eines Volumes kann die Tiering-Richtlinie des Volumes mithilfe von OnCommand System Manager oder der ONTAP CLI geändert werden.

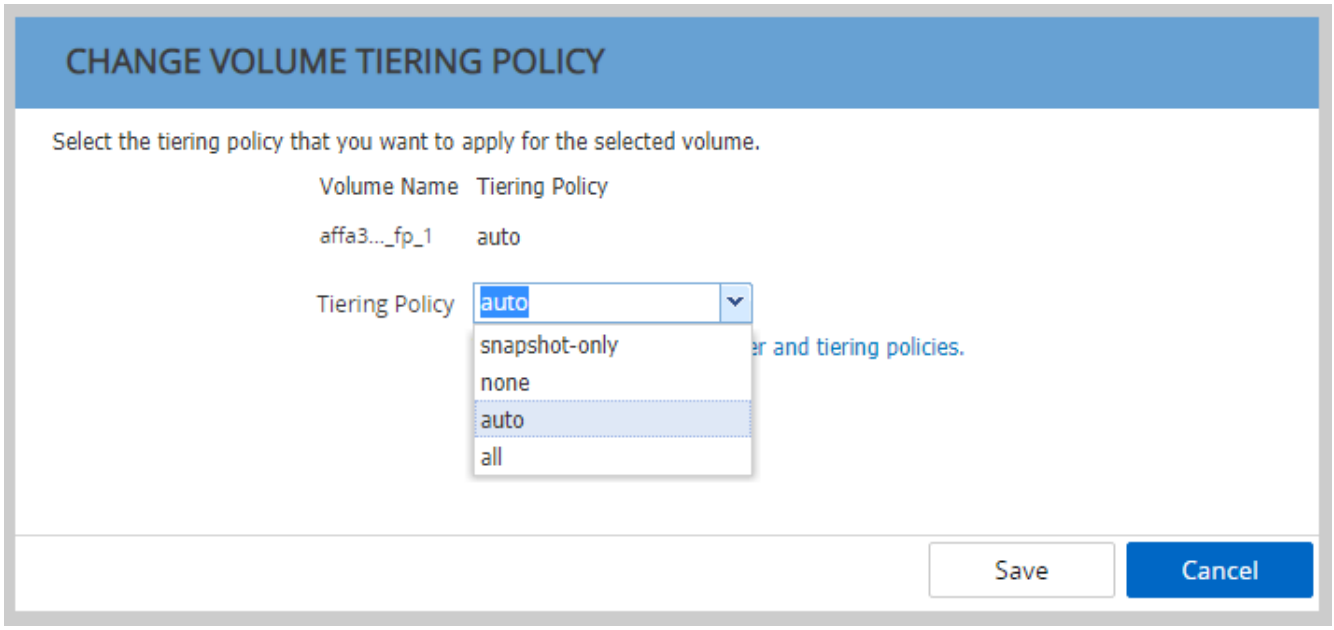
In Verbindung mit FlexPod bietet FabricPool drei Volume Tiering-Richtlinien: Automatisch, nur Snapshot und keine.

- **Auto**
  - Alle „kalten“ Blöcke im Volume werden in den Cloud-Tier verschoben. Angenommen, das Aggregat wird zu mehr als 50 % genutzt, es dauert etwa 31 Tage, bis inaktive Blöcke kalt werden. Die automatische Kühldauer kann mit dem zwischen 2 Tagen und 63 Tagen eingestellt werden `tiering-minimum-cooling-days` Einstellung.
  - Wenn selten genutzte, „kalte“ Blöcke in einem Volume mit einer auf „Auto“ eingestellten Tiering-Richtlinie zufällig gelesen werden, werden sie „heiß“ und in die Performance-Tier geschrieben.
  - Wenn selten genutzte, „kalte“ Blöcke in einem Volume mit einer auf „Auto“ festgelegten Tiering-Richtlinie sequenziell gelesen werden, bleiben sie „kalt“ und verbleiben auf der Cloud-Tier. Sie werden nicht in die Performance-Tier geschrieben.
- **Nur Snapshot**
  - „Kalte“ Snapshot Blöcke im Volume, die nicht mit dem aktiven Filesystem gemeinsam genutzt werden, werden in die Cloud-Tier verschoben. Angenommen, dass das Aggregat zu mehr als 50 % genutzt wird, dauert es etwa 2 Tage, bis inaktive Snapshot-Blöcke kalt werden. Die reine Snapshot-Kühldauer kann mit dem von 2 bis 63 Tagen angepasst werden `tiering-minimum-cooling-days` Einstellung.
  - Wenn selten genutzte, „kalte“ Blöcke in einem Volume mit einer Snapshot-basierten Tiering-Richtlinie gelesen werden, werden sie „heiß“ und auf die Performance-Tier geschrieben.
- **Keine (Standard)**
  - Volumes, die für die Verwendung von „Keine“ als Tiering-Richtlinie festgelegt sind, verlagern selten genutzte Daten nicht auf die Cloud-Tier.
  - Wenn Sie die Tiering-Richtlinie auf „Keine“ setzen, wird ein neues Tiering verhindert.
  - Daten, die zuvor in das Cloud-Tier verschoben wurden, verbleiben im Cloud-Tier, bis sie häufig verfügbar sind. Daten werden automatisch zurück in die Performance-Tier verschoben.

OnCommand System Manager

Um die Tiering-Richtlinie eines Volumes mithilfe von OnCommand System Manager zu ändern, führen Sie die folgenden Schritte aus:

1. Starten Sie den OnCommand System Manager.
2. Wählen Sie ein Volume aus.
3. Klicken Sie auf Weitere Aktionen, und wählen Sie Tiering Policy ändern aus.
4. Wählen Sie die Tiering-Richtlinie aus, die auf das Volume angewendet werden soll.
5. Klicken Sie auf Speichern .



CLI VON ONTAP

Um die Tiering-Richtlinie eines Volumes mithilfe der ONTAP CLI zu ändern, führen Sie den folgenden Befehl aus:

```
volume modify -vserver <svm_name> -volume <volume_name>
-tiering-policy <auto|snapshot-only|all|none>
```

"Weiter: Legen Sie die Mindestkühltage für das Volume Tiering fest."

Legen Sie für das Volume Tiering mindestens die Kühltage fest

Der `tiering-minimum-cooling-days` Die Einstellung legt fest, wie viele Tage vor dem Verlegen inaktiver Daten auf einem Volume mithilfe der Richtlinie „Auto“ oder „nur Snapshots“ als „kalt“ eingestuft werden müssen und für das Tiering geeignet sind.

Automatisch

Der Standardwert `tiering-minimum-cooling-days` Die Einstellung für die Auto-Tiering-Richtlinie beträgt 31 Tage.

Da die Blocktemperaturen durch Lesevorgänge heiß bleiben, kann eine Erhöhung dieses Werts die Menge der Daten reduzieren, die für Tiers geeignet sind, und die in der Performance-Tier aufzubewahren sind.

Wenn Sie diesen Wert ab den Standardwerten von 31 Tagen verringern möchten, beachten Sie, dass die Daten nicht mehr aktiv sein sollten, bevor Sie als „kalt“ markiert werden. Zum Beispiel, wenn eine mehrtägige Arbeitsbelastung erwartet wird, um eine erhebliche Anzahl von Schreibvorgängen am Tag 7, das Volumen durchzuführen `tiering-minimum-cooling-days` Die Einstellung sollte nicht niedriger als 8 Tage sein.

Objekt-Storage ist kein transaktionsorientierter ähnlicher Datei- oder Block-Storage. Änderungen an Dateien, die als Objekte in Volumes mit übermäßig aggressiven Mindestkühltagen gespeichert werden, können zur Erstellung neuer Objekte, zur Fragmentierung vorhandener Objekte und zur Ergänzung von Storage-Ineffizienzen führen.

Nur Snapshot

Der Standardwert `tiering-minimum-cooling-days` Die Einstellung für die reine Snapshot Tiering-Richtlinie beträgt 2 Tage. Ein Minimum von zwei Tagen gibt zusätzliche Zeit für Hintergrundprozesse, um maximale Storage-Effizienz zu gewährleisten und verhindert, dass tägliche Datensicherungsprozesse vom Cloud-Tier aus die Daten lesen müssen.

CLI VON ONTAP

Um die eines Volumens zu ändern `tiering-minimum-cooling-days` Führen Sie den folgenden Befehl aus, indem Sie die ONTAP-CLI verwenden:

```
volume modify -vserver <svm_name> -volume <volume_name> -tiering-minimum
-cooling-days <2-63>
```

Die erweiterte Berechtigungsebene wird erforderlich.

Durch Ändern der Tiering-Richtlinie zwischen „Auto“ und „nur Snapshot“ (oder umgekehrt) wird die Inaktivitätsdauer von Blöcken auf der Performance-Tier zurückgesetzt. Bei einem Volume, das die Auto-Volume-Tiering-Richtlinie verwendet und Daten auf der Performance-Tier, die 20 Tage inaktiv war, wird die Performance-Tier-Dateninaktivität auf 0 Tage zurückgesetzt, wenn die Tiering-Richtlinie nur Snapshot lautet.

Überlegungen zur Performance

Größe der Performance-Tier

Beachten Sie bei der Planung der Dimensionierung, dass die Performance-Ebene in der Lage sein sollte, die folgenden Aufgaben zu erfüllen:

- Unterstützung wichtiger Daten
- „Kalte“ Daten werden unterstützt, bis die Tiering-Scans die Daten in die Cloud-Tier verschieben
- Unterstützung von Cloud-Tiering-Daten, die heiß werden und in die Performance-Tier geschrieben werden
- Unterstützung von WAFL Metadaten, die der angeschlossenen Cloud-Tier zugeordnet sind

Für die meisten Umgebungen ist ein Performance-Verhältnis von 1:10 bei FabricPool-Aggregaten äußerst zurückhaltend und bietet gleichzeitig bedeutende Storage-Einsparungen. Wenn es beispielsweise Absicht ist, 200 TB auf Cloud-Tier zu verlagern, dann sollte das Performance-Tier-Aggregat mindestens 20 TB betragen.

Schreibvorgänge vom Cloud-Tier auf die Performance-Tier werden deaktiviert, wenn die Kapazität der Performance-Tier größer als 70 % ist. In diesem Fall werden Blöcke direkt aus der Cloud-Tier gelesen.

Größe des Cloud-Tiers

Bei der Planung der Dimensionierung sollte der als Cloud-Tier wirkende Objektspeicher in der Lage sein, die folgenden Aufgaben zu erfüllen:

- Unterstützung von Lesevorgängen vorhandener kalter Daten
- Unterstützung von Schreibvorgängen neuer kalter Daten
- Unterstützt das Löschen und Defragmentierung von Objekten

Betriebskosten

Der "FabricPool-Wirtschaftsrechner" Das unabhängige Unternehmen Evaluator Group kann die Kosteneinsparungen für Cold-Data-Storage vor Ort und in der Cloud projizieren. Der Rechner bietet eine einfache Schnittstelle, mit der Sie die Kosten für das Speichern von selten genutzten Daten auf einer Performance-Tier ermitteln können, statt sie für den verbleibenden Lebenszyklus der Daten an ein Cloud-Tier zu senden. Die Berechnung basiert auf einer 5-Jahres-Berechnung und ermittelt die Storage-Kosten über den Zeitraum mit den vier zentralen Faktoren wie Quellkapazität, Datenwachstum, Snapshot-Kapazität und Prozentsatz kalter Daten.

Schlussfolgerung

Der Weg in die Cloud unterscheidet sich zwischen Unternehmen, verschiedenen Geschäftsbereichen oder sogar zwischen den Geschäftsbereichen innerhalb eines Unternehmens. Einige entscheiden sich für eine schnelle Einführung, andere hingegen eher zurückhaltend. FabricPool wird unabhängig von ihrer Größe und unabhängig von der schnellen Einführung der Cloud in die Cloud-Strategie von Unternehmen integriert und demonstriert somit die Effizienz- und Skalierungsvorteile einer FlexPod Infrastruktur.

Wo Sie weitere Informationen finden

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

- FabricPool Best Practices in sich vereint

  "www.netapp.com/us/media/tr-4598.pdf"

- NetApp Produktdokumentation

  "https://docs.netapp.com"

- TR-4036: Technische Spezifikation für das FlexPod Datacenter

  "https://www.netapp.com/us/media/tr-4036.pdf"

FlexPod Datacenter for Hybrid Cloud with Cisco CloudCenter and NetApp Private Storage – Design

Haseb Niazi, Cisco David Arnette, NetApp

Cisco Validated Designs (CVDs) bieten Systeme und Lösungen, die entwickelt, getestet und dokumentiert sind, um Kundenimplementierungen zu vereinfachen und zu verbessern. Diese Designs umfassen eine breite Palette von Technologien und Produkten in ein Portfolio von Lösungen, die entwickelt wurden, um die geschäftlichen Anforderungen der Kunden zu erfüllen und sie vom Design bis zur Implementierung zu begleiten.

"FlexPod Datacenter for Hybrid Cloud with Cisco CloudCenter and NetApp Private Storage – Design"